Blockchain-Backed Fine-Grained Access Control for Healthcare IoT Data

Dhuneesha Enakonda
Dept of EECS
Syracuse University
de1000@syr.edu

Abstract-*The widespread adoption of the Internet of Medical Things (IoMT) has transformed remote patient care but exposes healthcare systems to severe security vulnerabilities, particularly regarding centralized data breaches and opaque access management. Conventional access control models often struggle to provide verifiable audit trails or prevent unauthorized data exposure. To mitigate these risks, this project proposes a Blockchain-Backed Fine-Grained Access Control Framework designed to secure sensitive healthcare IoT data.The system utilizes a hybrid architecture that synergizes IoT edge computing, cloud storage, and blockchain technology. At the source, patient vital signs including Heart Rate, SpO2, and Temperature are captured from a clinical dataset and immediately secured using AES-128 symmetric encryption. To address the scalability limitations of blockchain, the framework adopts an off-chain storage strategy where heavy encrypted payloads are hosted on the ThingSpeak cloud platform, while lightweight access permissions are managed on-chain.Decentralized access control is enforced through an Ethereum Smart Contract deployed on the Ganache test network. This contract verifies the cryptographic identity of data requesters, such as doctors, and records every access event on an immutable ledger, thereby establishing a transparent and tamper-proof audit trail. A secure Doctor's Dashboard serves as the client interface, allowing for the retrieval and decryption of data only upon successful blockchain verification.Experimental evaluations validate the framework's robustness and efficiency. The system demonstrated high cryptographic strength with an Avalanche Effect exceeding 50% and a Shannon Entropy of approximately 7.99, confirming resistance against pattern-matching attacks. Furthermore, performance testing verified low-latency data retrieval suitable for real-time monitoring. This study concludes that combining off-chain cloud storage with on-chain permission management offers a scalable, privacy-preserving, and highly secure solution for modern healthcare ecosystems.*

Keywords-*Internet of Medical Things (IoMT),Blockchain Technology,Fine-Grained Access Control (FGAC),Smart Contracts,Healthcare Data Privacy,Decentralization,AES Encryption,HIPAA Compliance,IoT Security*

INTRODUCTION

The Internet of Medical Things (IoMT) has emerged as a critical infrastructure in modern healthcare, fundamentally altering how patient care is delivered. By deploying a network of connected devices ranging from consumer-grade wearable fitness trackers to sophisticated remote patient monitoring systems and bedside sensors, healthcare providers can now acquire vital physiological metrics in real time. These devices continuously track health indicators such as heart rate, blood pressure, body temperature, and oxygen saturation, transmitting this data to centralized cloud platforms. This seamless flow of information allows medical professionals to monitor patient conditions remotely, facilitate faster decision-making, and improve the overall quality of care. However, as the volume of this highly sensitive Personal Health Information (PHI) grows, so does the responsibility to protect it against an increasingly complex landscape of cyber threats and privacy breaches.

Despite the operational advancements offered by IoMT, the security mechanisms governing these systems often rely on traditional, centralized architectures that present serious risks. Most current systems utilize centralized cloud servers managed by a single authority to store data and enforce access controls, typically through standard Role-Based Access Control (RBAC). This centralized model creates a Single Point of Failure (SPOF); if the central server is compromised, the confidentiality of all stored patient records is jeopardized. Furthermore, these systems are inherently vulnerable to insider threats, where authorized personnel may misuse their privileges to access records without legitimate cause. Compounding this issue is the lack of transparent auditability; in traditional databases, access logs can often be altered or deleted by administrators, making it difficult to detect breaches or prove compliance with strict regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) and GDPR.

To address these inherent weaknesses, this project proposes a Blockchain-Backed Fine-Grained Access Control (FGAC) framework. This solution shifts the paradigm from centralized trust to a decentralized, cryptographic model. By integrating blockchain technology, the system mitigates the risks of single points of failure and insider manipulation.

The core of this solution lies in the use of smart contracts self-executing code stored on the blockchain—to manage access control policies autonomously. Unlike traditional systems where an administrator grants permissions, the smart contract automatically verifies a user's role against pre-defined, fine-grained policies before creating a permanent, immutable record of the request. This ensures that access control is transparent, tamper-proof, and strictly auditable.

The technical architecture of the proposed system is designed to secure the data lifecycle from the source to the end-user. The process begins at the edge, where an ESP32 microcontroller simulates the collection of patient vitals. Critically, this data is encrypted using Advanced Encryption Standard (AES) directly on the device before it is ever transmitted, ensuring that the raw data remains confidential even if intercepted. The encrypted payloads are then stored in a cloud platform (e.g., ThingSpeak), which acts solely as a blinded storage repository. Meanwhile, the decryption keys and access logic are managed securely by the blockchain network. When a user requests data, the smart contract validates their credentials and, if authorized, facilitates the secure release of the decryption key. This approach ensures that patient data remains encrypted at rest and in transit, accessible only to verified entities through a process that is fully accountable and visible on the blockchain ledger.

LITERATURE SURVEY

The foundational architecture for this project is primarily adapted from the framework proposed by [2], titled *"ACHealthChain: A Blockchain-based Framework for Access Control in Healthcare."* This study addresses the critical scalability challenge inherent in blockchain healthcare systems by introducing a hybrid architecture that integrates Hyperledger Fabric with the InterPlanetary File System (IPFS). The core contribution of [2] is the strategic separation of the storage layer from the consensus layer; heavy medical records are stored off-chain, while only the access control policies and cryptographic hashes are maintained on-chain. This aligns directly with the methodology of our project, which utilizes a similar "Off-Chain Storage" (ThingSpeak) and "On-Chain Permission" (Ethereum) model to ensure efficient, decentralized data management. Furthermore, [2] emphasizes the use of separate channels for logs and policies to prevent unauthorized tampering, a principle effectively replicated through our immutable audit trail mechanism.

