10.48047/jocaaa.2024.33.08.456

A BLOCKCHAIN-ENABLED TRUST AND PRIVACY FRAMEWORK WITH DECENTRALIZED CONSENT MANAGEMENT FOR IOT-BASED HEALTHCARE SYSTEMS

Rimjhim Choudhary[1], Abhay Shukla[2], Somendra Tripathi[3]
Department of Computer Science and Engineering, Faculty of Engineering and Technology, Rama University, Mandhana, Kanpur, Uttar Pradesh 209217, India
Corresponding author email: rimjhimchoudhary490@gmail.com

Abstract

The integration of Internet of Things (IoT) technologies into modern healthcare systems has enabled continuous patient monitoring, real-time diagnostics, and improved clinical responsiveness. However, the distributed and heterogeneous nature of IoT-based healthcare introduces critical challenges related to data privacy, trust management, and secure information exchange. Sensitive medical data travers's multiple devices, networks, and cloud platforms, increasing vulnerability to unauthorized access, data breaches, and misuse. This paper proposes a blockchain-enabled trust and privacy framework designed to address these challenges through decentralized trust management and dynamic consent enforcement. The framework leverages a permissioned blockchain to ensure immutable record keeping, transparent auditability, and secure validation of data transactions. Smart contracts are utilized to implement patient-centric and adaptive consent mechanisms, allowing fine-grained control over data access and sharing. The proposed architecture adopts a multi-layered design consisting of sensing, gateway, privacy, blockchain, cloud, and application layers, each contributing to end-to-end security. In addition, a behavior-driven dynamic trust model is introduced to continuously evaluate system entities and mitigate insider and external threats. Analytical evaluation demonstrates that the framework improves privacy preservation, trust adaptability, scalability, and regulatory compliance compared to traditional and existing blockchain-based healthcare systems. The study provides a scalable and secure foundation for next-generation digital healthcare ecosystems by integrating decentralized governance, adaptive trust, and automated access control.

Keywords: IoT Healthcare, Blockchain, Trust Management, Data Privacy, Smart Contracts, Consent Management.

1. Introduction

The rapid evolution of IoT technologies has significantly transformed the healthcare sector by enabling continuous patient monitoring, remote diagnostics, and proactive treatment strategies. Wearable sensors, smart medical devices, and interconnected healthcare platforms facilitate real-time data collection, improving decision-making and patient outcomes. These advancements are particularly impactful in managing chronic diseases, elderly care, and post-operative recovery. Despite these benefits, IoT-based healthcare systems introduce substantial security and privacy challenges. Medical data is highly sensitive and requires strict protection mechanisms. Conventional architectures rely heavily on centralized cloud infrastructures, which create single points of failure, increase the risk of data breaches, and limit transparency in data usage. Another major limitation is the reliance on static trust models. In most systems, entities are considered trustworthy once authenticated, without continuous validation of behavior. This approach is inadequate in dynamic environments where devices may be compromised or users may misuse access privileges. Furthermore,

10.48047/jocaaa.2024.33.08.456

existing consent mechanisms lack flexibility and user control. Patients typically provide one-time authorization, with limited visibility or control over subsequent data usage. This reduces trust in digital healthcare systems and raises concerns regarding ethical data governance. To overcome these limitations, this paper introduces a blockchain-enabled trust and privacy framework that integrates decentralized trust management with dynamic consent control. By leveraging blockchain technology and smart contracts, the framework ensures transparent, secure, and patient-centric data handling while continuously evaluating trust across system entities. Unlike existing trust-centric healthcare frameworks, the proposed model introduces a hybrid approach that combines blockchain-based decentralized validation with behavior-driven dynamic trust evaluation and real-time consent enforcement. This integration enhances system transparency, adaptability, and security across all layers.

2. Related Work

Recent advancements in IoT-based healthcare systems have significantly improved remote patient monitoring and real-time diagnostics. However, these systems continue to face critical challenges related to data privacy, security, and trust management. Early approaches primarily focused on secure data transmission using encryption techniques and cloud-based storage solutions [1], [2]. While these methods improved accessibility and scalability, they introduced centralized trust dependencies, making systems vulnerable to data breaches and single points of failure. With the emergence of blockchain technology, several studies have explored decentralized solutions for healthcare data management. Blockchain-based frameworks provide immutable data storage, transparency, and improved security [9], [10], [11]. However, most of these approaches focus mainly on data integrity and secure storage, with limited emphasis on dynamic trust evaluation and user-controlled consent mechanisms. A trust-centric privacy engineering framework for IoT-based remote patient monitoring systems was proposed in [21], which integrates layered access control and privacy-aware data sharing. Although effective in enhancing data privacy, the framework does not incorporate blockchain-based decentralized validation or behavior-driven trust adaptation. Similarly, zero-trust models and access control mechanisms have been explored to strengthen security in distributed environments, but they are rarely integrated with blockchain-based healthcare architectures.

