

Blockchain-Enabled Secure Data Sharing Framework for Healthcare IoT Devices

Qi Jing*

School of Informatics, Computing
and Cyber Systems, Master
Northern Arizona University,
Flagstaff, Arizona, US

*E-mails: jinglegege@gmail.com

Received for publication
January 02, 2026.

Abstract

The growing use of IoT devices in healthcare has increased medical data security challenges, as traditional access control models like role-based access control (RBAC), attribute-based access control (ABAC), and mandatory access control (MAC) lack flexibility and context awareness. The healthcare Internet of Things (IoT) faces challenges such as limited scalability, lack of dynamic access controls, and security risks from a centralized point of vulnerability. The research aims to develop a resilient, decentralized access control solution that provides secure, time-sensitive permissions in healthcare IoT systems. A hybrid RBAC-ABAC model, built on blockchain and integrated with interplanetary file system (IPFS), enables secure data sharing across healthcare IoT devices, outperforming current models in accuracy, latency, and scalability. A dual smart contract-IPFS mechanism enables adaptive access control. Results show 96.5% precision, 3.2 ms policy evaluation, 120 ms response time, 74 TPS, low cost (US\$2.1), and 45–52 MB memory use. It outperforms ABAC, RBAC, and MAC, offering scalable, efficient security for healthcare IoT data sharing.

Keywords

blockchain, Internet of Things (IoT), access control, healthcare data security, smart contracts

1. Introduction

The healthcare industry has implemented Internet of Things (IoT) technology to enable transformative changes in provider monitoring of patients at remote facilities and to offer enhanced medical care through smart devices (Khan et al., 2025). Observational devices that measure body signals inside human tissue and home monitoring equipment help doctors make more precise diagnoses while enabling patients to obtain superior medical results with enhanced treatment power (Mohanta et al., 2025). Advanced medical technologies have introduced significant security, privacy, and access control challenges (Tang et al., 2025).

Advanced medical data privacy calls for rapid defense actions to stop unauthorized personnel from

entering while simultaneously blocking data misuse and tampering by internal staff through devices (Sarojini Karuppusamy, & Kumar, 2025). Two essential reasons exist for healthcare systems to implement information access controls through patient data privacy protection together with operational healthcare security establishment (Zhao et al., 2025).

The conventional data sharing methods in the healthcare industry rely on centralized systems that result in failure points and restricted visibility together with restricted expansion possibilities (Khan et al., 2025).

Standard role-based permission systems fail to adapt quickly to healthcare requirements because they do not provide enough flexibility when granting emergency or multi-institutional care temporary access (Sahu & Karthikeyan, 2024). Centralized

systems lack transparency, making it difficult to track when and how data is accessed (Nassa et al., 2025). The increasing adoption of blockchain technology aims to solve the existing limitations in healthcare security (Mazid et al., 2025).

Blockchain provides three essential properties: decentralization, encryption, and automated smart contracts that construct a modern system for trustworthy, secure data sharing (Abasaheb & Mallapur, 2025). The infrastructure-based deployment of control functions and policy enforcement through blockchain technology provides healthcare organizations with a trustworthy method to share data (Tlemçani et al., 2025).

The development of healthcare demands initiated major research into blockchain technology collaborations with advanced authorization systems for IoT healthcare solutions. User-based and environment-based decisions become more detailed when healthcare organizations integrate access control mechanisms ABAC and RBAC. Blockchain smart contracts enable healthcare institutions to develop self-operating access control systems with total transaction traceability that compels data sharing when pre-defined protocols exist (Pandey et al., 2025). System administrators achieve operational cost reduction while simultaneously receiving better system security and privacy features through this method (Greco et al., 2025).

The system operates with excellent efficiency alongside scalability through its off-chain storage method, which safely protects big data files, as chain-based storage keeps only hash codes. Using its integration capabilities, blockchain creates protected data exchange possibilities between various medical organizations that function across every healthcare supplier system. Blockchain-enabled secure data sharing frameworks have a crucial future role in advancing digital health systems since they provide vital support for real-time patient-centric care systems despite technical and healthcare industry evolution needs.

The research objective involves developing an exclusive framework for healthcare facilities to address security and privacy risks from healthcare IoT systems that share data. This research focuses on designing an access control framework with the aim of granting flexible time-sensitive access to medical data while solving problems with central access control methods. The research applies enhancing system scalability with adaptable data sharing practices along with transparency measures to boost protected sensitive patient data and operational

efficiency in real-time processes of healthcare IoT systems. This study investigates the potential of blockchain decentralized technologies to enhance healthcare organization needs in secure multi-institutional and emergency care management.

The current study extends prior research on IoT security in healthcare by proposing a hybrid access control framework that integrates role-based access control (RBAC) and attribute-based access control (ABAC) within a decentralized architecture supported by interplanetary file system (IPFS) and blockchain technology. Existing studies in this domain have primarily focused on traditional access control mechanisms or isolated blockchain-based solutions, often lacking flexibility and context-awareness in dynamic healthcare environments. In contrast, the proposed framework offers a flexible, scalable, and adaptive access control model capable of addressing the complex and evolving requirements of healthcare IoT systems. Furthermore, this study provides a comprehensive performance evaluation, incorporating metrics such as accuracy, latency, throughput, and sensitivity analysis, thereby offering a more rigorous assessment compared to prior works.

a. Key contributions

The principal contributions described below were made by this project:

- Designs a novel hybrid access control model by integrating RBAC and ABAC to enable dynamic and context-aware decision-making in healthcare IoT systems.
- Integrates IPFS with blockchain technology to achieve secure, decentralized, and scalable medical data storage and sharing.
- Implements a smart contract-based automated access control mechanism to ensure transparent, traceable, and efficient data access.
- Evaluates the proposed framework through comprehensive performance analysis, demonstrating improved accuracy, reduced latency, and enhanced scalability compared to traditional models such as RBAC, ABAC, and mandatory access control (MAC).

II. Related Works

Academic teams worldwide have conducted investigations about healthcare data security through the implementation of IoT and blockchain technologies for several years. These projects work as security

solutions addressing the main healthcare problems like inadequate access management systems and hidden asset visibility limitations, and unclear system security protocols.

The healthcare sector depends primarily on RBAC for its access control, but this method proves inadequate for medical environments that need advanced approval systems. The performance speed and ability to scale of blockchain solutions suffer during implementation when developers create unsuitable designs. The information in Table 1 demonstrates how field-oriented research compares to identify current operational statuses and existing gaps (Table 1). Multiple frameworks receive evaluation through criteria testing that evaluates both access control performance and blockchain deployment stages and scalability and security elements for their utility in healthcare IoT systems.

Ahmed et al. (2025) research looked into how blockchain technology strengthens overall data privacy by linking with IoT-based health monitoring systems while ensuring both transparency and data integrity. The research team developed a distributed framework where smart contracts acted to deal with patient health information while enabling protected device communications. Real-time patient information access combined with tamper-proof data storage characteristics was enabled through this technique. The medical records experienced the highest integrity due to this system protecting against unauthorized data modifications. The researchers revealed

performance problems in their study, yet they recognized that these operational problems specifically impact IoT devices with limited resources both in terms of their performance speed and communication operations.

Mazhar et al. (2025) studied blockchain operations between AI and IoT technologies to develop secure intelligent medical systems ecosystems. The authors created a united system structure that uses blockchain technology to handle dispersed health-care information and enable patient-controlled secure data access. Better data control and improved device and platform exchanging capabilities combined with tamper resistance formed the essential design benefits of this system. The system demonstrated limited performance potential because of integration problems and energy requirements as well as necessary regulatory clearances.

Meisami et al. (2023) created a blockchain protocol that focuses on e-health environments to support free medical data access without third-party intervention. The system incorporated an easy consensus operation that enables network use for basic IoT devices, which also provided encrypted private access management. The system reached better visibility and delivered precise access privileges and cost-effective network operations to patients as its principal benefits. The primary difficulties that arose from implementing this system stemmed from issues with scalability together with performance degradation within extensive real-time medical systems.

