International Journal of Engineering, Science and Information Technology
Volume 5 No. 2 (2025) pp. 572-579
ISSN 2775-2674 (online)
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i2.1520
Research Paper, Short Communication, Review, Technical Paper

Blockchain-Enabled Secure Data Sharing Framework for Healthcare IoT Devices

Qi Jing

University of Arizona, Arizona, United States

**Corresponding author Email: jinglegege@gmail.com*

The manuscript was received on 25 November 2024, revised on 11 January 2025, and accepted on 10 April 2025, date of publication 23 May 2025

Abstract

Medical data security challenges have increased dramatically because healthcare institutions continue to integrate more Internet of Things devices to deliver data-driven clinical services. Access control systems based on RBAC, ABAC and MAC do not meet the requirements of flexible protection and scalable and context-aware security which are needed for dynamic healthcare environments. The research objective focuses on creating a resilient decentralized access control solution which delivers secure time-sensitive access permissions in healthcare IoT systems. A blockchain-based hybrid access control framework with RBAC and ABAC provides the solution to meet this requirement. A dual mechanism of smart contracts and IPFS storage runs the model while variables and user-facing elements shift based on environmental characteristics and individual circumstances. Results from experimental evaluation show that this proposed framework delivers 96.5% access precision together with policy evaluation times below 3.2 ms and 120 ms response times while handling 74 transactions per second while remaining affordable at $2.1 and demanding 45 to 52 MB from critical system memory. The obtained results demonstrate better scalability together with enhanced performance and adaptability when compared to using ABAC, RBAC and MAC singularly. Healthcare IoT systems should implement a blockchain-based hybrid access control system as an optimal method to secure data sharing in real-time resource-constrained scenarios.

Keywords: *Blockchain, Internet of Things, Access Control, Healthcare Data Security, Smart Contracts.*

1. Introduction

The healthcare industry implemented IoT technology to make transformative changes for provider monitoring of patients at distant facilities and offer enhanced medical care through smart devices [1][3]. 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 [2]. Advanced medical technology has created healthcare security issues and privacy and access control problems according to research [4].

Advanced medical data privacy calls for rapid defense actions to stop unauthorized personnel entrance while simultaneously blocking data misuse and tampering by internal staff through devices ([5]. Two essential reasons exist for healthcare systems to implement information access controls through patient data privacy protection together with operational healthcare security establishment[6].

The conventional data sharing methods in healthcare industry rely on centralized systems that result in failure points and restricted visibility together with restricted expansion possibilities [7][8].

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 [9]These centralized systems fail to deliver adequate visibility into data access events since they lack transparency regarding when and how users access healthcare data and by whom access occurs [10].

The increasing adoption of blockchain technology aims to solve the existing limitations in healthcare security [11][12].

Blockchain provides three essential properties of decentralization and encryption and automated smart contracts that construct a modern system for trustworthy secure data sharing [13]. The infrastructure-based deployment of control functions and policy enforcement through blockchain technology provides healthcare organizations with a trustworthy method to share data[14].

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. System administrators achieve operational cost reduction while simultaneously receiving better system security and privacy features through this method.

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 to grant 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.

2. Literature Review

Academic teams worldwide have conducted investigations about healthcare data security through the implementation of IoT and blockchain technologies since 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 Role-Based Access Control (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.

Table 1. Research gap validation

Author(s)	Techniques Involved	Advantages	Disadvantages
Ahmed, I., 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, T., et al.,(2025)	Blockchain + AI + IoT hybrid architecture	Data ownership, interoperability, tamper resistance	Integration complexity, energy use, regulatory issues
Meisami, S., et al., (2023)	Lightweight blockchain with privacy-preserving access control	Transparency, low cost, patient-centric access	Scalability, performance in large systems
Cheikhrouhou, O., 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, A., et al., (2024)	Hyperledger Fabric for supply chain and medical record security	Supply chain transparency, data integrity, secure sharing	High setup cost, complex deployment

