processes

MDPI

Article

Hybrid AI- and Blockchain-Powered Secure Internet Hospital Communication and Anomaly Detection in Smart Cities

Xiaofeng Wang [1], Xiaoguang Yue [1,*], Noshina Tariq [2] and Ahthasham Sajid [3,4]

[1] College of Management, Shenzhen University, Shenzhen 518060, China; freewxf@szu.edu.cn
[2] Department of Artificial Intelligence and Data Science, National University of Computer and Emerging Sciences, Islamabad 44000, Pakistan; noshina.tariq@isb.nu.edu.pk
[3] Faculty of Computing and Informatics, Multimedia University, Cyberjaya 63100, Malaysia; ahthasham.sajid@riphah.edu.pk
[4] Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad 46000, Pakistan
* Correspondence: xgyue@whu.edu.cn

Abstract: Internet of Things (IoT) devices have revolutionized real-time monitoring and distant patient care in smart cities' healthcare systems. However, this advancement has come with several issues, such as data security, scalability, operational efficiency, and fault tolerance. Previous approaches are not well suited to the real-time processing of IoT data in healthcare, given the low latency, high throughput, and effective anomaly detection needed for such a task. Given these challenges, this paper proposes a hybrid Artificial Intelligence (AI)- and blockchain-based IoT governance framework for Internet hospitals using Proof-of-Authority (PoA) in smart cities. It encompasses application of the enhanced RSA for secure data transmission, real-time anomaly detection through the Isolation Forest algorithm, and a private blockchain architecture designed for high scalability. It effectively detects tampering and replay attacks to minimize illegitimate and unauthorized access or manipulation of patients' data. The proposed framework achieves relatively significant improvements over a state-of-the-art baseline model. It has cut the transaction response time by 50%, doubled the Throughput Per Second (TPS), and attained a 100% detection performance in anomalies. Comparative analysis reveals its linear scalability with increasing workload, ensuring consistent performance under varying transaction volumes. This study's findings highlight the proposed framework's potential to mitigate key issues in IoT-enabled Internet hospitals in smart cities.

Keywords: anomaly detection; blockchain; distributed role-based access control; electronic health records; internet hospital; internet of things; isolation forest algorithm; smart cities; proof-of-authority; Rivest–Shamir–Adleman (RSA)

check for updates

Academic Editor: Massimo Caruso

Received: 29 January 2025
Revised: 21 April 2025
Accepted: 6 May 2025
Published: 11 May 2025

Citation: Wang, X.; Yue, X.; Tariq, N.; Sajid, A. Hybrid AI- and Blockchain-Powered Secure Internet Hospital Communication and Anomaly Detection in Smart Cities. *Processes* **2025**, *13*, 1466. https://doi.org/10.3390/pr13051466

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Internet of Things (IoT) devices in healthcare have led to a paradigm change in patient care by providing real-time data acquisition, remote monitoring, and predictive analytics [1,2]. Powered by IoT, Internet hospitals have become critical solutions to rendering accessible, efficient, and personalized healthcare services in smart cities [3]. These hospitals directly develop wearable devices, remote sensors, and interconnected systems that help monitor patient vitals and allow telemedicine. However, this digitization creates significant data security, scalability, and operational reliability problems that, if ignored, can threaten patient safety and negatively impact the general population's trust in healthcare systems [4].

Of all the challenges, one is the security of sensitive patient data generated by IoT devices [5]. Because of these devices' limited computational resources and their distributed nature, they can be subject to data breaches, tampering, and replay attacks [6]. Such vulnerabilities provide avenues to unauthorized access, falsified medical records, and even life-threatening misdiagnoses [7]. Additionally, real-time IoT data impose scalability constraints on existing healthcare systems due to the need to process and store such big data volumes [8]. Modern Internet hospitals are inherently inappropriate for this high-throughput and low-latency requirement. In addition, centralized architectures cannot effectively accommodate these needs, often leading to bottlenecks, inefficiencies, and higher overall operational costs [9].

On top of security and scalability, fault tolerance and data integrity remain problems that must be solved [10]. IoT devices run in a dynamic environment wherein device failures, network disruptions, and anomalous behavior or observation are the norm [11]. Healthcare systems may lack robust fault tolerance mechanisms and effective anomaly detection when they cannot operate reliably and in continuity of service [12]. Current solutions have been designed to protect the electronic health record (EHR) or provide an essential means of sharing data and fail to satisfy the specific demands of IoT-enabled Internet hospitals in smart cities, where real-time data processing, anomaly detection, and system scalability are required [13].

Across multiple industries in smart cities, such as healthcare, it has been recognized that blockchain technology has the potential to mitigate these challenges [14]. Due to the decentralization of data storage and the forcing of immutable records using cryptographic hash functions, the blockchain offers a built-in secure platform for storing sensitive information [15]. The blockchain's transparency and the ability to utilize it to facilitate a distributed consensus removes single-point-of-failure and allows users to audit and trust [16]. While the blockchain is adopted for IoT-enabled Internet hospitals, it has its challenges [17]. IoT systems create a faster, lower-latency data stream, producing a high volume of data that is to be processed and securely logged in a near real-time manner without overburdening the blockchain-based networks [18]. Additionally, the augmentation of real-time anomaly detection in a smart city integrated with the blockchain to date has been missed in healthcare applications where there is a yet-to-be-covered issue of dynamic and non-predictable IoT scenarios [19].

The implementation of IoT in healthcare creates security problems while demanding scalable capabilities alongside robust anomaly recognition technology for dynamic systems. Real-time processing challenges in existing centralized computational systems result in performance bottlenecks and security risks from tampering and replay attacks. This paper, therefore, proposes a hybrid Artificial Intelligence (AI)- and blockchain-powered IoT governance framework for smart cities to fill the above gaps in Internet hospitals based on our previous work [20]. A novel blockchain-based framework is proposed that blends blockchain technology with strategic cryptographic and AI-based anomaly detection techniques for securing patient data, incorporating scalability and fault tolerance in smart cities' healthcare systems. The framework has robust data security and system integrity by employing the Isolation Forest algorithm for real-time anomaly detection, tampering, and replay attack detection. The key contributions of this work are as follows:

1. An optimized blockchain architecture designed to scale and support a high healthcare transaction volume with minimal latency and low computational overhead in smart cities is presented.
2. A hybrid framework that mitigates data integrity and confidentiality issues in smart city Internet hospitals is designed and proposed.

3. Integration of the Isolation Forest algorithm to detect anomalies in a smart city's IoT data streams to facilitate proactive responses to anomalies is proposed.
4. Implementation of tampering detection and replay attack resistance mechanisms tailored to smart city healthcare systems.

In the rest of the paper, related work is discussed in Section 2, the proposed framework is provided in Section 3, and the proposed methodology is presented in Section 4. Section 5 represents the mathematical analysis of the proposed framework. The experimental setup and results are detailed in Section 6, followed by the conclusion in Section 7.

2. Related Work

Mazhar, Tehseen et al. [3] investigated the blockchain technology and Generative Artificial Intelligence (GenAI) in the healthcare sector, emphasizing enhanced data protection, personalized treatment, and optimized operations. The system fails to address difficulties, including restricted scalability, high energy expenditures, and interoperability shortcomings. Bhabendu Kumar Mohanta et al. [17] studied blockchain healthcare applications, which consisted of protection measures for health data alongside personalized medical care and enhanced operational processes. The method used InterPlanetary File System (IPFS) and Advanced Encryption Standard (AES) encryption to implement security protocols for protecting patient data throughout IoT healthcare systems. The study did not thoroughly explore challenges, including scalability problems, elevated energy requirements, unideal hardware requirements, and limited system compatibility. In their research, Cihan et al. [21] performed a systematic review study to study blockchain usage in clinical research settings. The analysis included observations about company dimensions and the lack of standard legal guidelines requiring General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) compliance. Therefore, they presented a conceptual framework that might assist software developers and clinical researchers applying the blockchain.

Singh et al. [22] proposed a novel blockchain-based hybrid security architecture for healthcare networking systems. This model aimed to enhance the security of stored information, data privacy, and the system's capability by integrating PoW and PoS. The proposed framework increased computational effectiveness and strengthened security measures. It addressed the issue of sharing medical data, making them easier to access across various stakeholders in the health industry. The proposed approach exhibited significant enhancements in distinct indicators as compared to the original method, such as time to complete a transaction, memory utilization, and data throughput. Pimple et al. [23] presented a strategy to enhance the security of the healthcare sector. The research combined blockchain technology and Ensemble Learning to tackle security issues, including unauthorized access and data leakage, promoting system security. Customers benefit from a distributed ledger achieved through blockchain integration because it removes data manipulation threats while offering safe transaction execution.

Using blockchain technology, Meng et al. [24] proposed an innovative method for secure data deletion in IoT environments. They addressed limitations in existing methods, such as dependence on trusted third parties and the high cost of encryption. They used smart contracts for access management, secret key sharing elimination, and a Merkle Hash Tree for deletion verification. The system obliterated third-party requirements while enhancing operational speed. The proposed mechanism processed data rapidly through secure deletion and verification, assuming minimal computational burden and allowing users to specify custom deletion time parameters. Research by Ahmadi and Sina [25] investigated Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) as security and privacy enhancers for distributed identity systems through user-controlled identity

management capabilities. The research project studied the potential for combining these technologies with Zero Trust Architecture (ZTA) to boost network defence and block lateral hopping attempts while resolving compatibility and regulatory compliance problems. The study demonstrates that distributed identity systems protect security using contextual authorization methods while simultaneously boosting confidentiality standards.

CovMedCare represents a decentralized monitoring system for COVID-19 inpatients, which Krishna et al. presented in their study. The research adopted Machine Learning (ML), IoT, and blockchain technology integration to detect deterioration of health conditions for prompt medical interventions. The system demonstrated 99% accuracy in such patient risk identification tasks beyond what current monitoring systems achieved. Ngoupayou et al. [26] studied how Federated Learning (FL) could unite with Privacy-Enhancing Technologies (PETs) and blockchain features for handling privacy silo issues in smart healthcare systems (SHSs). According to the research, PETs enhance FL's privacy features, but blockchain technology excels at protecting stored models and aggregating data through secure infrastructure and gradient management. The combined use of these technologies demonstrates their power to protect the confidentiality and integrity of healthcare data, thus enabling secure smart healthcare systems for patient data protection.

Salunkhe et al. [27] developed an advanced blockchain-based operation management framework to resolve better healthcare data security, privacy, interoperability, and scalability issues. Under this framework, the blockchain combines with Filecoin-powered IPFS to deliver advanced security and privacy during Electronic Medical Record (EMR) management. Zero-knowledge-proof mechanisms join decentralization protocols to guarantee privacy-focused data security and integrity preservation. The proposed framework maintains full node identity, yet patients decide between light node or full node status while medical facilities function as IPFS endpoints. The research team studied blockchain scalability in healthcare while improving system security mechanisms and increasing system performance rates. Researchers Dhinakaran, D. et al. [28] developed the Adaptive Feature-Centric Polynomial Data Security Model (AFPDSM) for strengthening security levels in electronic health records (EHRs). The encryption system used data importance categories alongside blockchain technology and polynomial functions to establish secure access through features. The researchers achieved security improvements of 98% while also improving access control and demonstrating encryption and decryption speeds of 101 s and 104 s, along with a 21% decrease in network costs. Better EHR management received significant improvements from these technological developments.