Table 1: Research gap validation

Author(s)	Techniques involved	Advantages	Disadvantages
Ahmed et al. (2025)	Smart contracts in blockchain-enabled IoT health monitoring	Tamper-proof data, real-time access, strong privacy	High latency, computational load on IoT devices
Mazhar et al. (2025)	Blockchain + AI + IoT hybrid architecture	Data ownership, interoperability, tamper resistance	Integration complexity, energy use, regulatory issues
Meisami et al. (2023)	Lightweight blockchain with privacy-preserving access control	Transparency, low cost, patient-centric access	Scalability, performance in large systems
Cheikhrouhou et al. (2023)	Fog-computing with blockchain for remote monitoring	Faster response, better security and real-time processing	Reliance on fog nodes, consistency challenges
Rizzardi et al. (2024)	Hyperledger fabric for supply chain and medical record security	Supply chain transparency, data integrity, secure sharing	High setup cost, complex deployment

IoT: Internet of Things.

Cheikhrouhou et al. (2023) created a blockchain framework that integrates fog computing along with minimal weight features for establishing secure remote patient monitoring operations. Edge-computing data management employed blockchain technology such that unalterable data storage combined with fog nodes, which operated distributed data processing throughout the system, delivered faster performance and greater operational efficiency. The primary advantage of this system resulted from its 40% speed enhancement alongside new security and privacy capabilities that were implemented effectively within real-time systems. The operational framework had technical problems because it required centralized fog nodes along with struggles for decentralized elements to synchronize their data.

Rizzardi et al. (2024) created a blockchain-based architecture that unites IoT systems for protecting medical file management in healthcare supply chain operations. The system made use of Hyperledger Fabric to develop a blockchain platform that provided secure, traceable, and efficient data sharing capabilities for stakeholders. The implementation of this approach enabled better visibility into supply chains, lower levels of fraud, and secured data from tampering attempts. The study emphasized two key constraints that researchers encountered while implementing enterprise-grade blockchain solutions due to high setup expenses and complex learning process requirements.

The importance of having a secure and dependable healthcare system, especially for sensitive areas like healthcare IoT, has been supported by recent studies. According to Hassan et al. (2025) there is an increase in the number of cyberattacks and a growing number of impacts on the economy and operations from cyberattacks in all industries, which makes it imperative that there is a secure framework for security in all sensitive areas like healthcare IoT. In addition, Hoonsoon et al. (2025) examined self-efficacy as a factor influencing the adoption of telemedicine in emerging countries and concluded that trust in telemedicine systems and their reliability are significant factors affecting the adoption of digital healthcare technologies. Both of these studies demonstrate that it is essential to have secure, scalable, and user-centered access control mechanisms, as proposed in this paper.

III. Proposed Architecture

A hybrid access control strategy serves medical data exchange requirements in IoT platforms through the proposed framework. The proposed method

integrates role-based and ABAC. The suggested control method enables quick modifications of healthcare conditions through real-time management of rights, which encapsulate dynamically associated on-the-fly elements such as patient context, device status, and location information.

The proposed method for this study provides baseline access permissions that support fundamental access control related to professional duties for roles including patients and both nurses and doctors. These strategies are implemented using smart contracts, enabling scalable and adaptive access control. Figure 1 shows the suggested architecture.

The proposed architecture consists of two essential elements - blockchain-based IPFS serves as storage and implements different types of smart contracts on decentralized IoT to provide safe access control. Users gain access to their unique user ID through the client application so the system can store this key together with user profile information such as departmental affiliation, role, and name in the user management contract.

The medical data management contract accepts uploads of metadata for data storage from IPFS systems that refer to data owners through interplanetary file system content identifier (IPFSCID). The system allows users to determine ownership through their accounts, and they employ their user IDs to access the client application and authenticate data validation. User permissions get verified through an access control procedure that draws its established policies from the policy contract. IPFS receives the pertinent IPFSCID from the management contract to store data through its system before granting permitted clients access to download the files.

a. Threat architecture

The architecture system defines adversaries as external attackers together with malevolent actors who can have various levels of access to data and architecture components. External attackers are categorically unreliable. The proposed architecture becomes non-functional when external attackers send numerous requests through denial of service (DoS) and distributed DoS attacks that overload servers and validate the network, preventing authorized customers from receiving service. These attackers intercept and potentially modify communication between two entities through man-in-the-middle attacks in order to obtain sensitive information.

Phishing assaults prove to be substantial threats for users since criminals pretend to represent genuine

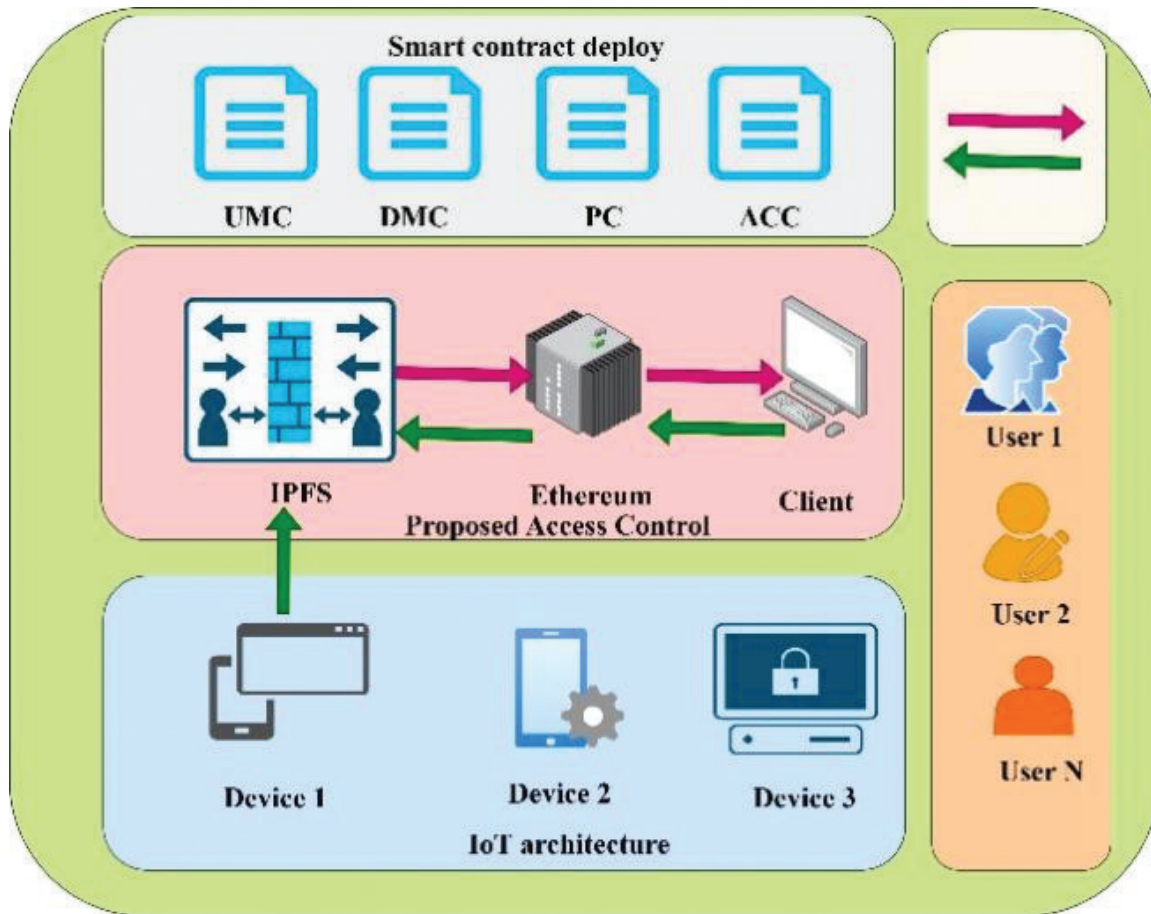


Figure 1: Proposed architecture with data access control. IPFS, interplanetary file system; UMC, user management contract.

organizations to acquire sensitive information such as login credentials and user IDs that enable identity theft. Terrorists within the organization operate without total honesty. Attackers often seek to modify authorization illegally, which allows them to validate regular data or they seek to sell user information for personal benefit even if their legal permissions cover some parts of data (Harish et al., 2025).

The proposed design addresses four security threats, which include sybil attacks and DoS attacks together with data integrity attacks and unauthorized data access attacks (Prajapat et al., 2025). Secure access management in IoT architecture demands the implementation of assumptions as a basis for the recommended design (Mishra et al., 2025). A permissioned blockchain system exists under the assumption that medical facilities have earned approval status, which grants them access to integrate with the architecture through transaction verification. Verification of hash encryption occurs after

the data transmission process in the proposed system architecture (Erukala et al., 2025). The system design assumes two principles: attackers do not have enough computing strength to decode standard cryptographic algorithms, and attackers cannot detect all system communications (Lakshmi et al., 2025).