Ahmedet al. [15] research investigated 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 were enabled through this technique. The medical records experienced 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.
Mazharet al. [16] studied blockchain operations between AI and IoT technologies to develop secure intelligent medical systems ecosystems. The authors created a united system structure which uses blockchain technology to handle dispersed healthcare 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. [17] created a blockchain protocol which focuses on e-health environments to support free medical data access without third-party intervention. The system incorporated 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.
Cheikhrouhou, et al. [18] 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 that 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 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.
Rizzardiet al. [19] 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 which provided secure traceable and efficient data sharing capabilities for stakeholders. The implementation of this approach enabled better visibility into supply chains and lower levels of fraud and secured data from tampering attempts. The study emphasized two key constraints which researchers

encountered while implementing enterprise-grade blockchain solutions due to high setup expenses and complex learning process requirements.

3. Methods

A hybrid access control strategy serves medical data exchange requirements in Internet of Things platforms through the proposed framework. The proposed method creates an access control system which integrates role-based and attribute-based access management. 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 and device status and location information.
The proposed method for this study provides baseline access permissions which support fundamental access control related to professional duties for roles including patients and both nurses and doctors. These strategies embedded in smart contracts enable the architecture to handle IoT system scalability along with automatic access control adaptations based on present scenarios and user features. Figure 1 shows the suggested architecture.

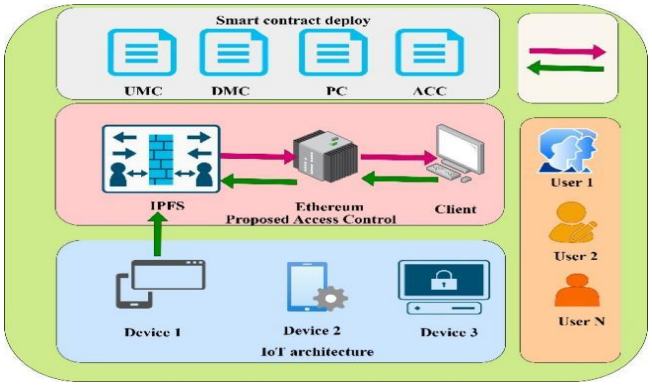

Fig 1. Proposed architecture with data access control

The proposed architecture consists of two essential elements - blockchain-based Interplanetary File System (IPFS) serves as storage and implements different types of smart contracts on decentralized Internet of Things 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 and 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 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.

3.1. 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 nonfunctional when external attackers send numerous requests through denial of service and distributed denial of service 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 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 [20].
The proposed design addresses four security threats which include sybil attacks and denial of service attacks together with data integrity attacks and unauthorized data access attacks [21][22] Secure access management in IoT architecture demands the implementation of assumptions as a basis for the recommended design [24]. 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 [25][26]. The system design assumes two principles: attackers do not have enough computing strength to decode standard cryptographic algorithms and attackers can detect all system communications [27].

3.2. User management contract (UMC)

In the IoT architecture, 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 [28] Each user in the architecture requires a specific identification which is generated through the hash function [29]. The implementation combines user primary attributes with department information and role access and address details and username text to create cryptographic hash value which establishes a secure and individual userID that resolves detection issues for single users throughout the complete architecture [30].
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 automatically produces a new entry with a special userID in the system [31]. 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[32]. 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 client enables administrators and users to both register users and acquire unique userID[33].

3.3. 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 which 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 datatype information alongside IPFSCID [34]. 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 [35]. During the encryption process the internal 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 [36].

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 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[37].

3.4. 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 (1), (2), (3);

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

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

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

Here, $u\epsilon U$, $p\epsilon P, r\epsilon R$, 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 and r for role and p for requested resource parameters. Using Access (u, Nurse, Nursing Record) a nurse service provider obtains access to departmental nursing records, yet patients use Access to view their personal medical data [38].