Research Contributions

This study makes several key contributions toward improving security, privacy, and trust management in IoT-based healthcare systems:

- **Decentralized Trust Framework:** A blockchain-enabled architecture is proposed to eliminate centralized trust dependency and ensure transparent and tamper-proof data validation.
- **Dynamic Consent Mechanism:** A smart contract-based consent model is introduced to enable real-time, patient-controlled access to healthcare data.
- **Behavior-Based Trust Model:** The framework incorporates a dynamic trust evaluation mechanism that continuously adjusts access privileges based on user behavior and contextual factors.
- **Layered Security Architecture:** A multi-layered system design is developed to ensure end-to-end protection across sensing, gateway, privacy, blockchain, cloud, and application layers.
- **Trust-Zone Model:** A novel trust zoning approach is introduced to classify system components based on risk levels and access privileges.

10.48047/jocaaa.2024.33.08.456

- **Comparative Analytical Evaluation:** The proposed framework is evaluated against existing approaches, demonstrating improvements in privacy, scalability, and trust adaptability.

3. Challenges in IoT-Based Healthcare Systems

IoT-based healthcare systems have transformed medical services by enabling continuous monitoring and real-time data collection. However, their reliance on interconnected devices, distributed networks, and cloud infrastructures introduces significant concerns related to security, privacy, and trust**.** Unlike traditional systems with controlled environments, IoT healthcare operates across multiple layers—devices, gateways, networks, and cloud platforms expanding the attack surface and increasing system complexity. Current implementations face several critical challenges, including centralized trust dependency**,** lack of data integrity verification**,** static consent mechanisms**,** insider threats**,** and limited **transparency**. Centralized cloud systems create single points of failure, while traditional storage lacks tamper-proof mechanisms. Consent models are often inflexible, and insider misuse remains difficult to detect. Additionally, insufficient auditability reduces user trust and complicates regulatory compliance. These limitations highlight the need for a shift toward decentralized and adaptive architectures. The proposed framework addresses these issues by introducing blockchain-based trust management**,** immutable data verification**,** dynamic consent enforcement**,** and transparent audit mechanisms, providing a more secure and patient-centric approach to healthcare data management.

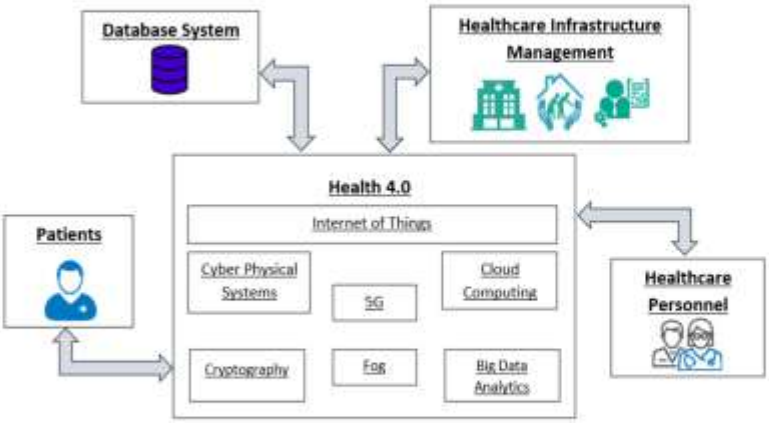

Figure 1: IoT-based Health 4.0 architecture connecting patients, cloud, and healthcare systems.