The use of a permissioned blockchain and the limited computing power available to attackers are assumptions made by healthcare environments regarding access by authorized parties (through a controlled network). These assumptions allow secure communication and efficient operation of the system. On the other hand, any changes to the assumptions, such as an increased ability for an attacker or that one or more of the nodes have been compromised, could negatively impact system security and increase the latency of responses. Thus, the robustness of this architecture is dependent upon keeping these assumptions operational.

b. User management contract

In the IoT architecture, the user management contract (UMC) controls user IDs. Through its decentralized storage system, the UMC develops registries that maintain user IDs safely with complete integrity and uniqueness attributes, which integrate blockchain immutability solutions (Kabra et al., 2025). Each user in the architecture requires a specific identification, which is generated through the hash function (Roy et al., 2025). The implementation combines user primary attributes with department information, role access, address details, and username text to create a cryptographic hash value that establishes a secure and individual userID that resolves detection issues for single users throughout the complete architecture (Li et al., 2025). The UMC provides multiple essential operational elements for operating dynamic user data management. The adduser method in user designs which includes departments, roles, addresses, and names and automatically produces a new entry with a special userID in the system (Vinayasree & Reddy, 2025). The user list functions as a permanent database for users to store the new entry after record addition. The system inserts verification steps within the function to guarantee effective, safe storage of data. The verification process of the user address against the input variable helps ensure data reliability (Bagchi et al., 2025). The system monitors user variations in real-time through information logging after triggering an event associated with the optimal addition process. The adduser function of UMC based on blockchain on the client enables administrators and users to both register users and acquire a unique userID (Venice et al., 2025).

c. Data management contract

The storage system allows secure management of medical data with tracking capabilities across IoT networks that run independently from each other. The smart contract implements blockchain traceability as an access management system that protects privacy through a protocol for data entry identification and recording. A unique identification emerges through the hash operation, which unites the data owner information with data type information alongside IPFSCID (Rastogi, Tripathi, & Sharma, 2025). The distinctive identity manages all data entries so they can be efficiently found on the blockchain while remaining private. Through addData, the system manages primary data entry processes. It creates a specific dataID first, then acquires the datatype information as well as the data owner details and IPFSCID (Verma & Yadav,

2025). During the encryption process, the internal application programming interface (API) function ensures data confidentiality by both encrypting the data collection and safeguarding IPFS-stored information links. The encrypted detector receives storage inside the contract's registry for handling verified access to sensitive data storage places without compromising their privacy (Whig et al., 2024).

The addData operation saves complete blockchain data, which users need to control their files efficiently. The designed contract system exists to enhance tracking and retrieval functionalities. Event-driven designs in compliance-oriented IoT applications require real-time data monitoring thus, this system implements this approach. Authentic data retrieval from saved entries can be conducted through the medical data ID function, which provides secure access based on unique ID specifications. First, this function verifies the datatype field to confirm the availability of the requested record. The decryption process of the IPFS-stored identifier reveals the data only when the check confirms its validity to protect both data safety and accessibility (Ahad et al., 2025).

d. Policy contract

The calculation of IoT access rights depends on essential elements known as policy contracts. The policy contract of this contract merges both ABAC and RBAC architectures to verify multiple access requirements (Vinnarasi & Dayana, 2025). A complete decision function evaluates user attributes while considering roles to pick an access policy dynamically which selects an access architecture. The definition of this access function features the following description Eqs. (1)–(3).

$$HasAccess(u,o) = \begin{cases} Access(u,r,p) & \text{if } S = false \\ Access(a,o,p) & \text{if } S = true \end{cases} \quad (1)$$

$$Access(a,o,p) = \begin{cases} "Allow" & \text{if } P_i = true \\ "deny" & \text{otherwise} \end{cases} \quad (2)$$

$$Access(a,o,p) = \begin{cases} "Allow" & \text{if } (u,r) \in UA, (r,p) \in PA \\ "deny" & \text{otherwise} \end{cases} \quad (3)$$

Here, $u \in U$, $p \in P$, $r \in R$, S is the Boolean function. RBAC functions as the core system of the policy contract because it grants access permissions through pre-defined roles, which represent individual users. The

access control system becomes more efficient when privileges are assigned to users via their assigned roles. RBAC functions as the primary manning methodology to control user access for those whose roles define their authorization needs. RBAC functionality requires that every occupation, including Doctor, Nurse, Technician, and Patient, maintain exclusive permission rules regarding resource access in the IoT network.

The system grants users' necessary access to execute their functions but blocks undesirable access to irrelevant data based on their assigned responsibilities. Each job role receives permissions that correspond with their specific tasks. $Access(u, r, p)$ is the formal function that evaluates RBAC access decisions through its u for user, r for role, and p for requested resource parameters. Using Access (u , Nurse, NursingRecord), a nurse service provider obtains access to departmental nursing records, yet patients use Access to view their personal medical data (Mehla et al., 2025).

The IoT requires access control as a systematic process that verifies users and their permission levels to guarantee safe data access. When an operation starts, the loginUser and Access Data function verifies user identity through their specific user ID. System verification results in updated user sessions as it fetches user department and role information from UMC using the get User function. The system validates permissions through the policy contracts (PC's) has Access function, ensuring that the user department and role comply with data access requirements. Users authorized by access control contract (ACC) can access specified data from medical data management contract (MDMC) through the access Data by Owner function along with the user authorization (Kulkarni et al., 2025).

The implementation of this access control system has three successive stages. Users establish their personal identification through web registration using their encrypted data in the initial stage.

The MDMC receives and includes content identifiers (CIDs) for each user-submitted data through IPFS though these CIDs are maintained inside the UserList of the UMC. The second phase login requires users to let the ACC verify their identification through comparison with UserList data. The system checks the Personal Computer against department and job access permissions for the requested data type. The system provides "Access denied, authorization required" message to users who request access without proper authorization. Permitted access allows the ACC to retrieve relevant data from the MDMC DataList, which becomes available for download

through the web interface. This approach implements an access architecture, which ensures role-based safety standards for healthcare environments.

Role-based permission checks together with user authentication ensure that the suggested access control system provides protected and efficient data processing functions. The system provides an extensive and scalable data access method through integration among ACC and UMC and their submodules PC and MDMC. Data retrieval remains uncomplicated for authorized roles while the system effectively prevents unauthorized users from accessing the system. The increased level of trust and security becomes possible through such solutions in healthcare IoT environments (Abdellatif et al., 2025).

IV. Results and Discussion

a. Experimental setup and parameter configuration

The experimentation evaluation was performed using many significant characteristics; these included the number of users (between 100 and 10,000), transaction rate, smart contract execution timing, and attribute complexities in the context of an ABAC model. These parameters are representative of healthcare IoT scenarios, where system load and access conditions are subject to dynamic changes. The total number of users is representative of system scalability, and total attributes' complexity and role hierarchies are related to the overall performance of access control determinations. Typical Healthcare deployment scenarios were studied to select the given parameter values based on their use in previous studies involving blockchain-enabled IoT systems. The range of users set by the study is a simulation of both small hospitals and larger hospitals. Additionally, the transaction and attribute settings reflect access requirements and the resource limitations of IoT devices.

According to the results from the experiment, this Hybrid Access Control Framework Provides Better Performance in a Healthcare IoT Environment Than a Standard Access Control Framework That Is Designed Specifically for a Healthcare Environment. The Accuracy of The Model Was 96.5%, The Response Time Was About 120 ms and the Throughput Was Approximately 74 TPS. Overall, The Model Is able to Operate in a More Efficient and Scalable Manner.

The newly proposed blockchain-accessed access control framework underwent experimental validation through tests that evaluated security levels as well

as core performance characteristics in healthcare IoT systems. A system performance test analyzed RBAC together with ABAC and MAC which are popular access control models. A hybrid RBAC-ABAC approach proved its excellence at adapting and being precise when making access decisions that involve both permanent roles and temporary contextual elements in dynamic healthcare environments. The security measures of Mandatory Access Control were very strong but the system restricted flexible access management between users and devices. The system developers used Python programming language with smart contract simulation libraries and blockchain integration tools that include web3.py and IPFS client libraries. The research execution involved testing a system that contained an Intel Core i7 processor (Intel Corporation, Santa Clara, CA, USA), 16GB RAM and Ubuntu 20.04 LTS (Canonical Ltd., London, UK) on an experimental setup. The model proved successful in securing precise data access management while minimizing delay times and boosting information retrieval effectiveness, which establishes its suitability for operational healthcare IoT systems.