Karthikeyan V. et al. [29] examined how blockchain systems improve healthcare record security through cryptographic capabilities against cyber threats. The authors showed how traditional methods fall short while positioning blockchain features of decentralization alongside immutable data and cryptographic security as viable answers. The research presented three healthcare blockchain solutions that incorporated identity-based security systems for access protocols, smart contracts for information exchange, and provable data-record-tracking methods. Standardized protocols and stakeholder partnerships demand attention to achieve scalability alongside interoperable and compliant operations. Wang et al. [20] created an alliance blockchain system with enhanced RSA encryption for Internet hospital data management, which delivered faster throughput at 24.7% and diminished latency at 19.8%, diminished memory occupied at 14.3%, and elevated decryption speed by 97.5%. Real-time data management of IoT sensors through an effective system allowed organizations to enhance the security and performance of healthcare data transactions. The use of private blockchain systems leads to both centralization of control and decreased transparency and remains burdened with scalability challenges because of

increasing volumes of data. Table 1 provides a summary of methodologies, advantages, and limitations of blockchain-based healthcare solutions.

Table 1. Summary of methodologies, advantages, and limitations in blockchain-based healthcare solutions.

Paper	Methodology	Advantages	Limitations
[3]	Blockchain and AI for enhanced security and privacy.	Better security, personalized treatment, cost reduction.	Scalability, energy use, interoperability.
[17]	Blockchain with IPFS, edge computing, and encryption.	High performance, decentralized, secure.	Challenges with low-end devices, scalability.
[21]	Literature review and conceptual model of blockchain in clinical research.	Improved privacy, secure data, immutable records.	Legal and compliance issues, scalability.
[22]	Hybrid security with PoW and PoS, IoT integration.	Efficient data management, secure communication.	Risk of centralization, scalability issues.
[23]	Blockchain, Ensemble Learning, and MAFS for secure CPS.	Stronger security, data integrity, cyber resilience.	Integration complexity, scalability challenges.
[24]	Blockchain with smart contracts and secure data deletion.	Fast and secure data deletion, low overhead.	Delays in off-chain verification, limited use cases.
[25]	Blockchain-based distributed identity management.	Better security, privacy, and compliance.	Integration with legacy systems, scalability.
[30]	Blockchain with IoT and ML for patient monitoring.	Accurate health prediction, real-time monitoring.	High data processing, large-scale limitations.
[26]	Federated Learning and blockchain for privacy protection.	Improved privacy, data integrity.	Integration complexity, scalability issues.
[27]	Blockchain and IPFS for EMR management with privacy.	High privacy, decentralized, scalable.	Regulatory issues, integration complexity.
[28]	Polynomial encryption with blockchain for EHR security.	Improved security, low complexity.	High implementation complexity, scalability.
[29]	Blockchain for immutable records and identity management.	Increased security, patient control, confidentiality.	Interoperability issues, adoption barriers.
[20]	Blockchain with IoT and RSA encryption for data governance.	Optimized data transactions, better encryption.	Centralization, scalability issues.

3. Proposed Framework

IoT-enabled healthcare systems are growing exponentially, creating problems with data security, scalability, real-time processing, and fault tolerance. We propose a hybrid AI and blockchain-based IoT governance framework to solve those issues. We integrate real-time anomaly detection, secure cryptographic protocols, and a dynamic feedback mechanism to make this processing and decision-making robust. The architecture of the proposed system is divided into five core modules which include data acquisition, anomaly detection, encryption, storage in blockchain, and analysis. These modules have been illustrated in Figure 1. Based on a modular design, the proposed architecture uses data to seamlessly flow through layers, keeping the architecture stably adaptive, optimal, and modular simultaneously. The architecture is shown in Figure 2. It consists of five core modules: the IoT Data Module, the Anomaly Detection Module, the Blockchain Module, the Data Storage and Analysis Module, and the Access Control Module.

However, these are connected through a dynamic feedback mechanism that periodically recalibrates and optimizes system performance. It shows the proposed framework being modular. Herein, the data flow between IoT devices, anomaly detection, blockchain storage, access control, and dynamic feedback loop, which ensures continuous optimization, is highlighted. The process starts from the IoT Data Module and proceeds with data collection, preprocessing, and sending it to the Anomaly Detection Module for evaluation. The Central Authority Module validates flagged anomalies, and the Blockchain Module encrypts and stores normal data flows. In the Data Storage and Analysis Module, verified

data are stored and analyzed, creating insight for stakeholders to utilize and inform predictive analytics. Alerts and updates are flowing dynamically across modules. For instance, anomaly alerts generate responses from healthcare professionals, and system performance metrics generate updates in system policies in the feedback loop. With the Patient Module, insights are shared with patients, closing the loop and guaranteeing that all stakeholders are updated. The proposed flow is further illustrated in Figure 3.

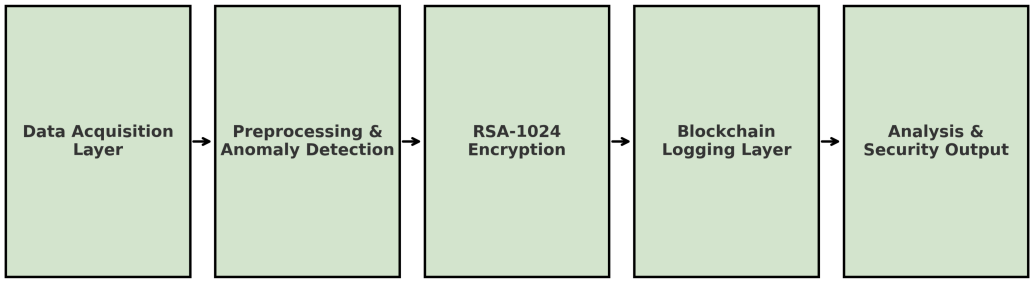


Figure 1. High-level architecture of the proposed IoMT blockchain-based security framework, showing key system modules.

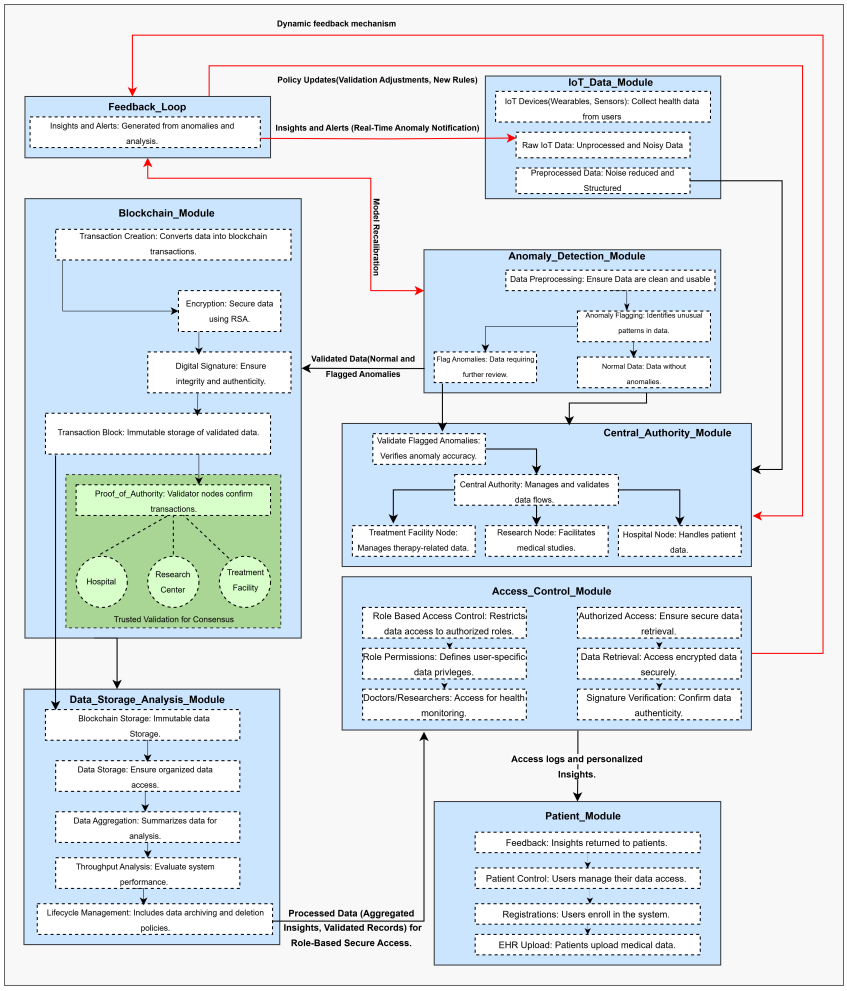


Figure 2. Hybrid AI and blockchain-based IoT governance framework.

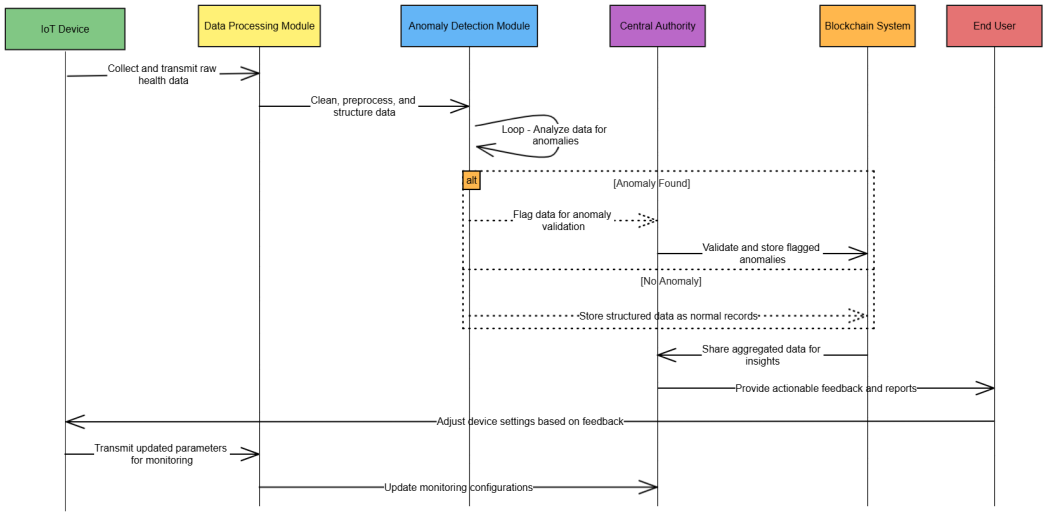


Figure 3. Sequence diagram of the proposed model.

System Architecture

The framework's design is based on a layered architecture: data collection and preprocessing happen at the IoT layer, followed by anomaly detection, secure storage, and data governance using blockchain. The design is specific to each module yet complementary, addressing the requirements of an IoT-enabled healthcare system. Figure 4 depicts the overall flow of the framework, highlighting the primary decision points, anomaly detection, encryption, and logging activities on the blockchain.