The Internet of Things requires access control as a systematic process which verifies users and their permission levels to guarantee safe data access. When an operation starts the login User 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 get User function. The system validates permissions through the PC's has Access function ensuring that user department and role comply with data access requirements. Users authorized by ACC can access specified data from MDMC through the access Data By Owner function along with the user authorization [39].

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 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 [40].

4. Results and Discussion

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 Mandatory Access Control (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 of a system that contained an Intel i7 processor, 16GB RAM and Ubuntu 20.04 OS 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.

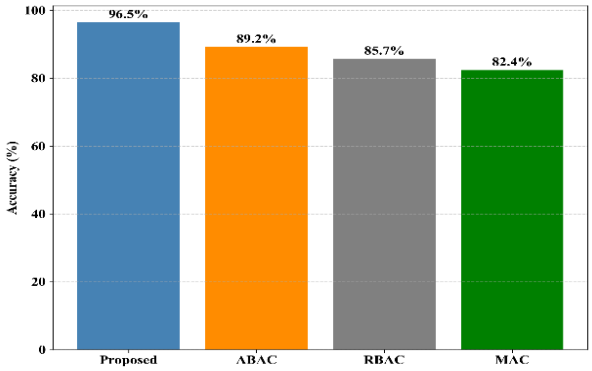

Fig 2. Accuracy

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 yields outstanding results when both role-based and attribute-based controls are simultaneously integrated into a context-aware framework by surpassing traditional approaches 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 role-based access control.

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 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.

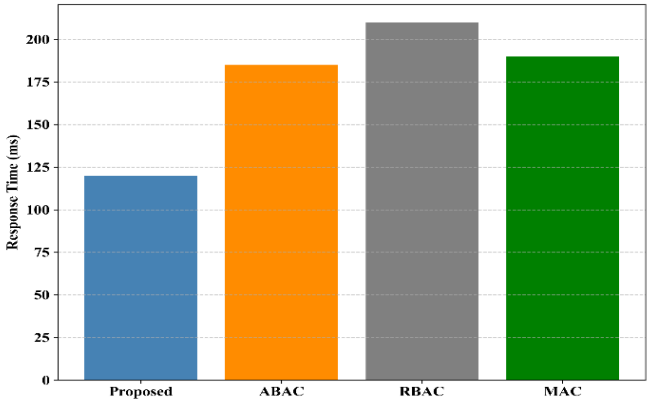

Fig 3. Response time

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 operations. The proposed hybrid model shows maximum operational efficiency because its response time reaches approximately 120 milliseconds 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. 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 reaches a response time of 90 ms faster than RBAC while maintaining a well-balanced accuracy and efficiency equilibrium. The system proves useful for real-time medical data access systems because it combines quick execution with high precision for these time-sensitive environments.

The 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 transactions per second 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.

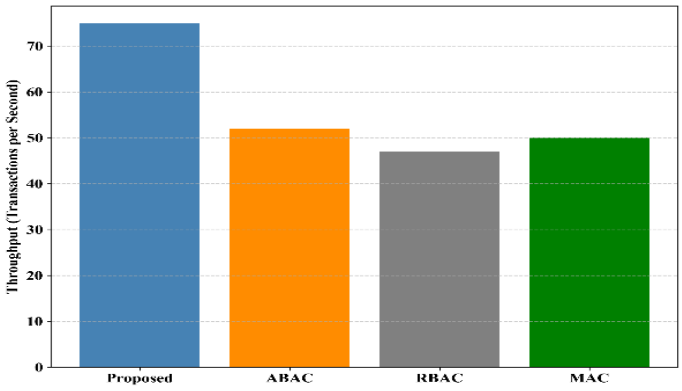

Fig 4. Throughput

Evaluation of various dynamic user attributes per access request reduces ABAC performance to 52 transactions per second while its throughput remains higher than the 52 transactions per second of ABAC. The implementation of RBAC results in a throughput of about 47 transactions per second 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 transactions per second due to limitations in its static access regulations that prevent adaptable rules. The Proposed Model outperforms RBAC by producing more than 20 transactions per second which demonstrates its high scalability effectiveness. 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.