Table 1: ***Key Challenges***

Challenge	**Description**
Centralized Trust	Cloud dependency creates vulnerabilities
Data Integrity	Lack of tamper-proof mechanisms
Static Consent	Inflexible permission models
Insider Threats	Misuse by authorized users
Limited Transparency	Lack of auditability

10.48047/jocaaa.2024.33.08.456

4. Research Methodology

This study adopts a design-oriented and analytical research methodology aimed at developing a secure and trust-aware framework for IoT-based healthcare systems. Unlike purely experimental approaches, this research emphasizes architectural innovation, systematic modeling, and logical validation to ensure both originality and practical applicability. The methodology is structured into five interconnected stages:

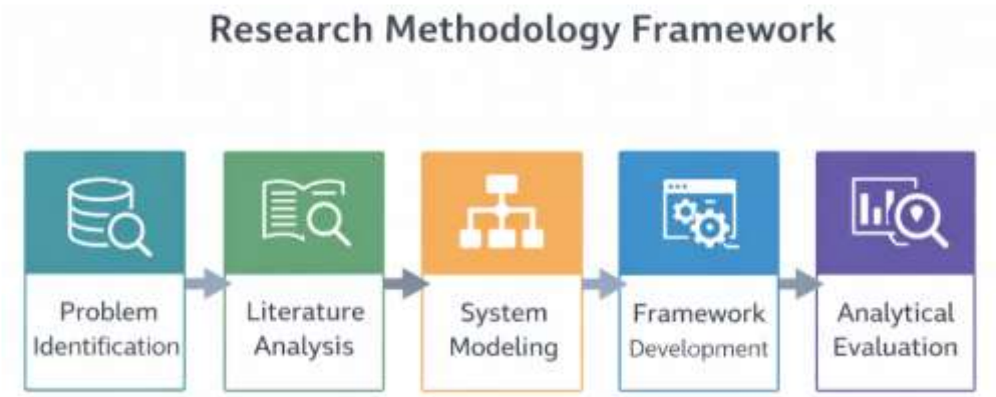

Figure 2: *Research Methodology Framework*

Stage 1: Problem Identification
A detailed analysis of existing IoT healthcare systems is conducted to identify critical limitations, including centralized trust dependency, lack of transparency, static consent mechanisms, and data integrity vulnerabilities.

Stage 2: Literature Synthesis
Instead of a general review, this study performs a targeted synthesis of prior work in blockchain-based healthcare, trust management systems, and privacy-preserving architectures to identify research gaps.

Stage 3: System Modeling
A multi-layered system model is constructed, defining entity roles, communication flows, and trust boundaries across IoT devices, gateways, blockchain nodes, and cloud infrastructure.

Stage 4: Framework Design
The proposed framework is developed by integrating decentralized blockchain mechanisms, smart contract-based consent control, and adaptive trust evaluation into a unified architecture.

Stage 5: Analytical Validation
The framework is evaluated using qualitative and analytical metrics, focusing on privacy robustness, trust adaptability, scalability, and system efficiency.

5. Conceptual Foundations

The proposed blockchain-enabled healthcare framework is built upon a set of core conceptual principles that define how data is generated, processed, and shared across the system. These foundations ensure that privacy, trust, and security are not treated as separate features but are embedded directly into the system design.

10.48047/jocaaa.2024.33.08.456

5.1 Multi-Entity System Environment

An IoT-based healthcare system operates as a **multi-entity ecosystem**, where different components interact to enable continuous monitoring and data exchange. Unlike traditional healthcare systems, where data is confined within a single organization, IoT-based systems involve multiple distributed entities with varying roles and responsibilities.

The primary entities involved include:

- **Patients**, who generate physiological data through wearable devices
- **IoT sensing devices**, which collect real-time health information
- **Edge gateways**, responsible for aggregating and preprocessing data
- **Blockchain nodes**, which maintain decentralized records and enforce trust
- **Cloud platforms**, used for storage, analytics, and long-term processing
- **Healthcare professionals**, who access data for diagnosis and treatment
- **Administrative authorities**, responsible for system governance and compliance

Each of these entities operates with different levels of access and trust. Therefore, a uniform access control mechanism is insufficient. The system must support **role-based and trust-aware interactions** to ensure that each entity accesses only the data relevant to its function.

This multi-entity nature introduces complexity but also provides an opportunity to design a **fine-grained and flexible security model** that adapts to diverse system participants.

5.2 Data Sensitivity and Classification

Healthcare data is inherently sensitive, but not all data carries the same level of risk. The proposed framework recognizes that different types of data require different levels of protection, leading to a **data classification-based security approach**.

The system categorizes healthcare data into multiple levels:

- **Highly sensitive data**: Raw physiological signals such as ECG readings, heart rate, and oxygen levels, which directly reflect a patient's health condition
- **Moderately sensitive data**: Processed information such as alerts, summaries, and diagnostic insights
- **Low sensitivity data**: Aggregated or anonymized datasets used for research or statistical analysis

Each category is handled differently within the system:

- High-sensitivity data requires **strict encryption and restricted access**
- Moderate data may be shared with authorized users under defined conditions
- Low-sensitivity data can be used for broader analysis with minimal privacy risk

By implementing this classification, the framework ensures **data minimization**, where only necessary information is shared, reducing the risk of unnecessary exposure.