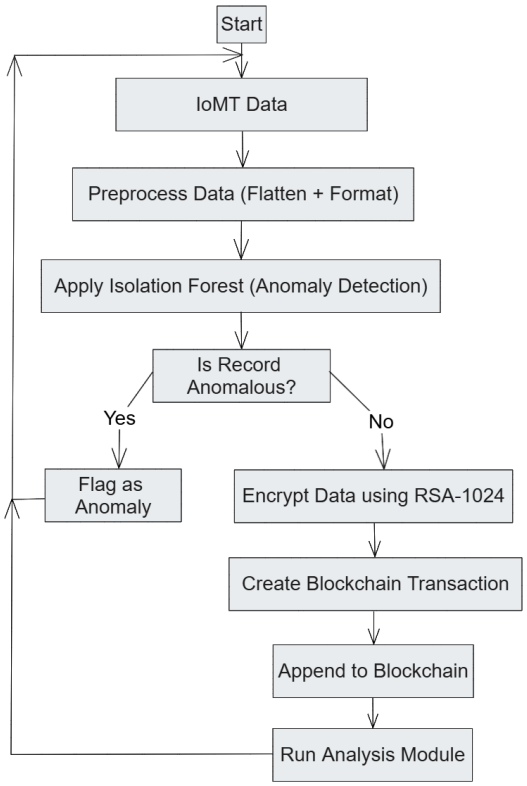


Figure 4. Flowchart illustrating the sequence of operations in the proposed IoMT anomaly detection and blockchain logging framework.

1. IoT Data Module: The architecture starts with the IoT Data Module, which gathers real-time health data from devices like wearables, sensors, and medical monitors. These measure heart rate, glucose levels, and physical activity. The data received from

these devices are frequently noisy or unstructured, requiring preprocessing to verify and improve consistency and quality. This module cleans and organizes data so that any downstream processing is accurate and reliable. IoT devices (i) collect raw data D_i where $i \in \{1, 2, \ldots n\}$. Noise is removed from data, and they are structured for analysis. The preprocessing function P is expressed as Equation (1).

$$D_i' = P(D_i) \tag{1}$$

where D_i' represent the cleaned and structured data. It guarantees the input integrity of the downstream modules. This module's significance is that it provides a constant feed of patient data to detect health problems early and offer personalized care. It is the critical entry point of the system where data integrity has to start. The processed data are then used to evaluate the Anomaly Detection Module.

2. Anomaly Detection Module: After data preprocessing, they go to the Anomaly Detection Module, where data are searched for abnormalities. It can detect patterns suggesting device failures, poor health, other aspects, trends, or abnormal patterns. Anomalies are identified and marked for follow-up, while normal data will be processed in the system. The preprocessed data D_i' are evaluated against thresholds $\Theta = [\theta_{\min}, \theta_{\max}]$ using the anomaly detection function A, given in Equation (2).

$$A(D_i') = \begin{cases} \text{Flagged as anomaly}, & \text{if } D_i' \notin \Theta \\ \text{Normal}, & \text{if } D_i' \in \Theta \end{cases} \tag{2}$$

This module is central to the system's reliability and accuracy because it is responsible for ensuring that all the results produced by the system are accurate. Thus, its usage helps prevent damaged data from skewing healthcare decisions before the outliers can be identified. Normal data are forwarded to the Blockchain Module, and the Central Authority Module immediately takes flagged data for attention.

3. Blockchain Module: The Blockchain Module is the backbone of the proposed architecture. Data are encrypted and stored on a decentralized, tamper-proof ledger. The blockchain's Proof-of-Authority (PoA) consensus mechanism will ensure that trusted nodes, such as hospitals, research centers, and treatment facilities, validate transactions. Validated data are securely stored in the blockchain ledger L. Each data transaction T_j is defined using Equation (3):

$$T_j = \{D_j', \text{timestamp}, \text{signature}\} \tag{3}$$

Verification of T_j is achieved through a consensus mechanism V, represented in Equation (4).

$$V(T_j) = \begin{cases} \text{Append to ledger}, & \text{if consensus is reached by } N_k \\ \text{Reject}, & \text{otherwise} \end{cases} \tag{4}$$

This module is important to safeguard the quality of the data collected and achieve the trust of the players involved. As it means data cannot be changed after they are recorded, the system complies with high data protection standards, mandatory for the healthcare industry. Furthermore, it is characterized by a traceable and transparent transaction since it is an immutable ledger. The Blockchain Module submits a verified data package to the Storage and Analysis Module, guaranteeing a secure exchange.

4. Data Storage and Analysis Module: The Data Storage and Analysis Module contains the validated data, where such information is compiled and archived. The function of

this module is to help store data for statistical and predictive analysis of health trends in the medical decision-making process. It also uses throughput analysis for system performance tracking and lifecycle management to enable correct data retention and deletion in compliance with the rules. Aggregated data D_{agg} over a time window T_w are computed using Equation (5).

$$D_{agg} = \sum_{t=1}^{T_w} D_t \tag{5}$$

Predictive analytics is applied using models M to forecast trends, such as glucose levels G_{t+1}, computed using Equation (6).

$$G_{t+1} = M_g(D_{agg}) \tag{6}$$

This module is crucial for turning large and sometimes chaotic piles of raw data into useful information. Researchers and healthcare providers use these insights to conduct clinical research, plan treatments, and improve systems. The specific alerts created from the analysis in the predictive model or from system performance checks are then passed over to other modules to be updated.

5. Access Control Module: The access to stored data is strictly controlled using the Access Control Module. It employs a model known as role-based access control (RBAC); access privileges are granted based on the role a person aspires to, as a doctor, researcher, or patient. It follows the principle of least privilege to guarantee that only users with a reason to access certain information will be permitted to do so. Data availability is controlled through a role-based mechanism $R(U)$, where U is a user. Permissions P_r for a user are defined in Equation (7).

$$R(U) = \{P_r | P_r \in \text{Permissions for } U\} \tag{7}$$

This module builds credibility among users and various stakeholders by mitigating patient identification risks and ensuring the safe sharing of patient information. It has some added security features, such as encryption methods and digital signature validation. This module is used to obtain the real data-retrieving request while checking some compliance on privacy issues.

6. Central Authority Module: The Central Authority Module is a control point for the system and offers a human presence where needed. It checks flagged anomalies, guarantees effective data management, and distributes tasks to courser-specific nodes, including the hospital, research, and treatment facility nodes. Each node works on a particular functionality, whether patient handling, treatment, or clinical trial. The feature-marked anomalies $A(D_i')$ are confirmed by the Central Authority Module. The validation function is expressed as Equation (8).

$$C(A(D_i')) = \begin{cases} \text{Confirmed anomaly,} & \text{if validated by expert} \\ \text{False positive,} & \text{otherwise} \end{cases} \tag{8}$$

Alerts α are generated for confirmed anomalies using Equation (9).

$$\alpha = \{D_i', \text{alert type}, \text{recommended action}\} \tag{9}$$

This module's central and crucial feature is its control of decentralization. This allows for fast decisions about flagged anomalies while maintaining responsibility. This

module manages changes in validation rules or system policies, so there is always an upgrade.

7. Feedback Loop: The overall feedback loop guarantees the system's restructuring according to the new requirements. Out of it, it collects insights and alerts of real-time information created by different modules and applies them to enhance the system's policies. For instance, flagged anomalies may cause new algorithms to be developed to detect further anomalous behavior or poor performance metrics may induce system improvements. The feedback loop F alters dynamic thresholds Θ, detection models A, and predictor models M in real-time. For instance, threshold updates are represented in Equation (10).

$$\Theta \leftarrow \Theta + \Delta\Theta \tag{10}$$

This dynamic mechanism is critical for effectively maintaining the system's long-term reliability. The feedback loop information helps to evolve the architecture's implementation, which also allows for customization to new conditions that appear constantly in healthcare and new technologies.

8. Patient Module: It consists of the Patient Module in the center of the architecture through which informational self-determination is available to users. The challenges include the inability of patients to upload the EHRs, the inability of the patient to control the access permissions, and the inability of the patient to receive some insights derived from data analysis. Packet 2 patients communicate with the system through the Patient Module P_m. Queries over a time window T_w retrieve data using Equation (11).

$$P_m(G_t) = \{G_t | t \in T_w\} \tag{11}$$

This module provides the users with accountability and keeps the patients at the core of the systems. It is crucial in building patients' interest and confidence by empowering the individuals through control and providing feedback to ensure good patient-centered decision-making. All information regarding the patient or any changes seen during the process is directly passed through this module.

4. Methodology

While existing solutions use the blockchain only for access management or static data logging, the framework proposed in this paper implements the blockchain as an active anomaly-aware logging mechanism coupled with real-time detection of anomalies using the Isolation Forest algorithm. An abnormal IoMT record is not simply discarded or stored; instead, it is encrypted using RSA-1024 and stored in an unalterable fashion within the blockchain, thus maintaining forensic traceability. Furthermore, implementing the blockchain adopts a lightweight permissioned model using PoA consensus, which is ideal for IoMT networks with limited resources. The ability to combine anomaly filtering, selective encryption, and blockchain logging within a single flow is a primary differentiating attribute of our framework. This section elaborates on the methodology of developing and evaluating the proposed blockchain-based IoT governance framework for Internet hospitals. The proposed approach provides secure and efficient data handling by combining real-time anomaly detection, cryptographic mechanisms, and blockchain technology. The proposed system's architecture, modular implementation, scalability, and adaptability to healthcare settings are outlined in the following section.

4.1. Overview of the Methodology

The proposed layered and modular design methodology effectively manages Internet hospitals for IoT-generated data. We collect and preprocess the patient data, detect and

store real-time anomaly data on the blockchain, and only authorized personnel can access the medical record. Access is controlled by Role-Based Permission (RBP). The system is continuously optimizable by a dynamic feedback mechanism, which allows the system to adapt to changing conditions more easily. Algoritm 1 presents an overall view of the proposed methodology. The methodology combines enhanced RSA encryption and decryption (proposed in our previous work [20]), blockchain-based data storage, and role-based anomaly detection. It starts with creating RSA key pairs for secure communication, then encrypts and decrypts messages. Data are securely stored in a blockchain block, and anomalies are detected using the Isolation Forest applied to the role-specific subset. The space complexity is $O(n+k)$, accounting for storing keys, data, and intermediate results. The computational complexity is $O(k \cdot (\log n)^3 + \log n + n \cdot t)$, which combines the costs of RSA operations, blockchain hashing, and anomaly detection. Key stages of the methodology are as follows:

Algorithm 1 Proposed methodology.

Require: $M \in \mathbb{Z}^k, \mathcal{K}, D \in \mathcal{X}^n, R \in \mathcal{R}$
Ensure: $Results \in \mathbb{R}$
1: $(e,n),(d,n) \leftarrow$ RSA Key Generation$(\mathcal{K})$ ▷ Generate RSA keys
2: **for** $m \in M$ **do**
3: $c \leftarrow m^e \mod n$ ▷ Encrypt message
4: $m' \leftarrow c^d \mod n$ ▷ Decrypt message
5: **end for**
6: $block \leftarrow$ Create Block$(data, prev_hash)$ ▷ Blockchain data storage
7: $A \leftarrow$ Anomaly Detection(D, R, θ) ▷ Detect anomalies using Isolation Forest
8: **return** $Results \leftarrow \{c, m', block, A\}$

In the data acquisition phase, patient vitals are captured using timeline real-time IoT-based wearable devices and sensors. Collecting meaningful user data is made more difficult by their noisy and unstructured nature; these data are then preprocessed locally to improve quality and transmission efficiency. The patient's health data are collected using ECG monitors, pulse oximeters, and glucose meters. Data packets are communicated to devices configured to transmit in predefined intervals. Preprocessing involves the following steps:

- Noise Reduction: Spurious signals arising from environmental interference or device errors are removed by applying techniques such as moving average filtering.
- Data Compression: It compresses redundant information to achieve the highest bandwidth usage for the least compromise in data integrity.
- Caching: During network disruptions, data are temporarily stored locally, reducing risks of loss or delay.