The results clearly show in Table 2 that the proposed model achieves higher accuracy, lower

response time, and better throughput compared to existing methods.

Table 3 presents a comparative analysis of the proposed framework with recent studies in blockchain-enabled healthcare IoT systems. The comparison is based on key performance metrics, including accuracy, response time, and throughput. The results indicate that the proposed model outperforms existing approaches by achieving higher accuracy (96.5%), lower response time (120 ms), and improved throughput (74 TPS). This performance improvement is attributed to the integration of hybrid RBAC-ABAC mechanisms with blockchain and IPFS, which enhances both flexibility and efficiency in access control.

The accuracy results between four access control models for healthcare IoT environments show that the Proposed Hybrid Model performs better than ABAC and RBAC, followed by MAC, according to Figure 2. The proposed model outperforms traditional approaches by combining role-based and attribute-based controls in a context-aware framework to reach an accuracy level of 96.5%. The accuracy rate for ABAC approaches 89.2% but remains inferior to the proposed model since it lacks core features that drive baseline RBAC.

The RBAC policy achieves 85.7% accuracy because it demonstrates strong administrative manageability along with simple design, yet real-time context handling remains inadequate. The accuracy rate of MAC stands at 82.4% because rule-based centrally managed policies demonstrate insufficient adaptability in healthcare environments that experience rapid changes. The Proposed Hybrid Framework demonstrates improved security and decision accuracy through its design while surpassing the security strengths of ABAC, RBAC, and MAC by 7.3%, 10.8%, and 14.1% respectively, which makes it a strong choice for modern medical data-sharing infrastructure.

Figure 3 illustrates how the Proposed Model performs regarding response time (in milliseconds) against three other access control methods namely ABAC, RBAC, and MAC, during healthcare IoT system

Table 2: Comparison of proposed model with existing access control methods

Model	Accuracy (%)	Response Time (ms)	Throughput (TPS)
RBAC	85.7	210	47
ABAC	89.2	185	52
MAC	82.4	170	50
Proposed Model	96.5	120	74

ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

Table 3: Comparison with existing studies

Study	Technique	Accuracy (%)	Response Time (ms)	Throughput (TPS)
Ahmed et al. (2025)	Blockchain + IoT	91.3	150	60
Mazhar et al. (2025)	AI + Blockchain	92.4	155	65
Meisami et al. (2023)	Lightweight Blockchain	88.7	165	55
Proposed Model	Hybrid RBAC-ABAC + Blockchain	96.5	120	74

ABAC, attribute-based access control; IoT, Internet of Things; RBAC, role-based access control.

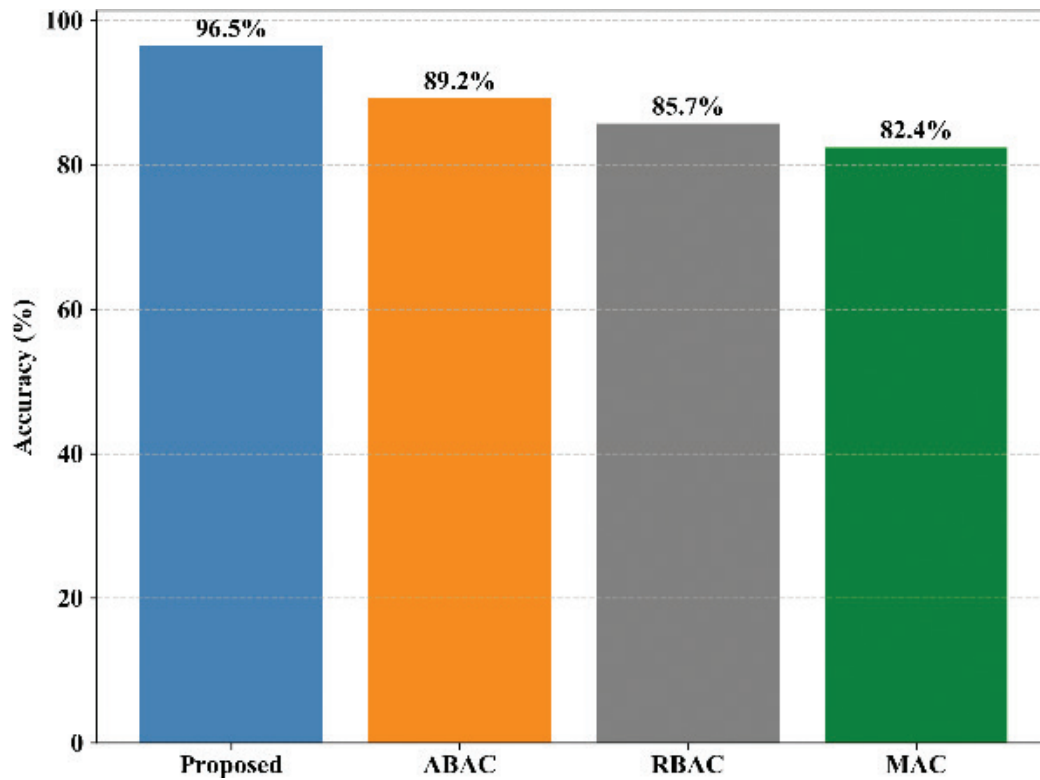


Figure 2: Accuracy. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

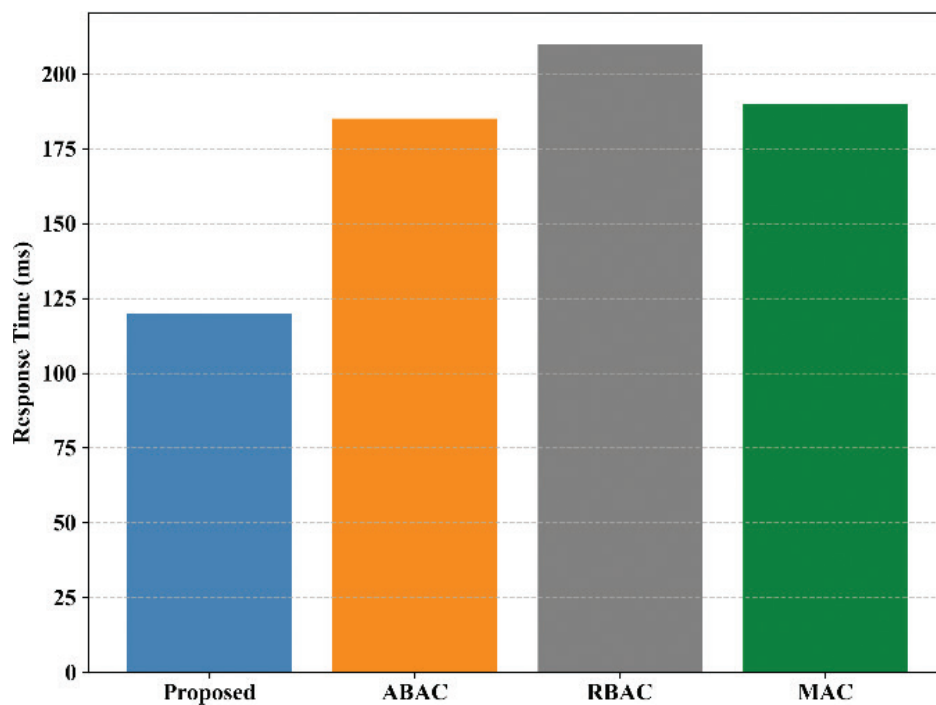


Figure 3: Response time. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

operations. The proposed hybrid model shows maximum operational efficiency because its response time reaches approximately 120 ms, which demonstrates its capability to handle access control requests quickly.