5.3 Dynamic Trust Management Model

10.48047/jocaaa.2024.33.08.456

Traditional healthcare systems often rely on **static trust models**, where devices and users are authenticated once and then granted continuous access. However, this approach is insufficient in dynamic and distributed environments.

The proposed framework adopts a **dynamic trust model**, where trust is continuously evaluated based on behavior, context, and policy compliance.

- Key characteristics of this model include:
- **Behavior-based trust evaluation**: Trust levels increase when entities consistently follow system policies and decrease when anomalies are detected
- **Context-aware access control**: Access decisions consider factors such as time, location, and usage patterns
- **Adaptive privilege management**: Access rights are adjusted dynamically based on trust levels

For example, a healthcare provider with consistent access behavior may be granted higher trust, while unusual activity may trigger restrictions or additional verification.

This dynamic approach enhances system resilience by:

- Reducing reliance on static credentials
- Detecting insider threats more effectively
- Preventing long-term misuse of access privileges

5.4 Decentralized Trust Assumption

A key conceptual shift in the proposed framework is the transition from **centralized trust to decentralized trust**. Instead of relying on a single authority, trust is distributed across blockchain nodes, where all transactions are verified collectively.

This approach ensures:

- No single point of failure
- Transparent and verifiable operations
- Immutable records of all activities

Decentralized trust strengthens the reliability of the system and enhances user confidence in data handling processes.

6. Proposed Framework

The proposed framework introduces a **blockchain-enabled trust and privacy architecture** for IoT-based healthcare systems. It is designed to overcome the limitations of traditional centralized models by integrating **decentralized trust management, dynamic consent enforcement, and layered security mechanisms**. This ensures that sensitive healthcare data is handled securely, transparently, and efficiently across all system components.

Unlike conventional systems where security is added as an external feature, this framework embeds **privacy and trust directly into the architecture**, ensuring that every stage of data

10.48047/jocaaa.2024.33.08.456

generation, transmission, storage, and access is governed by defined policies and verification processes.

6.1 Key Design Principles

- **Patient-centric data ownership:**
  Patients maintain control over their medical data, including who can access it and under what conditions.
- **Decentralized trust using blockchain:**
  Trust is distributed across multiple nodes, reducing reliance on a central authority and improving system reliability.
- **Least-privilege access control:**
  Access rights are granted based on roles, trust levels, and consent policies, minimizing unnecessary exposure.
- **Smart contract-based dynamic consent:**
  Consent policies are enforced automatically and can be updated in real time based on patient preferences.
- **Transparent and immutable auditability:**
  All transactions and access activities are recorded securely, ensuring traceability and accountability.

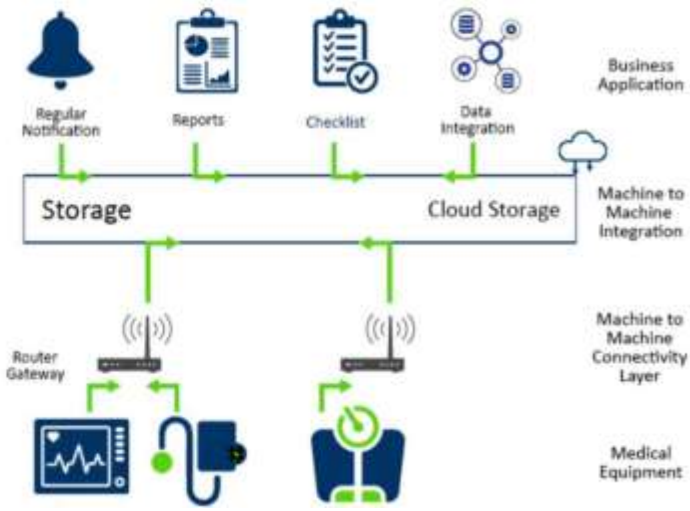

Figure3: ***Proposed layered architecture showing secure data flow across system components.***

6.2 Layered Architecture

The framework is structured into multiple layers, each responsible for specific operations and security functions:

10.48047/jocaaa.2024.33.08.456

- **Sensing Layer:**
  IoT devices collect real-time physiological data. This layer is considered low-trust due to potential device vulnerabilities.
- **Gateway Layer:**
  Acts as an intermediary that aggregates, validates, filters, and encrypts data before transmission, reducing exposure risks.
- **Privacy Layer:**
  Ensures that data is shared only after verifying patient consent and access policies. It supports anonymization and controlled data usage.
- **Blockchain Layer:**
  Serves as the trust backbone by storing hashes, executing smart contracts, and maintaining immutable audit logs.
- **Cloud Layer:**
  Provides secure storage and analytics capabilities, with access restricted based on blockchain-verified permissions.
- **Application Layer:**
  Enables interaction for users such as doctors, patients, and administrators, with access controlled by roles and trust levels.

Table 2: ***Layer Functions***

Layer	**Function**	**Security Role**
Sensing	Data collection	Low trust
Gateway	Processing	Encryption & validation
Privacy	Consent control	Data protection
Blockchain	Trust	Integrity & audit
Cloud	Storage	Controlled access
Application	User access	Authorization

6.3 Trust-Zone Model

To further strengthen security, the framework introduces **trust zones**, where entities are categorized based on risk and access privileges:

- **Zone 1 (Sensors):** Very low trust, limited to data generation
- **Zone 2 (Gateway):** Medium trust, handles validation and encryption
- **Zone 3 (Blockchain):** Very high trust, ensures integrity and audit
- **Zone 4 (Cloud):** Medium trust, manages storage and analytics
- **Zone 5 (Users):** High trust, access controlled through policies

10.48047/jocaaa.2024.33.08.456

This zoning mechanism ensures that data flows only through **trusted pathways** and reduces unauthorized interactions.

Table 3: ***Trust Zones***

Zone	Entities	Trust Level
Z1	Sensors	Very Low
Z2	Gateway	Medium
Z3	Blockchain	Very High
Z4	Cloud	Medium
Z5	Users	High

6.4 Block chain & Consent

The framework leverages blockchain to provide secure and transparent consent management:

- Stores **cryptographic hashes** instead of raw data to preserve privacy
- Uses **smart contracts** to automate access control decisions
- Enables:
    - Real-time consent updates
    - Transparent data usage tracking
    - Immutable logging of all actions

This ensures that patients have full control while maintaining system security.

6.5 Secure Workflow

The system follows a structured workflow to ensure secure data handling:

- ➢ Sensors collect patient data
- ➢ Gateway validates, filters, and encrypts data
- ➢ Privacy layer verifies consent and policies
- ➢ Blockchain records transactions and verifies trust
- ➢ Cloud stores encrypted data securely
- ➢ Authorized users access data based on permissions

10.48047/jocaaa.2024.33.08.456

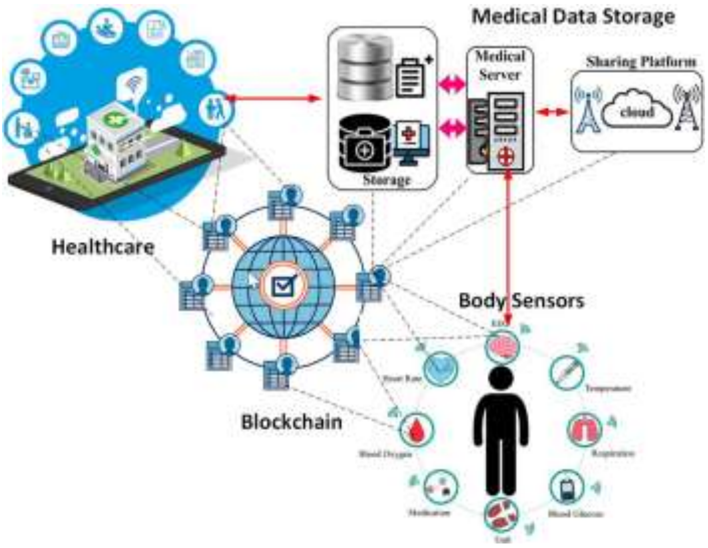

Figure 4: ***Data Flow***

6.6 Component Roles

- **Sensors:** Generate real-time health data
- **Gateway:** Ensures data filtering, validation, and encryption
- **Privacy Layer:** Enforces consent and access policies
- **Block chain:** Maintains trust, integrity, and audit logs
- **Cloud:** Provides storage and analytical processing
- **Application:** Enables secure user interaction.