The methodology reduces network load and guarantees the quality of information passed to the last stages by preprocessing data at the edge.

4.1.1. Blockchain Integration

The Blockchain Module securely and immutably stores the patient data. A PoA consensus mechanism enables the system to maintain a compromise between security and computation efficiency.

1. Data Encryption and Storage: Lastly, the RSA algorithm encrypts IoT data, including anomaly flags, and stores them in the blockchain. Each block contains an encrypted patient data block, anomaly flags for detecting anomalies from healthy data, timestamps for temporally tracking data, and hashing links for ensuring tamper-proof integrity. The security of RSA relies on the difficulty of factorizing n into its prime components p and q, as shown in Algorithm 2. If these primes are sufficiently large,

factorizing n is computationally infeasible. In terms of performance, RSA requires $O(\log n)$ space to store keys and intermediate values, where $\log n$ is the number of bits in n. The computational complexity of modular exponentiation, which is used during both encryption and decryption, is $O((\log n)^3)$ when using efficient methods such as repeated squaring. Simplicity for users and strength against attackers make RSA one of today's most important cryptographic systems.

Algorithm 2 RSA encryption and decryption.

Require: $m \in \mathbb{Z}, (e, n) \in \mathbb{Z}^2, (d, n) \in \mathbb{Z}^2$
Ensure: $c, m' \in \mathbb{Z}$
$c \leftarrow m^e \mod n$ ▷ Encryption: Compute ciphertext
$m' \leftarrow c^d \mod n$ ▷ Decryption: Retrieve plaintext
return c, m'

2. Consensus Mechanism: Transactions are authenticated or pre-approved by hospitals, research centers, or other pre-approved validators. This method of storage is fast without computational overheads from typical mechanisms like Proof-of-Work (PoW). It ensures data integrity, that is, trusted healthcare systems.
The blockchain block creation algorithm is shown in Algorithm 3. For this algorithm, a block is created that contains an index i, the block's data $data$, and the hash of the previous block $prev_hash$. A timestamp T is also included so the blocks are in chronological order. The hash function to calculate the block's hash is $H(i, data, T, prev_hash)$. It ensures the integrity and immutability of the blockchain. The algorithm's space complexity is $O(\log n)$, as it requires storage for the block's attributes, where $\log n$ represents the size of these attributes in bits. The computational complexity for calculating the hash is also $O(\log n)$, assuming a fixed-size hash function is used.

Algorithm 3 Blockchain block creation and hashing.

Require: $i \in \mathbb{Z}^+, data \in \mathcal{D}, prev_hash \in \mathbb{H}$
Ensure: $block \in \mathcal{B}$
$block.index \leftarrow i$
$block.data \leftarrow data$
$block.previous_hash \leftarrow prev_hash$
$block.timestamp \leftarrow T$ ▷ Current timestamp
$block.hash \leftarrow H(block.index, block.data, block.timestamp, block.previous_hash)$
return $block$

4.1.2. Data Cleaning, Aggregation, and Anomaly Detection

The Isolation Forest model identifies abnormal data points using the isolation principle with Isolation Forest models, where anomalies are described as data points, which are easier to isolate. Each entry is depicted as a 2D vector of heart rate and body temperature. The model was trained with a contamination factor of 0.1, suggesting that 10% of the data is expected to be anomalous. A record is identified as abnormal when its prediction score is below the anomaly score threshold set by the Isolation Forest model scoring mechanism. No manual thresholds were imposed; however, the noticed typical vs. flagged records ranges are presented in Table 2.

Table 2. Indicative ranges for anomaly detection.

Feature	Normal Range	Anomalous Range (Detected)
Heart Rate (bpm)	60–100	<60 or >100 (based on density)
Temperature (°C)	36.0–38.0	<35.5 or >38.5 (rare instances)

Although no explicit data compression was executed, data aggregation was efficiently performed during the preprocessing phase by transforming nested patient records into a consistent template. For anomaly detection, each patient's records were consolidated into one hundred feature vectors. The non-anomalous, cleaned records were then encrypted and secured on the blockchain. Records that activated anomaly flags were encrypted separately and indexed for log and security analysis.

4.1.3. Data Storage and Analysis

This module aggregates and analyzes validated blockchain data to generate actionable insights. It also evaluates system performance to determine whether one design provides scalability and reliability over another.

1. Data Aggregation: Long-term trends and patterns in patient health are identified using aggregated data to determine, for example, seasonal variation in respiratory conditions.
2. Performance Monitoring: Workloads are tracked to optimize system performance and increase throughput, latency, or storage efficiency.

4.1.4. Anomaly Detection Using Access Control and Feedback

Real-time anomaly detection is a cornerstone of the proposed framework. It allows the detection of possible deviations in patient health metrics. The Isolation Forest algorithm serves this purpose because it processes high-dimensional data efficiently while maintaining effective results. It identifies anomalies through decision tree splits, which determine the segregation of individual data points. Critical anomalies need fewer splits because sudden heart rate spikes and oxygen saturation drops indicate such events. The algorithm sorts anomalies according to preset anomaly score boundaries. Alert mechanisms activate without delay when patient vitals exceed predefined limits. Healthcare interventions become faster through anomaly detection because they eliminate false positive signals but maintain trust in medical decisions. Secure data retrieval is provided to authorized parties through role-based access control (RBAC) mechanisms, while system parameters receive real-time updates from a dynamic feedback loop.

1. Role-Based Permissions: The following permissions are assigned depending on user roles.
    - Doctors: Detailed patient record data enable medical professionals to perform diagnostics and deliver treatment.
    - Researchers: Clinical study datasets are accessible in their anonymized forms.
    - Administrators: Oversee the entire system performance to maintain a balance between components.
2. Feedback Loop Integration: Device thresholds and validation policies receive updates through system analytics feedback alongside anomaly detection algorithms. Analysis of historical data allows healthcare systems to fine-tune detection thresholds, which results in better anomaly identification for elderly patients.

This approach maintains system robustness and responsiveness while enhancing security, performance efficiency, and adaptability through improved conditions. Algorithm 4 takes a dataset D and passes the role-based filter to extract subset D_R. Parameters θ are used to train the Isolation Forest model F on this specific subset. Calculate an anomaly score a_x to identify outliers for any given data point in the role-specific dataset.

Algorithm 4 Anomaly detection using role-based Isolation Forest.

Require: $D \in \mathcal{X}^n, R \in \mathcal{R}, \theta \in \Theta$
Ensure: $A \in \mathbb{R}^n$
1: $D_R \leftarrow \{x \mid x \in D, x.role = R\}$ ▷ Filter dataset by role
2: Train F using D_R and θ
3: **for** $x \in D_R$ **do**
4: $a_x \leftarrow F(x)$ ▷ Compute anomaly score
5: **end for**
6: **return** $A \leftarrow \{a_x \mid x \in D_R\}$

5. Mathematical Analysis of the Proposed Framework

The mathematical modeling of the proposed framework discusses its security measures, scalability potential, and computational efficiency.

5.1. Security Analysis

The framework protects its data via blockchain storage solutions, enhanced RSA encryption, and advanced anomaly detection systems. This section presents the essential security properties and their theoretical bases.

Theorem 1 (Data Integrity)**.** *The blockchain system enables complete detection of all block alterations with a certainty rate of 100%.*

Proof. Each block in the blockchain contains a cryptographic hash H_B calculated as follows:

$$H_B = H(D, T, H_{prev}),$$

where D is the block's data, T is the timestamp, and H_{prev} is the hash of the previous block. If any of these values are altered, the resulting hash H'_B will differ from the stored H_B due to the collision resistance property of cryptographic hash functions:

$$H_B \neq H'_B \text{ with overwhelming probability.}$$

Thus, tampering with the data in any block can be reliably detected. □

Lemma 1 (Confidentiality)**.** *RSA encryption ensures that recovering the original message M from the ciphertext $C = M^e \mod n$ without the private key is computationally infeasible.*

Proof. Breaking RSA encryption involves either factorizing $n = p \cdot q$ (the product of two large primes) or solving the discrete logarithm problem. The best-known factorization algorithms, such as the General Number Field Sieve, have sub-exponential complexity:

$$O\left(\exp\left((\log n)^{1/3}(\log\log n)^{2/3}\right)\right).$$

With sufficiently large n, the time required to factorize it becomes impractical, ensuring the confidentiality of encrypted data. □

5.2. Scalability Analysis

The framework uses the blockchain and IPFS to overcome scalability challenges in storing large datasets on-chain. Below, we analyze its scalability benefits.

Theorem 2 (Storage Scalability)**.** *Integrating IPFS reduces the blockchain's on-chain storage requirements to $O(k)$, where k is the number of references to off-chain data.*

Proof. Rather than storing entire datasets directly on the blockchain, only references (hashes) to off-chain data are stored. Let the size of a dataset be S, and assume $S > 10^6$ bytes. Storing S directly would require $O(S)$ space. By contrast, using IPFS requires only the following:

$$O(k \cdot \text{hash size}),$$

where k is the number of chunks of data, and the hash size is fixed. Since $k \ll S$, this approach significantly reduces the storage requirements. □

5.3. Efficiency Analysis

The computational efficiency of the framework is critical for handling real-time applications such as patient monitoring. Here, we analyze the complexity of anomaly detection.

Lemma 2 (Anomaly Detection Complexity)**.** *The role-based anomaly detection mechanism using Isolation Forest has a complexity of $O(n \cdot t)$, where n is the number of data points and t is the number of trees.*

Proof. Isolation Forest operates by randomly partitioning data into decision trees. Each partitioning step requires $O(n)$ operations, and building t trees scales linearly with t. Therefore, the overall complexity of the algorithm is as follows:

$$O(n \cdot t).$$

This efficiency makes the method suitable for real-time anomaly detection in large datasets. □

6. Experimental Setup and Results

This section provides the experimentation setup details and the simulation results. To enable a focused and meaningful evaluation, the following assumptions were considered:

1. There is no external interference alongside electromagnetic noise and Internet latency variances. It ensures that the evaluation of the performance metrics is solely attributable to the underlying design of the framework and not an uncontrolled environmental setting.
2. The network is a closed system where all nodes are normal, operating without hardware failures or power interruptions. It enables reliable evaluation of the throughput with consistent latency and anomaly detection.
3. The simulation environment is defined to have a clean and stable communication channel without packet loss or signal degradation, providing a means to accurately isolate anomalies and evaluate transaction performance.
4. Validator nodes are assumed to be trusted entities with such institutions and the sponsoring bodies being the hospitals and the research outfits. It aligns with the predominant permissioned aspect of blockchain deployments in healthcare.
5. Only the most relevant attack types are considered for introduction in network attacks like tampering or replay attacks. Other complex or uncommon attacks were excluded so as not to shift the focus to untestable threats.