The optimum execution between smart contracts and hybrid decision rational combined with improved optimization functions allows the system to manage contextual parameters efficiently. Attribute-oriented/attribute-based access control (AOBAC) records approximately 185 ms of response time because it requires extra time to evaluate multiple real-time user attributes. RBAC reveals an extended response duration at 210 ms because its static role-based approval procedure demonstrates reduced performance in complex access situations. The proposed model exhibits a 190 ms response time, which ranks behind the proposed model yet surpasses the response of MAC between RBAC and the proposed model. The proposed model achieves a response time 90 ms faster than RBAC while maintaining high accuracy and efficiency. The system proves useful for real-time medical data access systems because it combines quick execution with high precision for these time-sensitive environments.

Figure 4 consists of a comparative evaluation between throughput rates (in transactions per second) of four access control models, namely Proposed Model, ABAC, RBAC, and MAC applied to healthcare IoT systems. The Proposed Model beats traditional access control mechanisms by delivering approximately 74 TPS as its maximum possible throughput. The model demonstrates excellent capability for processing a heavy number of access control transactions quickly because real-time healthcare applications need dependable and rapid data access.

Evaluation of various dynamic user attributes per access request reduces ABAC performance to 52 TPS, while its throughput remains higher than the 52 TPS of ABAC. The implementation of RBAC results in a throughput of about 47 TPS despite its conventional organizational structure because the hierarchical role evaluation methods slow down performance during high request periods. The throughput capability of MAC reaches approximately 50 TPS due to limitations in its static access regulations that prevent adaptable rules. The Proposed Model outperforms RBAC by producing more than 20 TPS, which demonstrates its high scalability effectiveness.

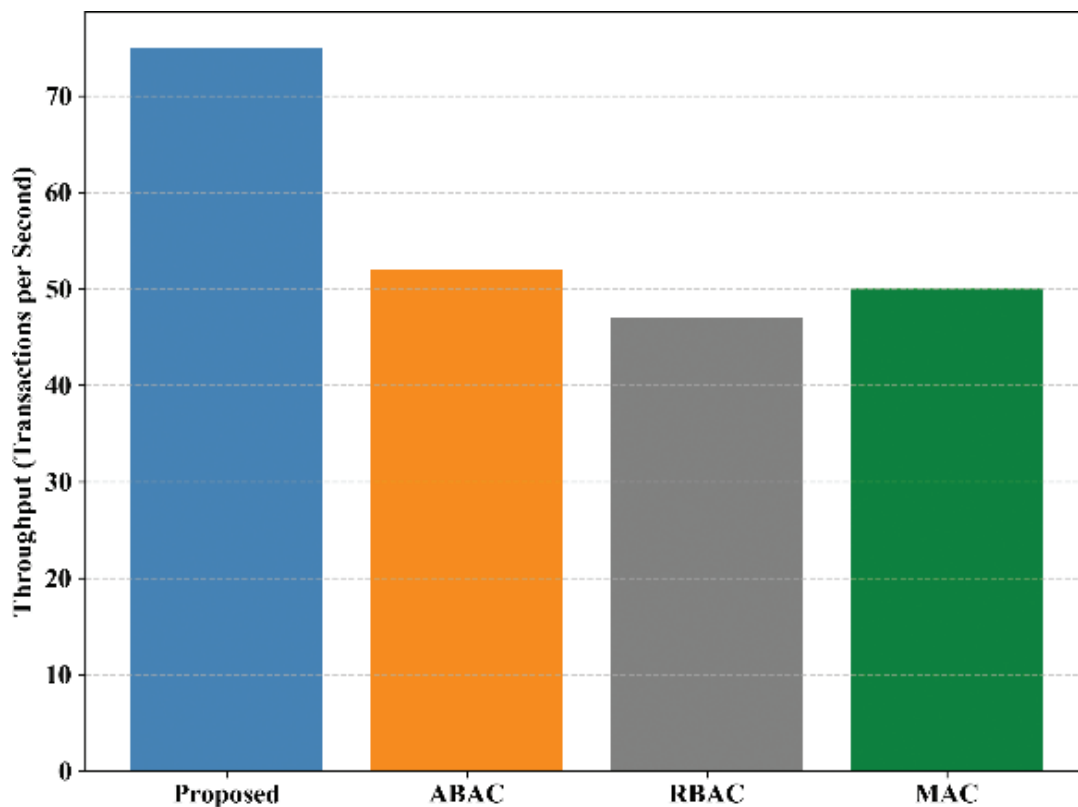


Figure 4: Throughput. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

The model's high-speed operation makes it suitable for deployment in busy healthcare data systems where it enables reliable combined data transactions and protected concurrent processing.

The cost comparison Figure 5 demonstrates that the proposed access control model has better economic efficiency than traditional methods. The proposed method proves economical by charging the lowest costs, which approach US\$2.1 because of its lightweight and optimized nature. The ABAC and MAC access control models bring about expenses totalling US\$3.8 while the RBAC necessitates a cost of about US\$4.1 yet the proposed model maintains the lowest cost of US\$2.1.

The traditional access systems face higher financial costs because their rigid permission mechanisms need increased computing resources together with substantial processing overhead requirements. The substantial decrease in costs through the proposed model makes it suitable for healthcare IoT applications because they operate under critical resource constraints. The proposed approach brings forward implementation benefits due to its low operational costs and performance metrics.

Performance improvements can be linked to the combined use of RBAC and ABAC providing

both structure and contextuality for access control. The use of a blockchain, along with Immutable and Transparent records, increases scalability through IPFS, which greatly reduces data storage needs. Lightweight permissioned blockchain and leveraging an infrastructure storage of IPFS, the framework has optimized its energy consumption and long-term operational costs. Only storing hash values on the blockchain and offloading actual data to IPFS allows for reduced computational overhead, thereby lowering energy consumption. The use of smart contract automation minimizes manual interventions, thus improving cost efficiency. The observed low operational cost (US\$2.1) makes this framework feasible for continued usage in large-scale healthcare IoT applications.

Access control models generate their responses to healthcare IoT requests according to the latency analysis depicted in Figure 6. The proposed framework demonstrates an operational response duration of about 120 ms that indicates both rapid information processing and quick decision operations. Between RBAC and ABAC models the proposed framework achieves 210 ms latency, which exceeds ABAC at 185 ms and completes at 170 ms with MAC model latency.

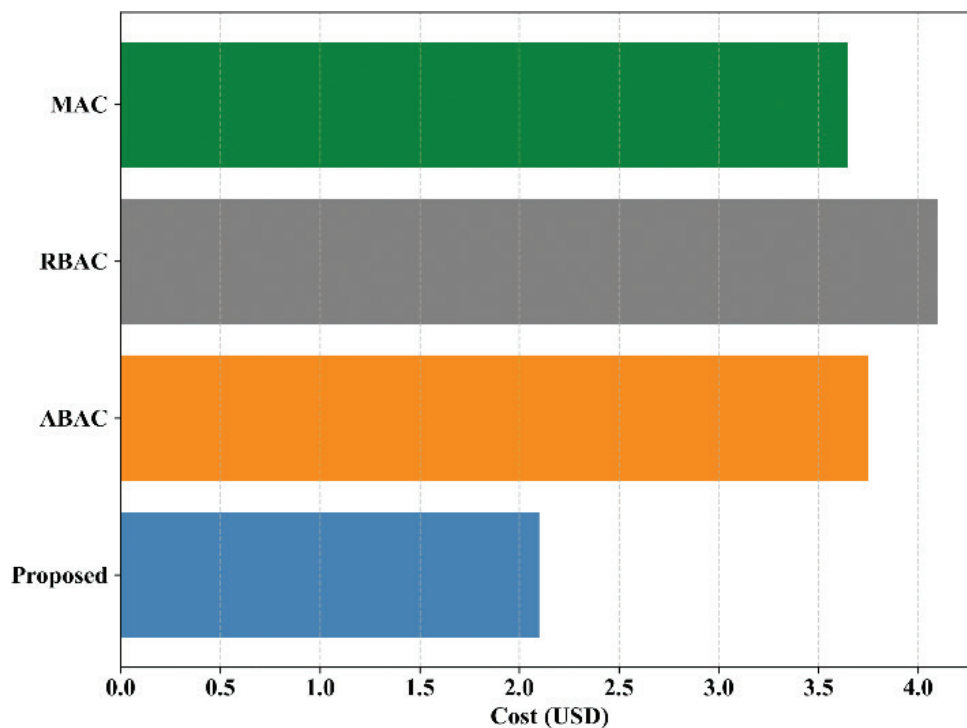


Figure 5: Cost utilization. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

Real-time access control operations from the proposed method outperform traditional methods according to recent testing results. Healthcare settings strongly need lower latency because quick access to data becomes essential for optimal patient outcomes. Reduced time delays in this proposed solution demonstrate its compatibility with time-sensitive IoT applications that require strict security requirements.