6.7 Algorithm for Secure Data Access

Input: User request, Patient consent policy, Trust score
Output: Access decision
Step 1: Receive access request from user
Step 2: Verify identity and authentication
Step 3: Retrieve patient consent policy
Step 4: Evaluate trust score of requester
Step 5: If (trust score ≥ threshold AND consent valid)
Grant access
Else
Deny access
Step 6: Record transaction on block chain
Step 7: Update trust score dynamically

7. Block chain Integration

Block chain is a key component of the proposed framework, enabling secure, decentralized, and transparent healthcare data management**.** Unlike traditional centralized systems, block chain uses a distributed ledger to validate and record transactions immutably, ensuring data integrity and accountability. This makes it highly suitable for handling sensitive healthcare data.

7.1 Core Functions of Block chain

10.48047/jocaaa.2024.33.08.456

- **Decentralized trust management:**
  Eliminates reliance on a single authority by distributing validation across multiple nodes.
- **Secure access control:**
  Smart contracts automate permission handling and enforce patient-defined consent policies.
- **Audit and transparency:**
  All system activities are recorded as immutable logs, enabling traceability and accountability.
- **Privacy-preserving storage:**
  Only hashes and metadata are stored on-chain, while actual data remains encrypted off-chain.

7.2 Data Integrity Process

- Each medical record is converted into a **cryptographic hash** before storage.
- The hash is stored on the blockchain for verification.
- During access, the hash is recalculated and compared to detect tampering.

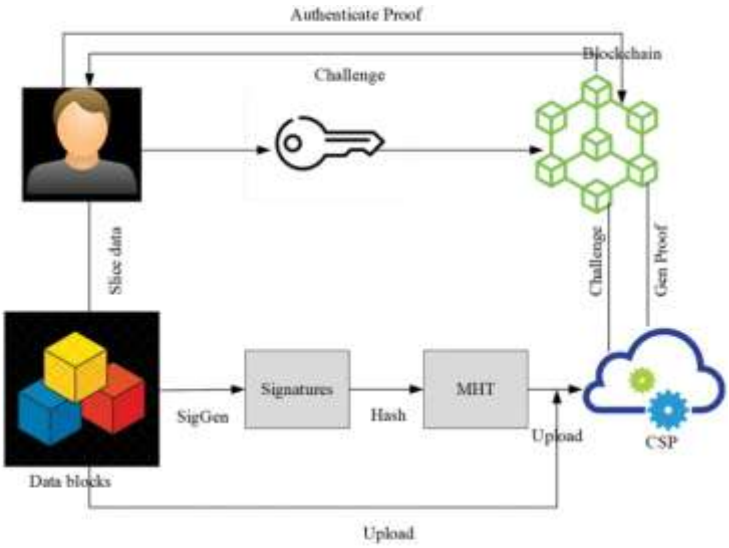

Figure 5 : ***Data Integrity Workflow***

7.3 Smart Contract-Based Access Control

- Smart contracts automatically evaluate access requests based on consent and trust policies.
- Access is granted or denied without manual intervention.
- All decisions are recorded on the blockchain for transparency.

10.48047/jocaaa.2024.33.08.456

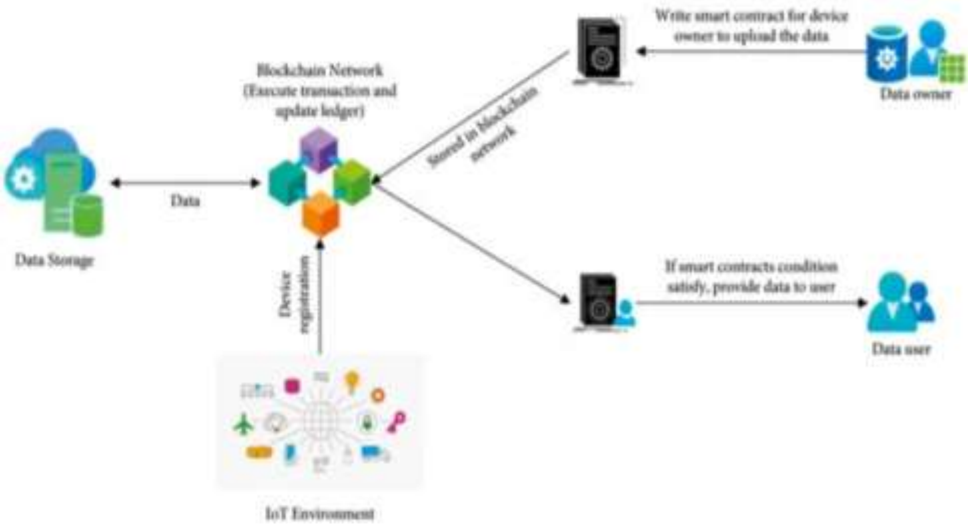

Figure 6: ***Smart Contract Access Flow***

7.4 Integration with IoT Healthcare Workflow

- IoT devices generate patient data
- Gateway encrypts and processes data
- Blockchain stores verification hashes
- Cloud stores encrypted data
- Access is controlled via smart contracts