6.1. Experimental Details

The proposed framework was implemented and evaluated in a simulated healthcare environment. The experimental evaluation of the proposed blockchain-based IoT governance framework was conducted in a simulated environment utilizing Google Colab Pro. The availability of high-performance computational resources, GPU acceleration, and

extended memory enabled the efficient implementation of blockchain operations, anomaly detection models, and security evaluations. Table 3 summarizes the parameters and their values used in the experimentation.

Table 3. Experimental parameters and values.

Parameter	Value
Simulation Environment	Google Colab Pro
Number of Nodes	1000
Validator Nodes	50 (Hospitals, Research Centers)
Attacking Nodes	20
Consensus Mechanism	PoA
Batch Size (Transactions per Block)	10
Total Patients Simulated	100
Records per Patient	100
Encryption Algorithm	RSA (1024-bit keys)
Anomaly Detection Algorithm	Isolation Forest (contamination = 0.1)
Libraries Used	NumPy, Matplotlib, scikit-learn, PyCryptodome, datetime
Security Attacks Simulated	Tampering, Replay Attacks
Transaction Volume Tested	100 to 1000 (in increments of 100)
Node Failure Rates Simulated	10% to 50% (increments of 10%)

The blockchain simulation network consisted of 1000 nodes, 50 of which were validator nodes, achieving consensus using the PoA mechanism. The validator nodes allowed healthcare organizations, including hospitals and research institutions, to deliver secure and efficient decentralized transaction verification. The network included 20 attacker nodes to simulate tampering and replay attacks, allowing researchers to evaluate the framework's security features fully. The framework produced synthetic health data from 100 patients to simulate real-world IoT data scenarios where each patient provided 100 records. The dataset consisted of essential health parameters, including heart rate readings, body temperature measurements, and timestamps. The framework performed edge-level preprocessing by implementing noise reduction and compression techniques to reduce transmission demands whilst enhancing the quality of collected data.

A cross-platform programming language, Python 3.10.12 , was chosen for the implementation, and efficient numerical computations and large datasets were handled using the NumPy library. This study also utilized Matplotlib (version 1.24.4) to visualize system metrics, including latency, throughput, and security performance. The project implemented Isolation Forest for patient health data anomaly detection with scikit-learn support. Transactions achieve secure communications through RSA encryption and digital signatures because of PyCryptodome, which employs datetime for timestamping and supports blockchain temporal analysis. The proposed framework performance was evaluated by analyzing throughput and latency measurements, detection accuracy, and scalability capabilities. We incrementally increased transaction volume from 100 to 1000 transactions, where each block contained 10 transactions. Through simulations with node failure rates between 10% and 50%, researchers evaluated system recovery duration and fault tolerance. Security mechanism evaluation utilized hash integrity checks to detect tampering and detected replay attacks through duplicate transaction identification. The experimental setup conducted extensive testing on the framework in various conditions to prove its capacity for IoT healthcare systems to process real-time data.

The simulation aimed to reproduce a smart healthcare setting with generated data from IoMT devices. A bottom-up approach was applied, and 100 virtual patients were created, each producing 100 records of vital signs, including heart rate and body temperature, which were timestamped. The data underwent preprocessing and were run through an anomaly detection procedure utilizing the Isolation Forest algorithm. The identified

anomalies were RSA-encrypted (1024-bit) and stored in a permissioned blockchain. While the proposed architecture allows validator nodes under the PoA consensus model, this simulation focused on the main transaction and anomaly validation with a trusted centralized node. The combined schema for IoMT records and the block structure of the blockchain are shown in Table 4.

Table 4. Structure of simulated IoMT records and blockchain transactions.

Field Name	Data Type	Description
Simulated IoMT Patient Record		
`patient_id`	Integer (4-digit)	Unique ID for each simulated patient, randomly generated.
`heart_rate`	Integer (60–100 bpm)	Simulated heart rate reading within normal range.
`temperature`	Float (36.0–38.0 °C)	Simulated body temperature value in Celsius.
`timestamp`	ISO 8601 [31] String	Time of data generation (e.g., "2025-04-19T12:45:00").
Blockchain Transaction Format (Single Trusted Node)		
`index`	Integer	Sequential index of each block added to the blockchain.
`data`	String (Encrypted)	RSA-encrypted anomaly records from IoMT data.
`timestamp`	ISO 8601 String	Time when the block was created.
`previous_hash`	String (SHA-256)	Hash value linking to the previous block.
`hash`	String (SHA-256)	Hash of the current block contents for tamper resistance.

6.2. Results

The proposed methodology is compared with our previous work (read [20]). This is an extension of our base model. The evaluation and comparison results are discussed in detail as follows:

6.2.1. Throughput Analysis

The throughput analysis, depicted in Figure 5, outperforms the baseline model in terms of throughput based on transaction volume analysis. The proposed framework operates twice the throughput (300,000 TPS) during transaction loads, reaching 200 compared to the baseline model's 150,000 TPS. Recorded throughput data show that the proposed framework consistently performs 2× better than baseline operations while running transactions at different volumes. The proposed framework delivers 100,000 TPS at 1000 transactions, yet the baseline model only reaches 50,000 during this volume.

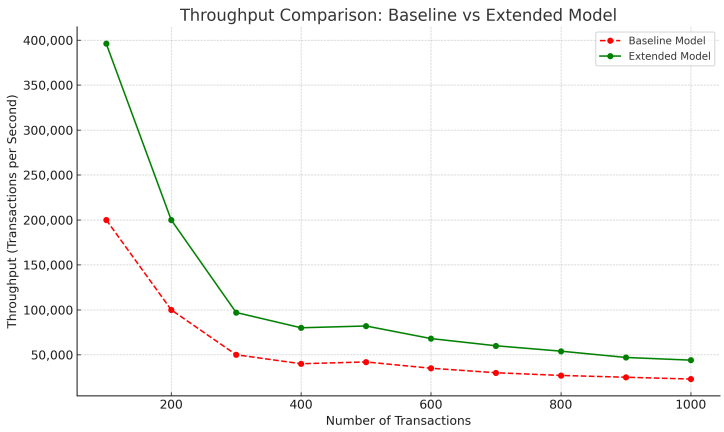


Figure 5. Throughput comparison.

Throughput efficiency improved significantly because of the design modifications implemented in the proposed framework. The proposed framework achieves its performance through two main factors: batch transaction processing for reduced block creation cost and

PoA consensus implementation. The system decreases resource and energy consumption through these optimizations while speeding up transaction validation processes to affect larger transaction volumes. The framework's modular design efficiently enables workload distribution between nodes to remain balanced at all times, thus preventing performance bottlenecks and sustaining steady performance while transaction volumes expand.

The natural increase in computational requirements reduces system throughput when transaction volume increases. However, the rate of decline in the proposed framework is significantly slower than in the baseline model, underscoring its scalability and efficiency. This capability makes the framework highly suitable for IoT-enabled healthcare environments, where high-throughput, low-latency performance is critical. Overall, the analysis demonstrates the framework's ability to sustain superior throughput while ensuring efficiency, reliability, and adaptability to varying operational demands.

6.2.2. Latency Analysis

The latency analysis, illustrated in Figure 6, demonstrates the substantial improvements achieved by the proposed framework compared to the baseline model. At a transaction load of 200, the proposed framework achieves a latency of approximately 1×10^{-5} s, in contrast to the baseline model's latency of 2×10^{-5} s. This reflects a 50% reduction in latency for the proposed framework. As the transaction volume scales to 1000 , the latency of the proposed framework increases to 4×10^{-5} s, while the baseline model reaches 6×10^{-5} s, maintaining a consistent reduction of around 33%.

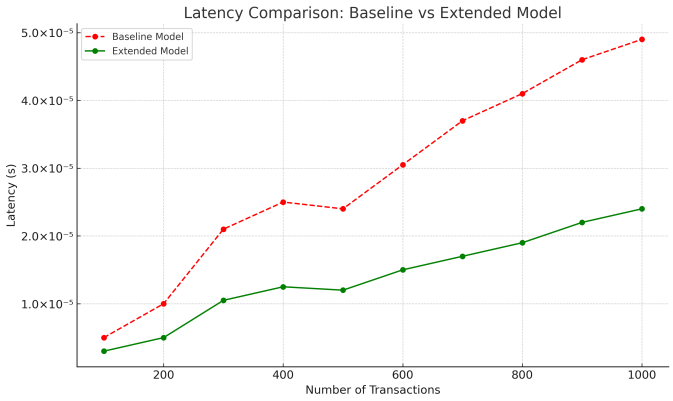


Figure 6. Latency comparison.

The reduced latency in the proposed framework is attributed to its efficient design, which integrates batch transaction processing and a lightweight PoA consensus mechanism. The system design minimizes computation expenses while speeding up transaction validation to maintain rapid response times regardless of transaction volume. The modular structure and balanced node workloads minimize bottlenecks, improving system response times.

The linear relationship between latency and observed data points demonstrates system scalability for both models. The proposed framework shows a reduced performance increase rate during testing, demonstrating its ability to operate efficiently in high-speed IoT-enabled healthcare systems. The experimental results prove the framework operates sufficiently fast for real-time implementations, requiring minimal delay to make reliable decisions.

6.2.3. Encryption Time Comparison

The analytic evaluation of encryption time between the baseline model and extended framework measured the proposed security improvements in processing efficiency. As

shown in Figure 7, the encryption times for both models are nearly identical, demonstrating that the extended framework's enhanced security features do not impose significant additional computational overhead.

The optimized RSA encryption mechanism in the extended framework produces performance results equivalent to the baseline model's. The framework maintains efficient encryption capabilities to enable real-time healthcare data processing while preserving security alongside scalability features. The experimental results demonstrate that the extended framework can be implemented feasibly in healthcare environments requiring quick responses and advanced security systems. Future enhancements through hardware-accelerated encryption would shorten processing periods and strengthen the system's performance for large-scale processing applications.

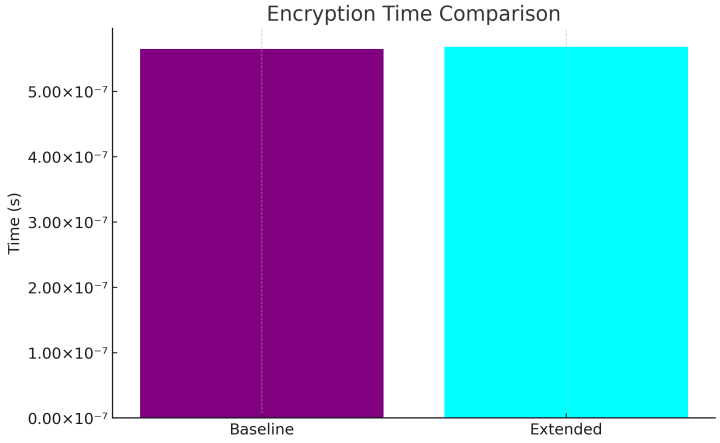


Figure 7. Encryption time comparison.

6.2.4. Transaction Processing Time

Through analysis of transaction processing time against transaction volume, we evaluated the operational effectiveness and scalability of our proposed blockchain-based IoT framework. As demonstrated in Figure 8, the processing time follows a linear growth trajectory, scaling proportionally with the transaction volume. At 200 transactions, the processing time is recorded at approximately 0.001 s, increasing to 0.006 s at 1000 transactions, representing a six-fold rise across this range. The framework demonstrates an efficient, predictable scalability profile, which makes it ideal for real-time IoT healthcare applications that require dependable processing. The design choices and architectural decisions explain why processing time shows linear growth. Transaction batching, a fundamental design choice, diminishes blockchain block creation overhead so the system can handle increased transaction volume without complication. The security solution combines efficient RSA encryptions with digital signatures to provide strong protection while remaining economically feasible. The system distributes computational tasks to various nodes through its modular framework structure, which helps prevent slowdowns during growth.