The proposed framework's memory usage analysis Figure 7 in the chart shows an extensive comparison against current models, including ABAC, RBAC, and MAC.

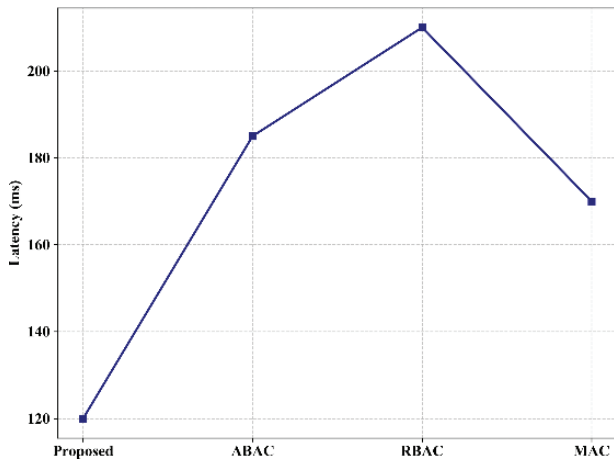


Figure 6: Latency validation. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

and MAC, throughout five essential components, which are Authentication, Authorization, Access Control, Audit Logging, and Encryption. The memory requirements of IoT-based healthcare systems play a crucial role since these medical devices need small computing power as well as minimal storage capacity.

The proposed system requires 45 MB for Authentication operations while using less memory compared to 60 MB for ABAC, 68 MB for RBAC, and 55 MB for MAC. Under Authorization the suggested system requires 50 MB, yet ABAC demands 65 MB, RBAC consumes 72 MB, and MAC requires 57 MB. The proposed system in the Access Control module demonstrates a memory usage of 48 MB, which surpasses the memory requirements of ABAC (62 MB), RBAC (69 MB), and MAC (56 MB).

The proposed system maintains efficient utilization in Audit Logging components since its usage stands at only 52 MB and surpasses its counterparts' resource needs - ABAC at 68 MB and RBAC at 75 MB and the slightly lower 60 MB requirement of MAC. The final Encryption module of the proposed framework requires 49 MB of memory, which proves more efficient than 64 MB for ABAC and 73 MB for RBAC and 59 MB for MAC. The proposed framework demonstrates superior memory optimization by using between 45 MB and 52 MB of memory storage across its entire components.

The memory usage for ABAC stands between 60 MB and 68 MB, while MAC uses 55–60 MB, but RBAC requires the highest amount, ranging from 68 MB to 75 MB. The high memory reduction

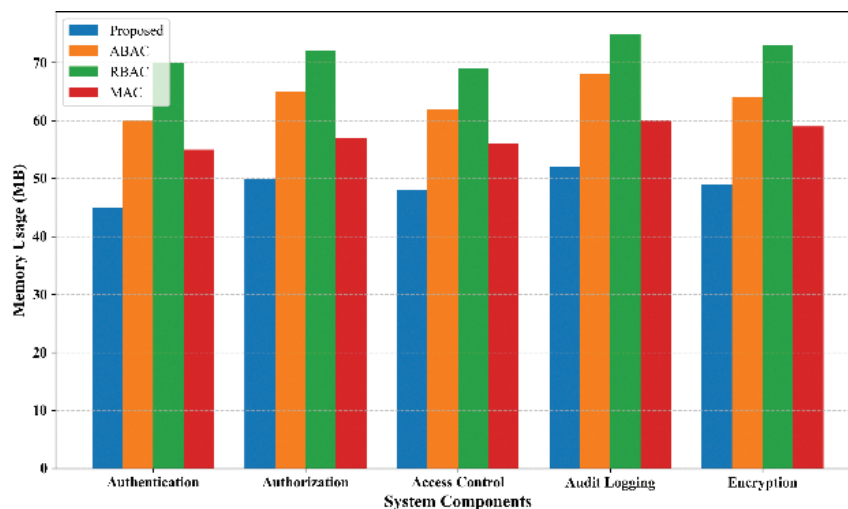


Figure 7: Memory utilization. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

capabilities of this proposed framework indicate its optimal deployment condition for resource-limited IoT-based healthcare setups. The efficient use of memory resources leads to quicker system performance and decreases hardware stress while extending the device operational life. All these elements are vital for monitoring health in real time. The memory-efficient configuration enables reliable device operation and reliable performance of portable medical IoT devices needed for critical Healthcare needs.

In addition to performance evaluation, the proposed framework is analyzed against diverse security threats to assess its robustness and reliability. The system demonstrates strong resistance to common attacks, including Sybil attacks, denial-of-service/distributed denial-of-service (DoS/DDoS) attacks, man-in-the-middle attacks, and unauthorized access. The use of a permissioned blockchain ensures data immutability and prevents malicious modification of records. Smart contracts enforce strict access control policies, thereby restricting unauthorized access attempts. Furthermore, data stored in IPFS is protected through cryptographic hashing, ensuring data integrity and confidentiality. These mechanisms collectively enhance the robustness and reliability of the framework in healthcare IoT environments.

The benefits of the proposed framework include the ability to scale well, provide for the security of decentralized data, and have low operating costs. There are a few limitations associated with the

research. The research relied on only simulation evaluations (not actual deployments in the real world). Since there is additional overhead associated with blockchains, performance issues may occur when deploying in a large-scale environment (where many transactions happen simultaneously).

Figure 8 demonstrates the responsiveness range of the proposed blockchain-enabled data-sharing framework relative to ABAC, RBAC, and MAC while monitoring user numbers from 100 to 10,000. The proposed framework tracks response time performance efficiently because it grows steadily between 110 ms at 100 users and 220 ms at 10,000 users. The data indicates that this system shows strong capabilities to handle demanding high-load situations.

RBAC demonstrates the greatest decline in performance since its response time elevates from 135 ms to 380 ms during the assessment period. The evaluation period of ABAC spans from 130 ms to 360 ms, showing a substantial increase and lower efficiency when loads intensify. The response times of MAC (125–330 ms) exceed those of ABAC and RBAC (98–350 ms) during all measurement points. The test results show that this proposed model provides better scalability as well as optimized performance when operating at high concurrency levels. Its ability to keep operating efficiently with many users makes the framework suitable for real-time healthcare IoT data-sharing applications that need fast response times.

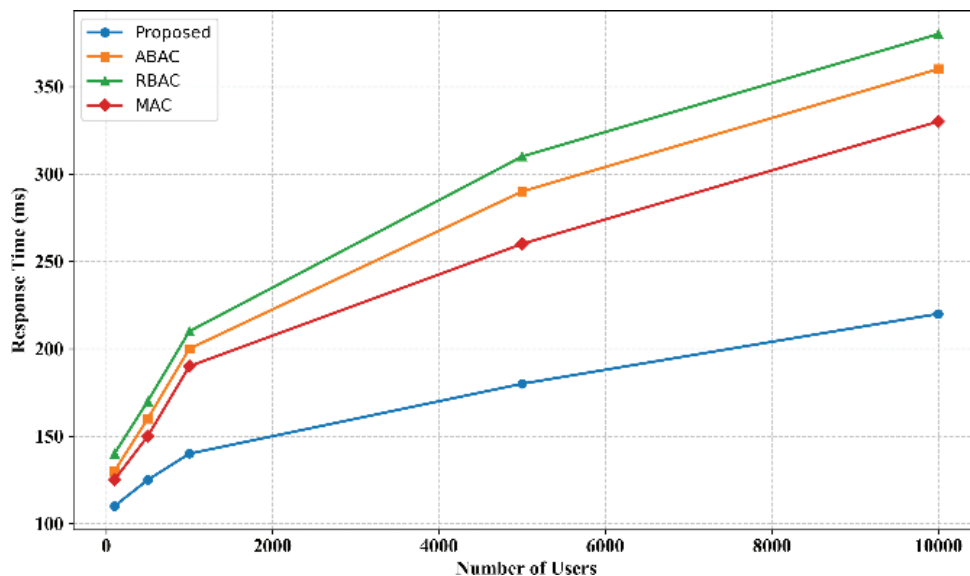


Figure 8: Response time versus number of users illustrating sensitivity of the system to varying workload. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