This integration ensures secure data flow, decentralized validation, and real-time access control.

Table 4: ***Block chain Contributions to System Security***

Feature	Contribution
Immutable Logs	Detect and prevent data tampering
Smart Contracts	Automate and enforce access control
Decentralization	Remove single point of failure
Cryptographic Security	Ensure data authenticity
Auditability	Enable transparent monitoring

8. Analytical Evaluation

The proposed block chain-enabled trust and privacy framework is evaluated using a conceptual approach, focusing on privacy, trust management, scalability, and performance. As the framework is architectural, the evaluation emphasizes logical consistency, security strength, and practical applicability rather than experimental results. The framework ensures strong privacy protection and adaptive trust management through a multi-layered design. Data is encrypted at the gateway, validated through consent policies, and securely tracked using block chain without exposing sensitive information. Trust is dynamically updated based on behavior, access patterns, and policy compliance, allowing the system to detect anomalies, reduce insider threats, and adjust access privileges accordingly.

10.48047/jocaaa.2024.33.08.456

In terms of scalability and performance, the framework adopts a modular architecture with edge processing and decentralized trust management to handle large-scale deployments efficiently. To reduce block chain overhead, only hashes are stored on-chain while actual data remains off-chain in encrypted storage. This approach ensures efficient performance while maintaining data integrity, making the system suitable for real-world healthcare applications. The proposed framework demonstrates improved adaptability and security compared to existing models due to the integration of decentralized validation and dynamic trust mechanisms.

Table 5 : ***Analytical Evaluation Summary***

Evaluation Parameter	**Observation**
Privacy Protection	Strong due to multi-layered enforcement
Trust Management	Adaptive and behavior-based
Scalability	High due to modular architecture
Performance Efficiency	Optimized using off-chain storage
Security Robustness	Enhanced through blockchain integration
System Transparency	High due to immutable audit logs

9. Comparative Analysis

To highlight the significance of the proposed framework, it is essential to compare it with existing approaches in IoT-based healthcare systems. Traditional healthcare architectures primarily focus on data collection and transmission, while more recent block chain-based systems introduce decentralization and improved data integrity. However, many of these solutions still lack comprehensive integration of dynamic trust management, consent control, and layered privacy enforcement**.** The proposed framework distinguishes itself by combining block chain technology with trust-centric design principles, resulting in a more secure, transparent, and adaptive system.

Table 6: ***Comparison***

Feature	**Traditional**	**Block chain**	**Proposed**
Trust	Centralized	Decentralized	Hybrid
Privacy	Weak	Moderate	Strong
Control	Low	Medium	High

10. Limitations

Although the proposed block chain-enabled trust and privacy framework introduces significant improvements in security, transparency, and data governance, several limitations must be acknowledged. These limitations primarily relate to implementation complexity, performance considerations, and practical deployment challenges.

10.48047/jocaaa.2024.33.08.456

- **Block chain latency and overhead:**
  Block chain operations require validation across nodes, which may increase latency and resource usage, especially under high transaction loads.
- **System complexity:**
  The multi-layered architecture involving IoT devices, gateways, blockchain, and cloud components makes system design, integration, and maintenance more complex.
- **Deployment challenges:**
  Implementation depends on advanced infrastructure such as blockchain networks, secure identity systems, and reliable communication, which may be costly and difficult to adopt.
- **Identity and key management issues:**
  Managing cryptographic keys across multiple users and devices is challenging and may lead to risks such as key loss, compromise, or recovery difficulties.
- **User awareness and consent complexity:**
  Dynamic consent mechanisms require user understanding, and incorrect configurations may result in overly restrictive or excessive data access.

11. Future Work

Although the proposed framework provides a strong foundation for secure IoT-based healthcare systems, several directions remain for future improvement and practical validation.