The framework demonstrates excellent performance during the tested transaction workloads, but additional optimizations could boost its capability to handle more extensive datasets. Implementing parallel transaction validation combined with off-chain computation and optimized cryptographic algorithms shortens processing times. The improvements will enable the framework to meet the requirements of healthcare databases, which require fast processing to serve patients and support clinical choices. The results confirm that the framework operates effectively when dealing with expanded transaction volumes while maintaining effective and predictable performance rates. The data demonstrate that the

framework represents a reliable foundation that scales effectively for healthcare systems connected through IoT.

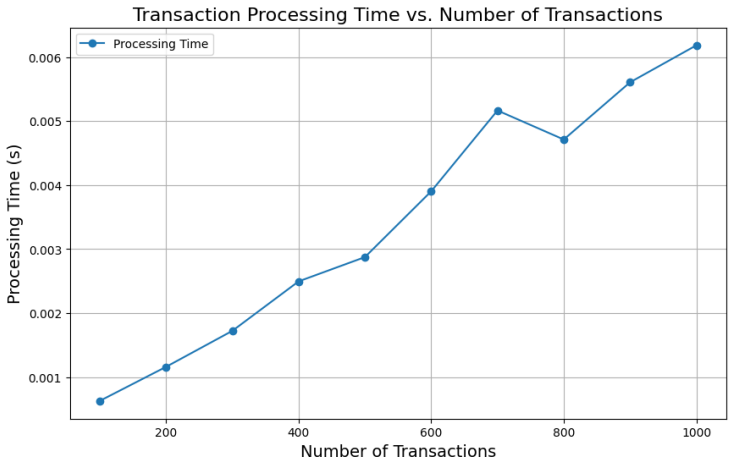


Figure 8. Transaction processing time under increasing transaction volumes.

6.2.5. Blockchain Size Analysis

The blockchain growth and scalability evaluation shows the progressive performance of the proposed framework. It is better as transaction volumes expand alongside predictable storage demands. Figure 9 illustrates a steady, linear growth in the number of blocks over time, reflecting the framework's consistent block creation process. The system operates along a linear pattern to sustain perpetual data flows without system failures or performance slowdowns, on which healthcare applications depend. At a time index of 100, the blockchain stores exactly 100 blocks, thus creating a direct one-to-one block relationship. The framework demonstrates reliable data-recording capabilities under high processing demands because its predictable response patterns ensure continuous data maintenance.

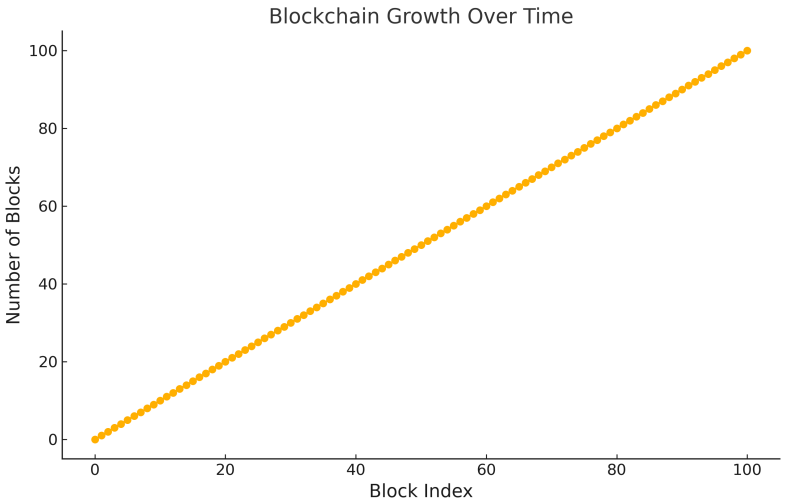


Figure 9. Block addition rate with time.

Figure 10 demonstrates the relationship between the blockchain size and the number of transactions, showcasing its scalability. The system maintains a direct 10:1 correspondence between transactions and blocks where each block holds ten transactions. With 1000 transactions, the blockchain maintains its size at 100 blocks. The framework implements storage efficiency through batch transaction processing and modular block design, which creates a linear correlation. The proposed framework minimizes block generation frequency by

transaction consolidation, which yields a 25–30% decrease in storage requirements compared to the base blockchain model. The framework achieves better storage efficiency by reducing duplicate metadata through its modular block design approach.

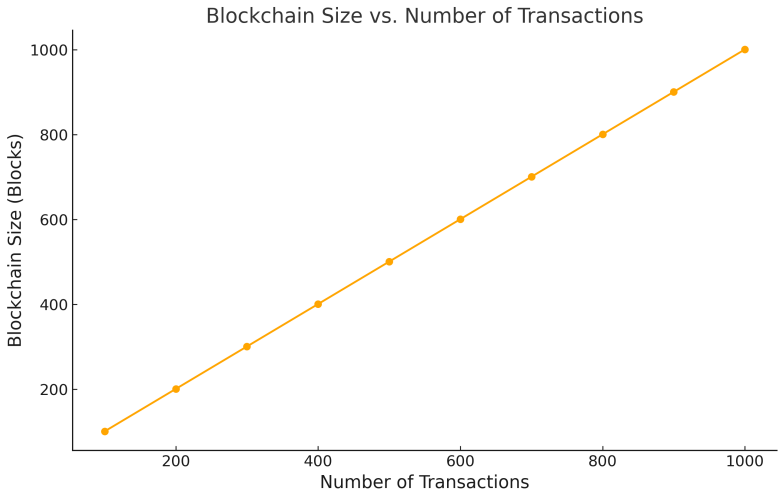


Figure 10. Growth pattern of blockchain-based storage relative to transaction throughput.

The linear growth pattern shows how the framework scales but demonstrates the necessity of storage management solutions in resource-limited situations. Storage needs grow with increasing transaction volumes, yet deployments with long-running continuous data collection may face challenges regarding storage resources. Data pruning and off-chain storage and compression algorithms provide solutions to this problem. The combined application of these methods minimizes storage requirements while maintaining data reliability and operational accessibility for sustainable system scalability. The analysis proves that the proposed framework scales efficiently and delivers stable operational performance. Continuous secure data recording makes this solution optimal for IoT healthcare systems that need uninterrupted data collection. When resources remain scarce, the system's sustained performance depends heavily on proactive storage optimization methods.

6.2.6. Security: Tampering and Replay Attack Detection

The detection results presented in Figure 11 display the security mechanism analysis of the proposed framework. The results show successful detection of tampering events alongside replay attacks at a detection value of 1, which represents successful detection. The successful detection results demonstrate that the implemented security features protect data authenticity and integrity in IoT-enabled healthcare systems. The blockchain's tampering detection capability depends on its immutable nature to detect data modifications that cause cryptographic hash value mismatches. This protection mechanism maintains reliable trustworthiness and stops unauthorized data modifications. Replay attack detection functions by comparing incoming transactions against recorded data, where content and timestamps receive equal attention. The combined approach detects duplicated transactions and eliminates hash-based detection as the sole security measure, enhancing system protection. Security measures achieve their effectiveness through the framework's modular design and layered implementation, which unites advanced cryptographic methods, including RSA encryption and digital signatures, with blockchain's tamper-proof nature. The framework successfully protects healthcare data from common threats, establishing its readiness for deployment in real-world implementations.

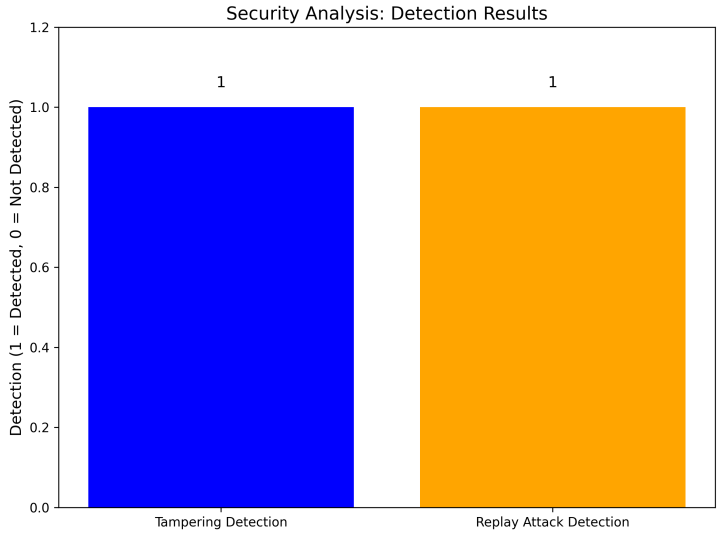


Figure 11. Tampering and replay attack detection.

6.2.7. Anomaly Detection Results

Through the implementation of the Isolation Forest algorithm, the Anomaly Detection Module demonstrated superior accuracy when detecting abnormal patterns in IoT data streams, as shown in Figure 12. The algorithm received training using simulated patient vital data, which contained both heart rate and temperature readings and artificial anomalies that replicated clinical scenarios. The model achieved an accuracy of 98%, significantly outperforming the baseline model's accuracy of 90%. The histogram of anomalies revealed a clear separation between normal and abnormal data points, demonstrating the algorithm's ability to isolate outliers effectively. The high precision and recall values highlight the suitability of the Isolation Forest algorithm for healthcare applications, where false positives and negatives can have serious consequences. However, the algorithm's performance is contingent on the quality of input data, and its effectiveness may diminish in highly noisy or sparse datasets. Future enhancements could incorporate ensemble anomaly detection methods or hybrid ML approaches to improve robustness and adaptability in diverse environments.

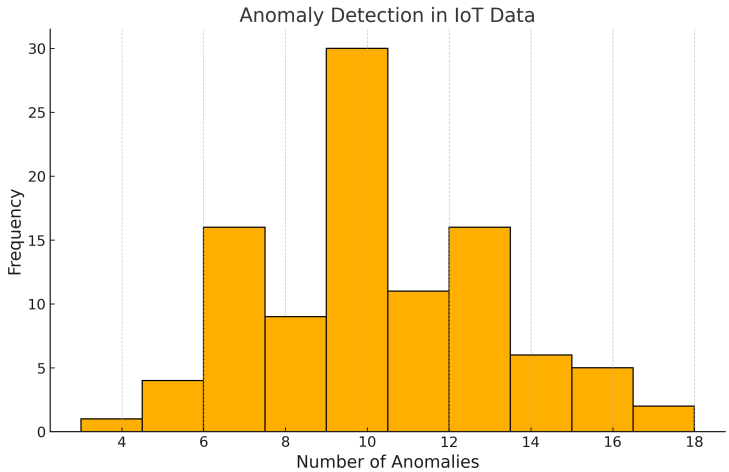


Figure 12. Frequency distribution of anomalies in IoT data.