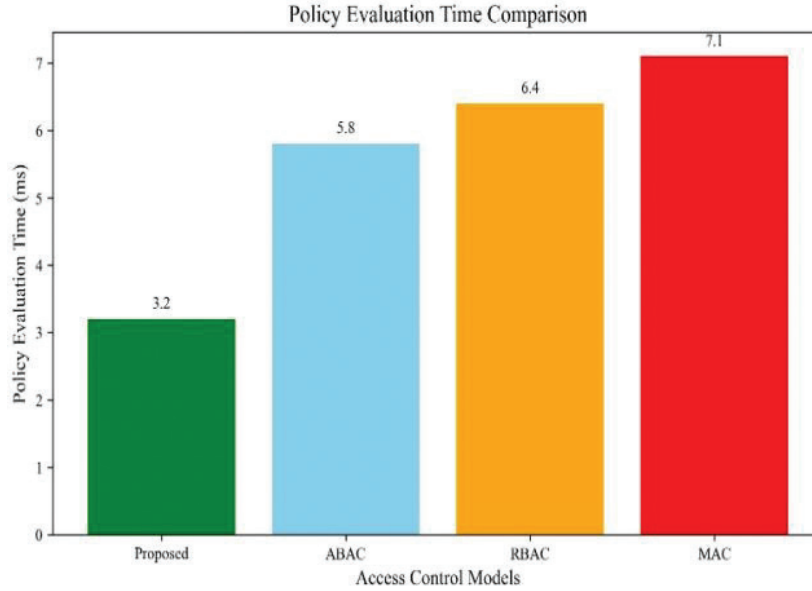


Figure 9: Policy evaluation time. ABAC, attribute-based access control; MAC, mandatory access control; RBAC, role-based access control.

According to the performed sensitivity analysis, increasing the number of users has a direct effect on the amount of time it takes for the system to respond. This confirms that the system is scalable. The complexity of attributes has very little impact on how quickly the system evaluates, and the throughput of the system does not change during this test phase. Thus, this confirms that the proposed framework is robust. The proposed framework scales based on user load (100–10,000 users). The results show that as user volume increases, response time increases at a controlled pace, demonstrating both stability and scalability. Furthermore, blockchain and IPFS reduce the need for storage, while smart contracts enable efficient management of access rights. Consequently, the proposed framework is capable of supporting large healthcare systems that distribute multiple institutions and high data volumes.

The access control models proposed together with ABAC, RBAC, and MAC undergo a comparative analysis in Figure 9 for evaluation time testing. According to the graph data shows that the proposed model performs best since it takes only 3.2 ms to complete policy evaluation. Rapid decision-making in access rights verification becomes feasible through an optimized mechanism in the proposed method due to critical needs in real-time applications and extensive systems. The evaluation times from the ABAC and RBAC models amount to 5.8 and 6.4 ms, respectively, demonstrating complex rule-checking

performance compared to the proposed method. The hierarchical access structure of MAC leads to its longest evaluation time reaching 7.1 ms while the system performs multiple static checks.

The access policy evaluation system offers swift and responsive evaluation services that optimize critical operational scenarios. This extended policy evaluation speed enhances system performance together with scalability when operational conditions become busy. When referring to access evaluation operations, the proposed model decreases computational strain to generate improved performance with smoother usability for system users.

This performance assessment is based upon a premise of having both stable network conditions and trusted participants in the system. However, if these assumptions (e.g., network disruption, untrustworthy nodes) are violated, then this may affect the latency and throughput. Nevertheless, the framework proposed herein demonstrates resilience to what would be considered “typical” Healthcare IoT conditions.

V. Conclusion

The proposed framework enables secure data sharing in healthcare IoT using blockchain. The system implements a hybrid access control approach by uniting RBAC with ABAC capabilities to generate dynamic security solutions that control data privacy configurations.

The hybrid system enables detailed permission assignment through pre-defined user roles, as well as dynamic logical variables including device status, patient condition, and user location to deliver suitable healthcare data interaction methods. Smart contracts automate policies within a system that stores decentralised data on the IPFS network to deliver secure, detail-oriented data handling capabilities. Through performance testing, the proposed system validated better security features and real-time adaptability with scalability capabilities than RBAC, ABAC, and MAC systems. Implementing the healthcare framework through Python programming and system configuration tools proves practical because it fulfills the operational needs of healthcare facilities.

The model prevents unauthorized access, ensures data integrity, and protects against common attacks in addition to internal malicious behaviors through its unalterable audit track combined with rigorous policy enforcement. The research establishes safe healthcare platforms by implementing protected role-based data access functionalities for decentralized networks, which will result in future improvements to care services, operational management, and data administration.

The proposed framework is very promising in terms of secure and efficient sharing of data related to IoT in healthcare settings, but the next steps involve implementing the framework in practice, finding ways to improve the performance of the underlying blockchain system, and integrating the framework with next-generation technologies (such as artificial intelligence) to provide intelligent access control. The framework has not only been validated by simulation, but also has a design that allows for its practical use in today's healthcare environment. The addition of Blockchain, Smart Contracts, and IPFS allows the Framework to integrate with current healthcare IT systems; hence can be implemented securely and at scale. The next step is to deploy and test the system in clinical settings, which will allow for further validation of the system's performance, interoperability, and usability under normal conditions.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Data Availability

The data that support the findings of this study are not publicly available due to confidentiality agreements but are available from the corresponding author upon reasonable request.

Code Availability

Not applicable.

Authors' Contributions

Qi Jing designed the research framework, analyzed performance, validated the results, and wrote the manuscript. Collected the required information for the framework, developed and provided the software, conducted the critical review, and managed the project.

References

- Abasaheb, J. P., & Mallapur, S. V. (2025). Blockchain-integrated secure healthcare information sharing via advanced Blowfish encryption standard with optimal key generation. *Transactions on Emerging Telecommunications Technologies*, 36(3), e70077. DOI: 10.1002/ett.70077
- Abdellatif, A. A., Shaban, K., & Massoud, A. (2025). Blockchain-enabled distributed learning for enhanced smart grid security and efficiency. *Computers and Electrical Engineering*, 123, 110012. DOI: 10.1016/j.compeleceng.2024.110012
- Ahad, M. T., Morshed, M. M., Atkins, A. S., & Yu, H. (2025). An IoT-enabled blockchain system to secure medical data. In *Digital twin, blockchain, and sensor networks in the healthy and mobile city* (pp. 121–146). Elsevier.
- Ahmed, I., Syed, M. A., Maaruf, M., & Khalid, M. (2025). Distributed computing in multi-agent systems: A survey of decentralized machine learning approaches. *Computing*, 107(1), 2. DOI: 10.1007/s00607-024-01356-0
- Bagchi, P., Bisht, A., Das, A. K., Saxena, N., & Hossain, M. S. (2025). Designing quantum-safe lattice-based multi-authority CP-ABE scheme for blockchain-enabled IoT-based consumer healthcare electronics. *IEEE Transactions on Consumer Electronics*. DOI: 10.1109/TCE.2025.3552021
- Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., & Moosavi, S. R. (2023). A lightweight blockchain and fog-enabled secure remote

patient monitoring system. *Internet of Things*, 22, 100691. DOI: 10.1016/j.iot.2023.100691

Erukala, S. B., Tokmakov, D., Perumalla, A., Kaluri, R., Bekyarova-Tokmakova, A., Mileva, N., & Lubomirov, S. (2025). A secure end-to-end communication framework for cooperative IoT networks using hybrid blockchain system. *Scientific Reports*, 15(1), 11077. DOI: 10.1038/s41598-025-96002-w

Greco, A., Saggese, A., Sansone, C., & Vento, B. (2025). An experimental evaluation of smart sensors for pedestrian attribute recognition using multi-task learning and vision language models. *Sensors*, 25(6), 1736. DOI: 10.3390/s25061736

Harish, M., Sharma, I., Singh, M., Gupta, A., Asad, M., & Saxena, R. (2025). An IoT-based blockchain-enabled secure storage for healthcare systems. In *Explainable IoT applications: A demystification* (pp. 99–113). Springer Nature Switzerland. DOI: 10.1007/978-3-031-59432-8_6