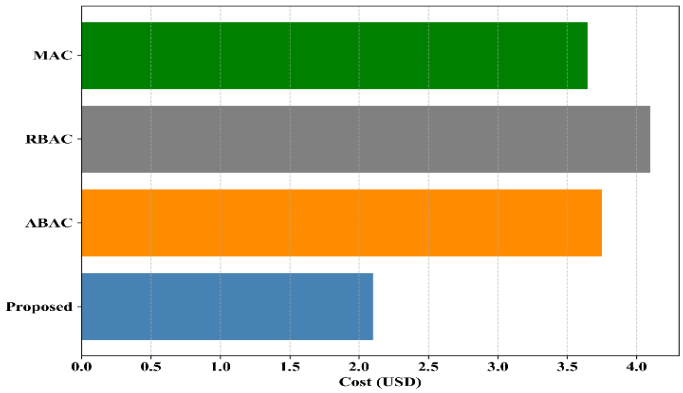

Fig 5. Cost utilization

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 $2.1 because of its lightweight and optimized nature. The ABAC and MAC access control models bring about expenses totalling $3.8 while the RBAC necessitates a cost of about $4.1 yet the proposed model maintains the lowest cost of $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.

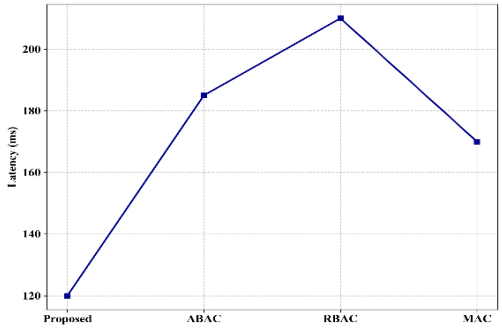

Fig 6. Latency validation

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 milliseconds 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.

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.

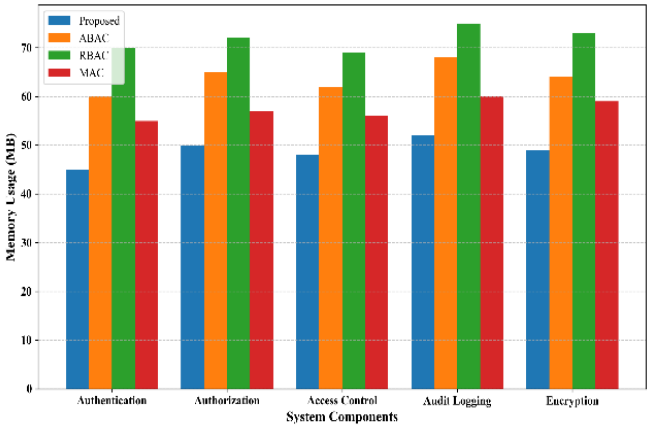

Fig 7. Memory utilization

The proposed framework's memory usage analysis figure 7 in the chart shows an extensive comparison against current models including ABAC, RBAC, 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 and 68 MB for RBAC and 55 MB for MAC. Under Authorization the suggested system requires 50 MB yet ABAC demands 65 MB and 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 to 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 MB to 60 MB but RBAC requires the highest amount ranging from 68 MB to 75 MB. The high memory reduction 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.

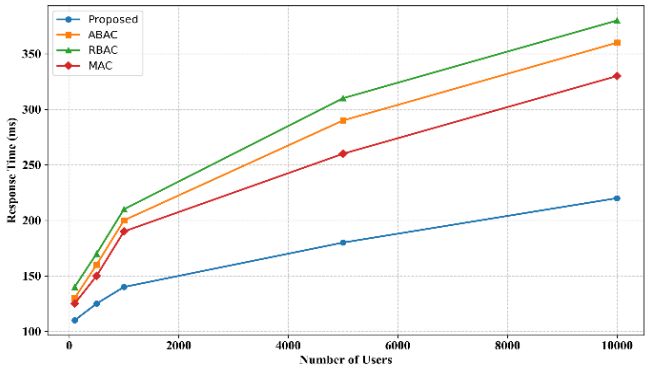

Fig 8. Response time vs number of users

Figure 8 demonstrates the responsiveness range of the proposed blockchain-enabled data-sharing framework relative to ABAC and 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 to 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 milliseconds until 360 milliseconds showing substantial increase and lower

efficiency when loads intensify. The response times of MAC (125 to 330 ms) exceed those of ABAC and RBAC (98 to 350 ms) during all measurement points. The test results exhibit 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.