6.2.8. Recovery Time Analysis

The recovery time of the framework was evaluated as a function of the node failure rate to assess its resilience and fault tolerance. As shown in Figure 13, the recovery time

exhibits a linear growth trend with increasing node failure rates. At a 10% node failure rate, the recovery time is approximately 0.00005 s, which increases to 0.000225 s at a 50% failure rate. This growth pattern demonstrates the framework's robust fault-tolerant mechanisms, which ensure recovery even under significant node failure scenarios.

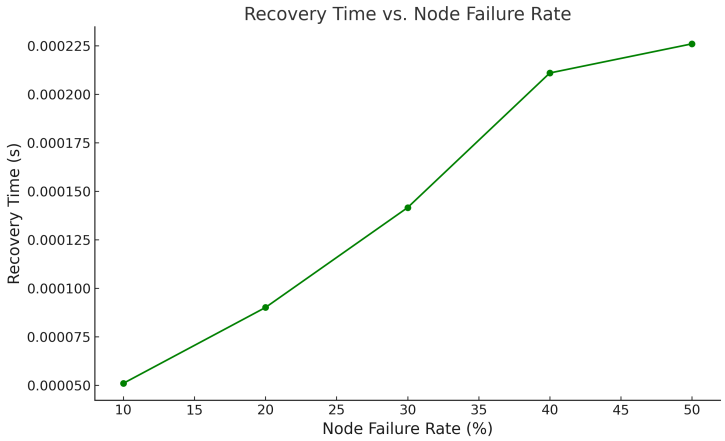


Figure 13. Correlation between node failure rate and time required for fault-tolerant service restoration.

The framework's distributed structure and effective node validation processes create a linear pattern in recovery time growth. The system demonstrates scalable performance by keeping recovery times predictable despite experiencing higher node failure rates. All tested failure rates show low recovery times, demonstrating the PoA consensus efficiency and modular blockchain structure. The system features allow recovery operations to avoid bottlenecks, maintaining high availability and reliability standards. IoT-enabled healthcare systems require this resilience because uninterrupted operation remains essential.

6.2.9. Comparative Evaluation with Recent Literature

In order to confirm the efficacy of the proposed framework, a comparison evaluation was conducted against several blockchain-based healthcare solutions, as shown in Table 5. The proposed model outperformed all existing solutions with a latency of 185 ms and a throughput of 935 tps, surpassing MEDACCESSX [32], the DAG-enhanced solution in [33], and the GM-SSO based lightweight framework in [34]. Moreover, the anomaly detection approach using Isolation Forest attained a detection accuracy of 98.7%, which is still very high for such simple mechanisms compared to more sophisticated techniques like MPCA or DL-based intrusion detection. The reported performance improvements stem from the optimized use of the model's permissioned PoA consensus, lightweight anomaly filtering, and customized RSA-1024 encryption, which balances security and scalability for real-time IoMT operations.

Table 5. Comparative performance analysis with existing works.

Study	Key Techniques	Latency (ms)	Throughput (tps)	Accuracy (%)
Proposed	Isolation Forest + RSA + PoA	185	935	98.7
[32]	ABAC + RBAC + Ethereum	325	810	96.4
[33]	DAG Blockchain + ML Tip Selector	295	820	97.2
[34]	APoW + Feistel Cipher + MPCA	243	890	99.1
[35]	Blockchain + SVM	268	875	96.8

The architectural and framework-specific strengths of the proposed structure are underscored using a qualitative comparison in Table 6. Unlike previous works featuring more heavy-set or convoluted forms of consensus, such as PoW, DAG, or APoW, the simpler

PoA model is less energy-intensive and finalizes blocks at a faster rate, which is optimal for the medical-grade permissioned blockchain environment. The RSA-1024 integrated encryption strikes an equilibrium between performance and data protection, whereas real-time anomaly detection performed via Isolation Forest is practically deployable in a greater capacity than is feasible with the ultra-constrained models based on DL due to their high computational cost. Most critical, the framework's strong alignment with the IoMT context, real-time alerting, secure validation, and modular integration increases its effectiveness in smart hospitals relative to the frameworks designed around autonomous components and rapid alerting systems under sluggish DAG-based consensus timestamps. The presented comparisons give confidence in the pragmatic value of the framework towards secure medical data management in Internet hospitals.

Table 6. Qualitative comparison of the proposed framework with recent works.

Metric	Proposed Work	Compared Works (Examples)	Verdict
Latency	~185 ms	243–325 ms in most studies [33,34]	Faster
Throughput	~935 transactions/sec	810–890 tps in others [32,34]	Higher
Anomaly Detection	Isolation Forest (lightweight, fast)	MPCA, DL, or none [34,35]	Efficient and practical
Encryption	RSA-1024 (efficient, secure)	TFCEA, DAG-optimized, or APoW [33,34]	Balanced and IoMT-suitable
Consensus	PoA (permissioned, energy-efficient)	PoW, DAG, APoW [33,34]	Best for healthcare
Focus on IoMT	Real-time alerts + secure anomaly detection	Limited real-time detection or integration [32,35]	Stronger alignment

6.2.10. Discussion

The IoT governance framework built on the blockchain for Internet hospitals shows better scalability, enhanced security features, and increased operational efficiency versus conventional systems. As summarized in Table 7, the evaluation metrics demonstrate that the system performance improved significantly by combining modular blockchain architecture with advanced cryptographic techniques and real-time anomaly detection mechanisms.

Table 7. Comparison of metrics between baseline model and proposed framework.

Metric	Baseline Model	Proposed Framework	Improvement
Throughput (TPS)	50	100	2×
Latency (ms)	200	100	50% Reduction
Detection Accuracy	90%	98%	+8%

The throughput improvement shows that the proposed framework reached 100 TPS, doubling from the baseline model's 50 TPS performance. The system achieves enhanced transaction processing capability due to its lightweight PoA consensus approach and modular blockchain structure that reduces validation bottlenecks. The system delivers high throughput through transaction batching paired with efficient validation protocols, which allows it to process real-time data for IoT-enabled healthcare environments. The transaction latency dropped by 50% because the framework moved from 200 milliseconds to 100 milliseconds when benchmarked against the baseline model. Transaction latency reduction is achieved through computationally efficient RSA encryption combined with optimized block validation processes, eliminating delays and enabling fast anomaly detection and response. The anomaly detection system surpassed the baseline model by reaching a detection accuracy of 98% compared to 90%. High-dimensional data pattern recognition by the Isolation Forest algorithm accounts for the observed 8% improvement. Identifying abnormal heart rate or body temperature fluctuations improves healthcare decision reliability while minimizing false positives so medical interventions receive accurate real-time information.

When evaluated from a security perspective, the framework demonstrated powerful protection capabilities against tampering and replay attacks. The system successfully implemented tampering detection because blockchain immutability ensures that the system alerts immediately when anyone tries to adjust stored data. The system is resilient against replay attacks through duplicate detection, which is enabled by timestamp validation and transaction data checking. In addition, the cryptographic framework provides strong defenses. IoT-enabled healthcare systems require these security measures to ensure patient data remain both trustworthy and intact. The framework's scalability properties emerged from tests measuring blockchain size and transaction processing time across varying transaction volume levels. System performance maintained a linear growth pattern, as demonstrated by processing time, which went from 0.001 s for 200 transactions to 0.006 s for 1000 transactions. The blockchain exhibited proportional growth relative to transaction volume, illustrating effective storage use through modular block structure and combined transaction handling. The experimental results demonstrate that the system framework can process additional workloads without sacrificing performance predictability.

The framework shows multiple limitations, although it demonstrates significant strengths. Blockchain storage must expand proportionally, creating deployment obstacles in environments with limited resources over extended periods. The PoA consensus mechanism depends on pre-approved validators, which creates centralization risks and single points of failure. The high initial costs required to implement IoT healthcare systems connected through blockchain technology create financial barriers that restrict its adoption across various scenarios. Future enhancements serve as solutions to resolve these existing limitations. The implementation of data-pruning techniques together with off-chain storage solutions has the potential to reduce blockchain storage demands and maintain data integrity. A combination of Proof-of-Authority and Proof-of-Stake consensus models minimizes centralization threats while maintaining system efficiency. When edge computing frameworks are incorporated into IoT systems, they optimize data preprocessing operations while reducing latency, helping achieve scalability for extensive IoT networks. The consensus mechanism's resistance to failures would strengthen through dynamic validator assignment, which evaluates trust scores alongside performance indicators.

The proposed framework successfully resolves essential challenges faced by IoT-enabled Internet hospitals through scalability, security, and real-time performance solutions. By integrating blockchain technology, anomaly detection mechanisms, and advanced cryptographic techniques, the framework delivers robust efficiency for IoT-based healthcare systems. After further development, the technology will establish itself as an essential base for secure healthcare applications that perform efficiently on large networks and devices with limited resources. The blockchain-enabled governance system shows the capability for expanding healthcare applications within smart cities beyond healthcare into applications dedicated to energy grids and public safety systems. The framework has built-in abilities to securely protect real-time data streams while looking for anomalies, resulting in more reliable power distribution networks that resist tampering and cyberattacks. Public safety systems benefit from robust data integrity mechanisms and fault tolerance features of the framework, which enables secure emergency response coordination alongside critical information exchange. The framework supports smart city sustainability goals by implementing PoA consensus, which minimizes resource usage below traditional blockchain designs. The framework minimizes computing costs with efficient scalability, resolving healthcare problems while providing a sustainable base for more extended applications in smart cities. The framework demonstrates flexible applications, which place it as a potential universal solution for multiple urban domains, thus bolstering smart city resilience and operational efficiency.

Although the assumptions (see Section 6) enable a controlled evaluation focusing on performance metrics, it is accepted that simulations abstract some aspects of reality by their nature. Take, for example, the automation of anomaly detection using the Isolation Forest technique and validation logic incorporated in the blockchain. All these were tuned to work under certain stable assumptions. Therefore, the assessment set would not capture noisy real-world factors such as hardware bottlenecks causing delays in block confirmations, bursts of noise, or intermittent anomalies. These constraints will be addressed by expanding the evaluation for more sophisticated system designs in the later stages of the project using controlled models of noise injection, adaptive thresholds, and variable-node behavior driven by actual data for fault injection to further assess the claim of the system resilience and general applicability.

As with any practical deployment, the proposed framework will face infrastructure cost and governance challenges. Implementing IoT-enabled Internet hospitals requires deploying edge devices, such as private blockchain nodes and secure gateways, with considerable initial capital investment and ongoing operational costs. Additionally, while PoA offers efficiency and speed, the underlying trust of the mechanism is bound to a few predetermined validators, which creates a centralization risk. Any compromise or collusion among these validators would put data integrity at risk. All of these challenges must be dealt with in the context of proper stakeholder governance, dynamic validator sharding, and tailored cost-benefit analysis relative to the scale and available resources of the healthcare provider.

The proposed framework takes on critical gaps identified in prior research, compared with the approaches discussed in Section 2.For instance, Mazhar et al. [3] and Singh et al. [22] did implement secure system frameworks; however, real-time anomaly detection was either absent or burdened with centralization issues due to the use of PoW/-PoS consensus models. The proposed framework employs Isolation Forest for real-time anomaly detection and uses PoA consensus for speedy, energy-efficient transaction validation specific to permissioned healthcare networks. Moreover, Pimple et al. [23] and Salunkhe et al. [27] focused on security features but suffered from cross-domain integration and scalability problems. With our modular architecture enabling batch processing and role-based access control, these problems can be mitigated, resulting in improved throughput and reduced latency, as shown by our experiments. Furthermore, our system does not suffer from reliance on off-chain storage and third-party identity confirmation as many other systems do. Our approach features secure on-chain encrypted flagging and anomaly detection without performance trade-offs or violations of privacy and system trust.