Hassan, S. A. D. H., Rasheed, A. A., Mousa, A. A., Hussein, Z. A., & Ambudkar, B. (2025). *The rising cost of cyberattacks: Trends and impacts across industries*. *HighTech and Innovation Journal*, 6(2), 524–536. DOI: 10.28991/HIJ-2025-06-02-011

Hoonsopon, D., Ketkaew, C., Puriwat, W., Viriyasitavat, W., & Tripopsakul, S. (2025). The impact of self-efficacy on telemedicine adoption in emerging country. *HighTech and Innovation Journal*, 6(1), 123–134. DOI: 10.28991/HIJ-2025-06-01-09

Kabra, S., Sharma, S., & Sachdeva, M. (2025). Blockchain: A new frontier in secure patient data management. In *Blockchain-enabled solutions for the pharmaceutical industry* (pp. 319–334). DOI: 10.1002/9781394287970.ch15

Khan, A. A., Laghari, A. A., Baqasah, A. M., Bacarra, R., Alroobaea, R., Alsafyani, M., & Alsayaydeh, J. A. J. (2025). BDLT-IoMT—a novel architecture: SVM machine learning for robust and secure data processing in Internet of Medical Things with blockchain cybersecurity. *The Journal of Supercomputing*, 81(1), 1–22. DOI: 10.1007/s11227-024-06782-7

Khan, S., Khan, M., Khan, M. A., Khan, M. A., Wang, L., & Wu, K. (2025). A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. *IEEE Journal of Biomedical and Health Informatics*. DOI: 10.1109/JBHI.2025.3538623

Kulkarni, D. Y. R., Sugave, D. S., Jagdale, D. B., & Gutte, V. (2025). Spinal PMDMNN: A new blockchain-based IoT network for healthcare classification. *Australian Journal of Electrical and Electronics Engineering*, 1–15. DOI: 10.1080/1448837X.2025.2451566

Lakshmi, S. M., Malathi, M., & Mythili, K. (2025). Blockchain-enabled security for smart medicine vending

machines handling expired medications. In *Blockchain-enabled solutions for the pharmaceutical industry* (pp. 189–206). DOI: 10.1002/9781394287970.ch10

Li, M., Harish, A. R., Yu, C., Yu, Y., Zhong, R. Y., & Huang, G. Q. (2025). Blockchain-based medical data asset sharing framework for healthcare 4.0. *IEEE Transactions on Industrial Informatics*. DOI: 10.1109/TII.2024.3488795

Mazhar, T., Khan, S., Shahzad, T., Khan, M. A., Saeed, M. M., Awotunde, J. B., & Hamam, H. (2025). Generative AI, IoT, and blockchain in healthcare: Application, issues, and solutions. *Discover Internet of Things*, 5(1), 5. DOI: 10.1007/s43926-025-00095-8

Mazid, A., Kirmani, S., Abid, M., & Pawar, V. (2025). A secure and efficient framework for Internet of Medical Things through blockchain-driven customized federated learning. *Cluster Computing*, 28(4), 225. DOI: 10.1007/s10586-024-04896-4

Mehla, R., Garg, R., & Khan, M. A. (2025). Privacy-preserving solution for data sharing in IoT-based smart consumer electronic devices for healthcare. *IEEE Transactions on Consumer Electronics*. DOI: 10.1109/TCE.2025.3540642

Meisami, S., Meisami, S., Yousefi, M., & Aref, M. R. (2023). Combining blockchain and IoT for decentralized healthcare data management. *arXiv preprint*. DOI: 10.48550/arXiv.2304.00127

Mishra, D. P., Rajeev, B., Mallick, S. R., Lenka, R. K., & Salkuti, S. R. (2025). Efficient blockchain-based solution for secure medical record management. *International Journal of Information and Communication Technology*, 14(1), 59–67. <https://doi.org/10.11591/ijict.v14i1.pp59-67>

Mohanta, B. K., Awad, A. I., Dehury, M. K., Mohapatra, H., & Khan, M. K. (2025). Protecting IoT-enabled healthcare data at the edge: Integrating blockchain, AES, and off-chain decentralized storage. *IEEE Internet of Things Journal*. DOI: 10.1109/JIOT.2025.3528894

Nassa, V. K., Santhakumar, G., Kanwer, B., Kumar, N. K., Kumar, B., & Prasad, C. R. (2025). Blockchain-Enabled Secure Data Sharing and Communication in IoT Networks. In *Interdisciplinary Approaches to AI, Internet of Everything, and Machine Learning* (pp. 131–142). IGI Global Scientific Publishing.

Pandey, S., Chaudhary, M., & Tóth, Z. (2025). An investigation on real-time insights: Enhancing process control with IoT-enabled sensor networks. *Discover Internet of Things*, 5, 29. DOI: 10.1007/s43926-025-00124-6

Prajapat, S., Kumar, P., Das, A. K., & Muhammad, G. (2025). Generative AI-Enabled Quantum Encryption

Algorithm for Securing IoT-Based Healthcare Application Using Blockchain. *IEEE Internet of Things Journal*.

Rastogi, H., Tripathi, A. N., & Sharma, B. (2025). Blockchain Technology for Securing Healthcare Data in Cyber-Physical Systems. *Artificial Intelligence and Cybersecurity in Healthcare*, 85–112.

Rizzardi, A., Sicari, S., & Coen-Porisini, A. (2024). IoT-driven blockchain to manage the healthcare supply chain and protect medical records. *Future Generation Computer Systems*, 161, 415–431.

Roy, P., Sherazi, S. H. T., Delda, M. J. M., Maqsood, M., & Ahmad, M. (2025). Secure Data Sharing in Healthcare: A Blockchain and Digital Twins Approach. In *Digital Twins for Sustainable Healthcare in the Metaverse* (pp. 255–286). IGI Global Scientific Publishing.

Sahu, N., & Karthikeyan, I. (2024). Secure Privacy-preserving Resolution Adaptive Data Sharing in Hybrid Blockchain Controlled Medical IOT Environment. *International Journal of Intelligent Engineering & Systems*, 18(1).

Sarojini Karuppusamy, G., & Kumar, S. M. (2025). TwoFish-Integrated Blockchain for Secure and Optimized Healthcare Data Processing in IoT-Edge-Cloud System. *Transactions on Emerging Telecommunications Technologies*, 36(3), e70076.

Tang, Y., Wang, K., Niyato, D., Li, J., Dobre, O. A., & Duong, T. Q. (2025). Secure Data Sharing and Prediction with Digital Twin and Blockchain in Healthcare. *IEEE Communications Magazine*.

Tlemçani, K., Azbeg, K., Saoudi, E., Fetjah, L., Ouchetto, O., & Andaloussi, S. J. (2025). Empowering Diabetes Management through Blockchain and Edge

Computing: A Systematic Review of Healthcare Innovations and Challenges. *IEEE Access*.

Venice, J. A., Vettriselvan, R., Rajesh, D., Xavier, P., & Shanthi, H. J. (2025). Optimizing Performance Metrics in Blockchain-Enabled AI/ML Data Analytics: Assessing Cognitive IoT. In *Enhancing Automated Decision-Making Through AI* (pp. 97–122). IGI Global Scientific Publishing.

Verma, G., & Yadav, S. (2025). Blockchain for management of healthcare data. In *Blockchain and Digital Twin for Smart Healthcare* (pp. 419–437). Elsevier.

Vinayasree, P., & Reddy, A. M. (2025). A Reliable and Secure Permissioned Blockchain-Assisted Data Transfer Mechanism in Healthcare-Based Cyber-Physical Systems. *Concurrency and Computation: Practice and Experience*, 37(3), e8378.

Vinnarasi, A. P., & Dayana, R. (2025). OSL-ABE: an optimal secure and lightweight attribute-based encryption method for blockchain-enabled IoT-based healthcare systems. *Neural Computing and Applications*, 37(1), 123–148.

Whig, P., Sharma, R., Yathiraju, N., Jain, A., & Sharma, S. (2024). Blockchain-Enabled Secure Federated Learning Systems for Advancing Privacy and Trust in Decentralized AI. *Model Optimization Methods for Efficient and Edge AI: Federated Learning Architectures, Frameworks and Applications*, 321–340.

Zhao, F., Yang, B., Su, Z., Li, C., & Ding, Y. (2025). A blockchain-enabled privacy-preserving and incentive mechanism-driven federated learning scheme for IoV. *Computer Networks*, 111262.