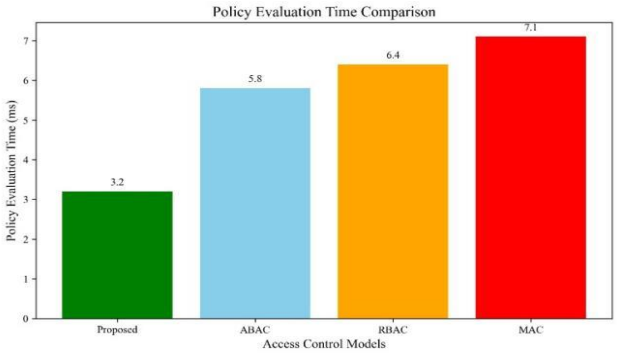

Fig 9. Policy Evaluation Time

The access control models Proposed together with ABAC, RBAC and MAC undergo a comparative analysis under Figure 9 for evaluation time testing. According to the graph data shows that the Proposed model performs best since it takes only 3.2 milliseconds 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 milliseconds and 6.4 milliseconds 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 performing 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.

5. Conclusion

The developed framework utilizes blockchain technology to establish secure data sharing for healthcare IoT environments. The system implements a hybrid access control approach by uniting RBAC with ABAC capabilities to generate dynamic security solutions which control data privacy configurations.

The hybrid system enables detailed permission assignment through pre-defined user roles besides dynamic logical variables including device status and 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 operational needs of healthcare facilities.

This model blocks unauthorized access and defense security breaches of data integrity while preventing denial-of-service 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 and operational management and data administration.

References

[1] J. P. Abasaheb and S. V. Mallapur, “Blockchain-integrated secure healthcare information sharing via advanced Blowfish encryption standard with optimal key generation,” *Trans. Emerg. Telecommun. Technol.*, vol. 36, no. 3, e70077, 2025.

[2] A. A. Abdellatif, K. Shaban, and A. Massoud, “Blockchain-enabled distributed learning for enhanced smart grid security and efficiency,” *Comput. Electr. Eng.*, vol. 123, p. 110012, 2025.

[3] M. T. Ahad, M. M. Morshed, A. S. Atkins, and H. Yu, “An IoT-enabled blockchain system to secure medical data,” in *Digital Twin, Blockchain, and Sensor Networks in the Healthy and Mobile City*. Amsterdam, The Netherlands: Elsevier, 2025, pp. 121–146.

[4] M. Mejail, B. K. Nestares, and L. Gravano, “The evolution of telecommunications: Analog to digital,” *Prog. Electron. Commun. Eng.*, vol. 2, no. 1, pp. 16–26, 2024, doi: 10.31838/PECE/02.01.02.

[5] I. Ahmed, M. A. Syed, M. Maaruf, and M. Khalid, “Distributed computing in multi-agent systems: A survey of decentralized machine learning approaches,” *Computing*, vol. 107, no. 1, p. 2, 2025.

[6] P. Bagchi, A. Bisht, A. K. Das, N. Saxena, and M. S. Hossain, “Designing quantum-safe lattice-based multi-authority CP-ABE scheme for blockchain-enabled IoT-based consumer healthcare electronics,” *IEEE Trans. Consum. Electron*., early access, 2025.

[7] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi, “A lightweight blockchain and fog-enabled secure remote patient monitoring system,” *Internet Things*, vol. 22, p. 100691, 2023.