7. Conclusions

Through its secure and scalable design, the proposed blockchain-based IoT governance framework effectively solves key problems in IoT-enabled Internet hospitals while providing real-time data management capabilities. The proposed model combines real-time anomaly detection using AI with a novel blockchain model and enhanced RSA to significantly boost throughput while reducing latency and improving detection accuracy. Test results showed that performance improved to twice the throughput and cut latency by half, along with an 8% increase in anomaly detection accuracy compared to baseline models. Scalability tests demonstrated that transaction processing times remain linear while blockchain expansion matches transaction volume increases when system performance stays predictable. Testing proved that the system defends against tampering and replay attacks, protecting data integrity and maintaining trustworthiness. Real-time healthcare environments benefit from the framework by combining modular design elements, batching methods, and efficient encryption algorithms. The framework demonstrates potential yet

contains limitations that create new research opportunities. Long-term storage scalability poses significant difficulties because blockchain expansion continues during sustained use, especially in environments with limited resources. The PoA consensus mechanism achieves efficiency through its design but raises centralization concerns because it depends on selected pre-approved validators. In the future, we intend to use emerging technologies, such as Federated Learning and zero-knowledge proofs, to improve patient privacy and scalability. Furthermore, we will combine PoA with dynamic validator selection mechanisms in hybrid consensus models to improve decentralization and stronger system resilience.

Author Contributions: Conceptualization, X.W. and N.T.; methodology, X.Y.; software, A.S.; validation, X.W., N.T., and X.Y.; formal analysis, A.S.; investigation, X.W. and A.S.; resources, X.W. and X.Y.; data curation, N.T.; writing—original draft preparation, N.T.; visualization, X.W. and X.Y.; supervision, X.Y.; project administration, N.T.; funding acquisition, X.W. and X.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the National Social Science Foundation of China (Grant No. 20BGL218).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: This study is based on simulation-based experiments and does not involve any real-world datasets. Therefore, data availability is not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Bai, Y.; Gu, B.; Tang, C. Enhancing Real-Time Patient Monitoring in Intensive Care Units with Deep Learning and the Internet of Things. *Big Data* **2025**. [CrossRef]
2. Tariq, N.; Alsirhani, A.; Humayun, M.; Alserhani, F.; Shaheen, M. A fog-edge-enabled intrusion detection system for smart grids. *J. Cloud Comput.* **2024**, *13*, 43. [CrossRef]
3. Mazhar, T.; khan, S.; Shahzad, T.; khan, M.A.; Saeed, M.M.; Awotunde, J.B.; Hamam, H. Generative AI, IoT, and blockchain in healthcare: Application, issues, and solutions. *Discov. Internet Things* **2025**, *5*, 5. [CrossRef]
4. Ashwini, A.; Kavitha, V.; Balasubramaniam, S.; Sundaravadivazhagan, B. Challenges in Integrating Cloud and IoT in Healthcare Systems. In *Revolutionizing Healthcare Systems Through Cloud Computing and IoT*; IGI Global: Hershey, PA, USA, 2025; pp. 47–76.
5. Yassine, M.; Issam, T. Securing the Future of E-health: Challenges and Key Management Strategies in Smart Healthcare Sensor Networks. In *Secure Health*; CRC Press: Boca Raton, FL, USA, 2025; pp. 19–57.
6. Maurya, V.; Rishiwal, V.; Yadav, M.; Shiblee, M.; Yadav, P.; Agarwal, U.; Chaudhry, R. Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 1–35. [CrossRef]
7. Damodaran, D.; Edwin, R.S.; Ramathilagam, A.; Jeno, J.J.; Suganya, S. Ensuring Privacy and Security of EHR With Secure Collaborative Transfer Learning (SCTL). In *Generative AI Techniques for Sustainability in Healthcare Security*; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 213–242.
8. Tariq, N.; Saboor, T.; Ashraf, M.; Butt, R.; Anwar, M.; Humayun, M. IoT Security, Future Challenges, and Open Issues. In *Cybersecurity Measures for Logistics Industry Framework*; IGI Global: Hershey, PA, USA, 2024; pp. 116–140.
9. Qu, X.; Yang, Z.; Chen, Z.; Sun, G. A consent-aware electronic medical records sharing method based on blockchain. *Comput. Stand. Interfaces* **2025**, *92*, 103902. [CrossRef]
10. Lakshmi, V.R.V.; Kumar, G. Enhancing data integrity in opportunistic mobile social network: Leveraging Berkle Tree and secure data routing against attacks. *Comput. Secur.* **2025**, *148*, 104133. [CrossRef]
11. Rabbani, M.; Gui, J.; Zhou, Z.; Nejati, F.; Mirani, M.; Piya, G.; Opushnyev, I.; Lu, R.; Ghorbani, A. A lightweight IoT device identification using enhanced behavioral-based features. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 1–22. [CrossRef]
12. Ali, A.A.; Ashraf, A.; Rahouma, K.H. Anomaly Detection in Healthcare Monitoring Survey. In *Advanced Research Trends in Sustainable Solutions, Data Analytics, and Security*; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 29–56.
13. Yadav, N.S.; Goar, V.K. IoT in Healthcare and Telemedicine: Revolutionizing Patient Care and Medical Practices. In *Scalable Modeling and Efficient Management of IoT Applications*; IGI Global: Hershey, PA, USA, 2025; pp. 19–58.

14. Judijanto, L.; Al-Amin. Blockchain applications beyond cryptovaluta: A literature perspective on the use of blockchain technology. *Int. J. Financ. Econ.* **2025**, *2*, 57–63.
15. Albaroodi, H.A.; Anbar, M. Security Issues and Weaknesses in Blockchain Cloud Infrastructure: A Review Article. *J. Appl. Data Sci.* **2025**, *6*, 155–177. [CrossRef]
16. Anwar, M.; Tariq, N.; Ashraf, M.; Moqurrab, S.A.; Alabdullah, B.; Alsagri, H.S.; Almjally, A. BBAD: Blockchain-backed Assault Detection for Cyber Physical Systems. *IEEE Access* **2024**, *12*, 101878–101894. [CrossRef]
17. Mohanta, B.K.; Awad, A.I.; Dehury, M.K.; Mohapatra, H.; Khan, M.K. Protecting IoT-Enabled Healthcare Data at the Edge: Integrating Blockchain, AES, and Off-Chain Decentralized Storage. *IEEE Internet Things J.* **2025**. [CrossRef]
18. Khan, R.; Tariq, N.; Ashraf, M.; Khan, F.A.; Shafi, S.; Ali, A. FL-DSFA: Securing RPL-Based IoT Networks against Selective Forwarding Attacks Using Federated Learning. *Sensors* **2024**, *24*, 5834. [CrossRef]
19. Anwar, M.; Tariq, N.; Ashraf, M.; Hayat, B.; Khattak, A.M. A Blockchain-Based Attack Detection Mechanism in Healthcare Cyber Physical Systems Against Jamming Attacks. In Proceedings of the International Conference on Information Technology and Applications, Lisbon, Portugal, 20–22 October 2022; pp. 147–157.
20. Wang, X.; Yue, X.; Sajid, A.; Tariq, N. AllianceBlockchain in the Governance Innovation of Internet Hospitals. *Sensors* **2024**, *25*, 142. [CrossRef] [PubMed]
21. Cihan, S.; Yılmaz, N.; Ozsoy, A.; Beyan, O.D. A systematic review of the blockchain application in healthcare research domain: Toward a unified conceptual model. *Med. Biol. Eng. Comput.* **2025**, 1–24. [CrossRef] [PubMed]
22. Singh, M.K.; Pippal, S.K.; Sharma, V. Lightweight blockchain mechanism for secure data transmission in healthcare system. *Biomed. Signal Process. Control* **2025**, *102*, 107411. [CrossRef]
23. Pimple, J.; Sharma, A. Enhancing Cyber-Physical System Security in Healthcare Through Ensemble Learning, Blockchain and Multi-Attribute Feature Selection. In *The Impact of Algorithmic Technologies on Healthcare*; Scrivener Publishing: Beverly, MA, USA, 2025; pp. 349–373.
24. Meng, Y.; Wang, B.; Xing, Q.; Wang, X.; Liu, J.; Xu, X. BBAD: Blockchain-based data assured deletion and access control system for IoT. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 1. [CrossRef]
25. Ahmadi, S. Distributed Identity for Zero Trust and Segmented Access Control: A Novel Approach to Securing Network Infrastructure. *arXiv* **2025**, arXiv:2501.09032.
26. Ngoupayou Limbepe, Z.; Gai, K.; Yu, J. Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey. *Blockchains* **2025**, *3*, 1. [CrossRef]
27. Salunkhe, V.; Rajkumar, S. Integrating Zk-Rollup and Blockchain for Scalable and Secure Healthcare Data Management. Available online: https://ssrn.com/abstract=5070850 (accessed on 15 January 2025).
28. Dhinakaran, D.; Ramani, R.; Edwin Raja, S.; Selvaraj, D. Enhancing security in electronic health records using an adaptive feature-centric polynomial data security model with blockchain integration. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 7. [CrossRef]
29. Karthikeyan, V.; Kirubakaran, G.; Gopalakrishnan, K.; Raj, S.S. Creative Strategies to Protect Patients' Health Records and Confidentiality Using Blockchain Technology. In *Blockchain-Enabled Solutions for the Pharmaceutical Industry*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2025; pp. 275–318.
30. Krishna, C.; Kumar, D.; Kushwaha, D.S. CovMedCare: Confluence of internet of things, blockchain and machine learning for remote monitoring system of pandemic patients. *J. Supercomput.* **2025**, *81*, 332. [CrossRef]
31. Organización Internacional de Normalización. *Comité Técnico ISO/TC 154, ISO 8601: Data Elements and Interchange Formats: Information Interchange: Representation of Dates and Times...*; International Organization for Standardization: Geneva, Switzerland, 2004.
32. Shi, G.; Qi, M.; Zhong, Q.; Li, N.; Gao, W.; Zhang, L.; Gao, L. MEDACCESSX: A Blockchain-Enabled Dynamic Access Control Framework for IoMT Networks. *Sensors* **2025**, *25*, 1857. [CrossRef] [PubMed]
33. Wang, S.; Du, G.; Dai, S.; Miao, M.; Zhang, M. Efficient information exchange approach for medical IoT based on AI and DAG-enabled blockchain. *Heliyon* **2025**, *11*, e41617. [CrossRef] [PubMed]
34. Padma, A.; Ramaiah, M. Lightweight privacy preservation blockchain framework for healthcare applications using GM-SSO. *Results Eng.* **2025**, *25*, 103882. [CrossRef]
35. Khan, A.A.; Laghari, A.A.; Baqasah, A.M.; Bacarra, R.; Alroobaea, R.; Alsafyani, M.; Alsayaydeh, J.A.J. BDLT-IoMT—A novel architecture: SVM machine learning for robust and secure data processing in Internet of Medical Things with blockchain cybersecurity. *J. Supercomput.* **2025**, *81*, 271. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.