First, integrating AI-based trust models can enhance the system's ability to analyze behavior, detect anomalies, and dynamically adjust trust levels, making the framework more adaptive and intelligent. Second, the use of federated learning can support privacy-preserving analytics by enabling model training without sharing raw patient data, thereby reducing exposure risks while maintaining data utility. Third, future research should focus on real-world implementation and prototype development to evaluate system performance, scalability, and usability in practical healthcare environments. Additionally, exploring lightweight block chain solutions and optimized consensus mechanisms can help reduce latency and improve system efficiency for real-time applications. Finally, improving interoperability and standardization will allow seamless integration with existing healthcare systems and support secure data exchange across institutions.

12. Conclusion

This study proposed a block chain-enabled trust and privacy framework for IoT-based healthcare systems to address key challenges related to security, trust, and patient data control. By combining decentralized block chain mechanisms with dynamic consent management, the framework ensures secure, transparent, and patient-centered data handling. The model replaces centralized control with a distributed trust approach, enabling data integrity through immutable records and automated access control using smart contracts. Its layered architecture enforces privacy and security throughout the data lifecycle, while dynamic trust evaluation enhances protection against misuse and evolving threats. Analytical and case-based evaluation indicates that the framework provides strong privacy protection, adaptability, and scalability without significant performance compromise. Overall, the proposed approach offers a practical foundation for developing secure and reliable next-generation healthcare systems, with potential for further enhancement through emerging technologies such as AI and privacy-preserving analytics.

10.48047/jocaaa.2024.33.08.456

REFERENCES

[1] P. Gope and T. Hwang, “BSN-care: A secure IoT-based modern healthcare system using body sensor network,” IEEE Sensors Journal, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[2] P. Verma and S. K. Sood, “Cloud-centric IoT-based disease diagnosis healthcare framework,” Journal of Parallel and Distributed Computing, vol. 116, pp. 27–38, Jun. 2018.

[3] M. T. Mardini, Y. Iraqi, and N. Agoulmine, “A survey of healthcare monitoring systems for chronically ill patients and elderly,” Journal of Medical Systems, vol. 43, no. 50, 2019.

[4] W. T. Vambe and K. Sibanda, “A fog computing framework for QoS optimization in IoT ecosystem,” in Proc. IMITEC, 2020, pp. 1–8.

[5] Z. Sun et al., “Sensing cloud computing in IoT: A novel data scheduling optimization algorithm,” IEEE Access, vol. 8, pp. 42141–42153, 2020.

[6] R. L. Devi and V. Kalaivani, “Machine learning and IoT-based cardiac arrhythmia diagnosis using ECG features,” Journal of Supercomputing, 2019.

[7] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[8] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: Challenges and solutions,” arXiv preprint arXiv:1608.05187, 2016.

[9] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control,” Journal of Medical Systems, vol. 40, no. 10, 2016.

[10] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” Information, vol. 8, no. 2, p. 44, 2017.

[11] H. Liang et al., “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” IEEE Access, vol. 5, pp. 24189–24199, 2017.

[12] M. Hölbl et al., “A systematic review of the use of blockchain in healthcare,” Symmetry, vol. 10, no. 10, p. 470, 2018.

[13] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[14] Z. Zheng et al., “An overview of blockchain technology: Architecture, consensus, and future trends,” in Proc. IEEE BigData Congress, 2017, pp. 557–564.

[15] K. Fan et al., “MedBlock: Efficient and secure medical data sharing via blockchain,” Journal of Medical Systems, vol. 42, no. 8, p. 136, 2018.

[16] J. Zhang et al., “A secure system for pervasive social network-based healthcare,” IEEE Access, vol. 4, pp. 9239–9250, 2016.

10.48047/jocaaa.2024.33.08.456

[17] A. Shahnaz, U. Qamar, and A. Khalid, “Using blockchain for electronic health records,” IEEE Access, vol. 7, pp. 147782–147795, 2019.

[18] R. Gupta et al., “Blockchain-based secure healthcare system: A survey,” IEEE Systems Journal, 2020.

[19] M. Esposito et al., “Blockchain: A panacea for healthcare cloud-based data security and privacy?” IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, 2018.

[20] Y. Zhang and J. Lin, “Blockchain-based secure and privacy-preserving data sharing in healthcare systems,” IEEE Transactions on Services Computing, 2020.

[21] S. S. Manogaran et al., “A trust-centric privacy engineering framework for IoT-based remote patient monitoring systems,” NeuroQuantology, 2022.