[8] S. B. Erukala et al., “A secure end-to-end communication framework for cooperative IoT networks using hybrid blockchain system,” *Sci. Rep*., vol. 15, no. 1, p. 11077, 2025.

[9] M. Harish et al., "An IoT-based blockchain-enabled secure storage for healthcare systems," in *Explainable IoT Applications: A Demystification*. Cham, Switzerland: Springer Nature, 2025, pp. 99–113.
[10] K. Choset and J. Bindal, "Using FPGA-based embedded systems for accelerated data processing analysis," *SCCTS J. Embedded Syst. Des. Appl.*, vol. 2, no. 1, pp. 79–85, 2025.
[11] S. Kabra, S. Sharma, and M. Sachdeva, "Blockchain: A new frontier in secure patient data management," in *Blockchain-Enabled Solutions for the Pharmaceutical Industry*, 2025, pp. 319–334.
[12] A. A. Khan et al., "BDLT-IoMT—a novel architecture: SVM machine learning for robust and secure data processing in Internet of Medical Things with blockchain cybersecurity," *J. Supercomput.*, vol. 81, no. 1, pp. 1–22, 2025.
[13] S. Khan et al., "A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems," *IEEE J. Biomed. Health Inform.*, early access, 2025.
[14] A. James, W. Thomas, and B. Samuel, "IoT-enabled smart healthcare systems: Improvements to remote patient monitoring and diagnostics," *J. Wireless Sensor Netw. IoT*, vol. 2, no. 2, pp. 11–19, 2025.
[15] D. Y. R. Kulkarni, D. S. Sugave, D. B. Jagdale, and V. Gutte, "Spinal PMDMNN: A new blockchain-based IoT network for healthcare classification," *Aust. J. Electr. Electron. Eng.*, pp. 1–15, 2025.
[16] S. M. Lakshmi, M. Malathi, and K. Mythili, "Blockchain-enabled security for smart medicine vending machines handling expired medications," in *Blockchain-Enabled Solutions for the Pharmaceutical Industry*, 2025, pp. 189–206.
[17] M. Li et al., "Blockchain-based medical data asset sharing framework for healthcare 4.0," *IEEE Trans. Ind. Informat.*, early access, 2025.
[18] T. Mazhar et al., "Generative AI, IoT, and blockchain in healthcare: Application, issues, and solutions," *Discover Internet Things*, vol. 5, no. 1, p. 5, 2025.
[19] A. Mazid, S. Kirmani, M. Abid, and V. Pawar, "A secure and efficient framework for Internet of Medical Things through blockchain-driven customized federated learning," *Cluster Comput.*, vol. 28, no. 4, p. 225, 2025.
[20] K. P. Uvarajan, "Advances in quantum computing: Implications for engineering and science," *Innov. Rev. Eng. Sci.*, vol. 1, no. 1, pp. 21–24, 2024, doi: 10.31838/INES/01.01.05.
[21] R. Mehla, R. Garg, and M. A. Khan, "Privacy-preserving solution for data sharing in IoT-based smart consumer electronic devices for healthcare," *IEEE Trans. Consum. Electron.*, early access, 2025.
[22] S. Meisami, S. Meisami, M. Yousefi, and M. R. Aref, "Combining blockchain and IoT for decentralized healthcare data management," *arXiv:2304.00127*, 2023.
[23] D. P. Mishra, B. Rajeev, S. R. Mallick, R. K. Lenka, and S. R. Salkuti, "Efficient blockchain-based solution for secure medical record management," *Int. J. Inf. Commun. Technol.*, vol. 14, no. 1, pp. 59–67, 2025.
[24] B. K. Mohanta, A. I. Awad, M. K. Dehury, H. Mohapatra, and M. K. Khan, "Protecting IoT-enabled healthcare data at the edge: Integrating blockchain, AES, and off-chain decentralized storage," *IEEE Internet Things J.*, early access, 2025.
[25] V. K. Nassa et al., "Blockchain-enabled secure data sharing and communication in IoT networks," in *Interdisciplinary Approaches to AI, Internet of Everything, and Machine Learning*. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 131–142.
[26] S. Prajapat, P. Kumar, A. K. Das, and G. Muhammad, "Generative AI-enabled quantum encryption algorithm for securing IoT-based healthcare application using blockchain," *IEEE Internet Things J.*, early access, 2025.
[27] G. G. Bianchi and F. M. Rossi, "Reconfigurable computing platforms for bioinformatics applications," *SCCTS Trans. Reconfigurable Comput.*, vol. 2, no. 1, pp. 16–23, 2025.
[28] H. Rastogi, A. N. Tripathi, and B. Sharma, "Blockchain technology for securing healthcare data in cyber-physical systems," in *Artificial Intelligence and Cybersecurity in Healthcare*, 2025, pp. 85–112.
[29] A. Rizzardi, S. Sicari, and A. Coen-Porisini, "IoT-driven blockchain to manage the healthcare supply chain and protect medical records," *Future Gener. Comput. Syst.*, vol. 161, pp. 415–431, 2024.
[30] P. Roy, S. H. T. Sherazi, M. J. M. Delda, M. Maqsood, and M. Ahmad, "Secure data sharing in healthcare: A blockchain and digital twins approach," in *Digital Twins for Sustainable Healthcare in the Metaverse*. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 255–286.
[31] N. Sahu and I. Karthikeyan, "Secure privacy-preserving resolution adaptive data sharing in hybrid blockchain-controlled medical IoT environment," *Int. J. Intell. Eng. Syst.*, vol. 18, no. 1, 2024.
[32] G. SarojiniKaruppusamy and S. M. Kumar, "TwoFish-integrated blockchain for secure and optimized healthcare data processing in IoT-edge-cloud system," *Trans. Emerg. Telecommun. Technol.*, vol. 36, no. 3, e70076, 2025.
[33] Y. Tang, K. Wang, D. Niyato, J. Li, O. A. Dobre, and T. Q. Duong, "Secure data sharing and prediction with digital twin and blockchain in healthcare," *IEEE Commun. Mag.*, early access, 2025.
[34] K. Tlemçani et al., "Empowering diabetes management through blockchain and edge computing: A systematic review of healthcare innovations and challenges," *IEEE Access*, early access, 2025.
[35] J. A. Venice, R. Vettriselvan, D. Rajesh, P. Xavier, and H. J. Shanthi, "Optimizing performance metrics in blockchain-enabled AI/ML data analytics: Assessing cognitive IoT," in *Enhancing Automated Decision-Making Through AI*. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 97–122.
[36] G. Verma and S. Yadav, "Blockchain for management of healthcare data," in *Blockchain and Digital Twin for Smart Healthcare*. Amsterdam, The Netherlands: Elsevier, 2025, pp. 419–437.
[37] P. Vinayasree and A. M. Reddy, "A reliable and secure permissioned blockchain-assisted data transfer mechanism in healthcare-based cyber-physical systems," *Concurrency Comput.: Pract. Exp.*, vol. 37, no. 3, e8378, 2025.
[38] A. P. Vinnarasi and R. Dayana, "OSL-ABE: An optimal secure and lightweight attribute-based encryption method for blockchain-enabled IoT-based healthcare systems," *Neural Comput. Appl.*, vol. 37, no. 1, pp. 123–148, 2025.
[39] R. Thompson and L. Sonntag, "How medical cyber-physical systems are making smart hospitals a reality," *J. Integr. VLSI, Embedded Comput. Technol.*, vol. 2, no. 1, pp. 20–29, 2025, doi: 10.31838/JIVCT/02.01.03.
[40] P. Whig, R. Sharma, N. Yathiraju, A. Jain, and S. Sharma, "Blockchain-enabled secure federated learning systems for advancing privacy and trust in decentralized AI," in *Model Optimization Methods for Efficient and Edge AI: Federated Learning Architectures, Frameworks and Applications*, 2024, pp. 321–340.