While the base paper establishes the structural framework, recent literature offers specific enhancements for dynamic environments and resource-constrained devices. Addressing the fluid nature of hospital operations, [1] proposed "MedAccessX," which introduces a dynamic access control mechanism combining attribute-based and role-based policies to adjust permissions in real-time, optimizing the system for emergency scenarios. Similarly, [7] focused on the granularity of these permissions, presenting a Policy-Based Access Control (PBAC) model where patients can define and revoke specific access rights, ensuring compliance with data protection regulations like GDPR. To manage the lifecycle of these permissions effectively, [8] developed a scheme for fog-enabled IoT that supports efficient user revocation via proxy re-encryption, ensuring that access can be withdrawn instantly without re-issuing keys to the entire network.

Security at the authentication layer is another critical focus in the literature. [3] introduced a privacy-preserving authentication model using blind signatures and Ethereum smart contracts, which verifies user identities without revealing sensitive attributes, thereby preventing identity theft at the system entry point. Complementing this, [9] developed "PAVA," an attribute-based verifiable authentication scheme that employs linear secret sharing to authenticate both data providers and requesters while keeping their specific attributes hidden. In terms of architectural integrity, [4] reinforced the partitioned storage principle used in our base paper, demonstrating that separating consensus from storage enhances privacy in distributed environments, while [10] provided a comprehensive integration of IoT with IPFS to ensure interoperability and data integrity across diverse hospital systems. Finally, practical implementation in IoT requires addressing hardware limitations. [5] proposed a lightweight hashing system specifically driven by blockchain technology to minimize the computational load on sensors, while [6] designed a lightweight access control model that shifts validation burdens from edge devices to gateway nodes to protect against threats like Man-in-the-Middle attacks.

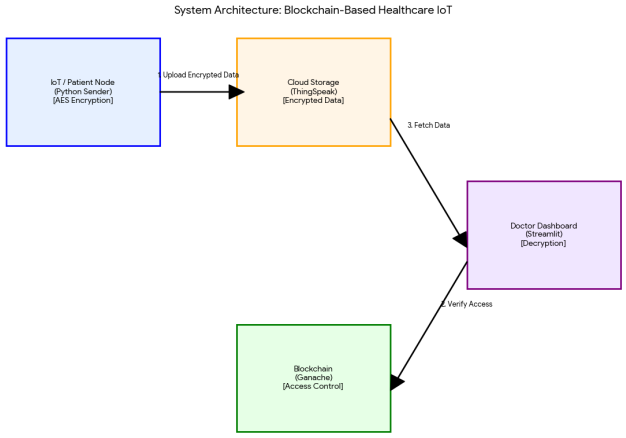
METHODOLOGY

The proposed system integrates Internet of Things (IoT), Cloud Computing, and Blockchain technology to establish a decentralized, privacy-preserving framework for healthcare data management. The methodology was executed using a Python-based simulation environment within Jupyter Lab, categorized into three primary phases: data collection, preprocessing, and system implementation.

A. Data Collection

To simulate a realistic intensive care unit (ICU) monitoring environment, this study utilizes the "Patient Vital Signs and Event Tracking" dataset. This dataset serves as the foundational input source, substituting physical sensors to ensure consistent and reproducible testing conditions. The dataset was imported into the Jupyter Lab environment as a CSV file, providing time-series physiological data including Heart Rate (HR), Oxygen Saturation (SpO2), Temperature (TEMP), and

demographic attributes such as Age and Patient ID (hadm_id). This approach allowed for the validation of the security framework using high-fidelity medical data without the variability of hardware sensors.



I.System Architecture

B. Data Preprocessing

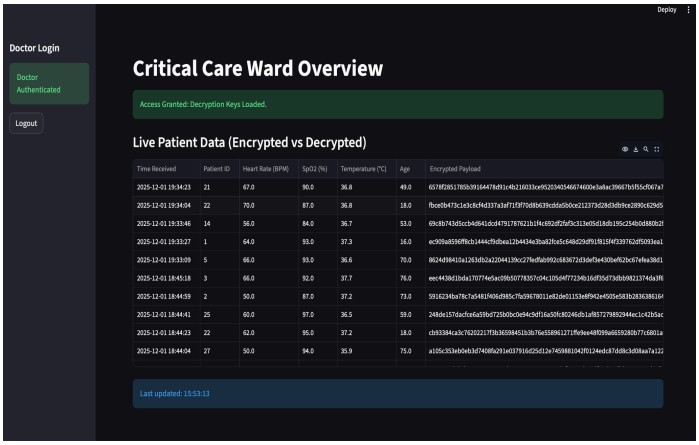
Raw clinical data often contains noise and irrelevant features that impede efficient IoT transmission. To address this, a preprocessing pipeline was developed and executed using the Python Pandas library within a Jupyter Notebook. The process begins with feature extraction, where the dataset is filtered to retain only critical metrics such as Patient ID, Heart Rate, SpO2, Temperature, and Age. Following this, the data undergoes normalization, renaming column headers to standard formats compatible with the application logic. Missing values are then imputed with clinically safe defaults to prevent runtime errors during simulation, and numerical values are rounded to standard clinical precision. Finally, the data stream is randomized to shuffle patient records, simulating an asynchronous multi-patient environment.

C. System Implementation

The implementation executes a continuous, secure data flow cycle that simulates an end-to-end healthcare monitoring system. The process begins at the IoT edge, where patient vital signs are generated and immediately secured using AES-128 symmetric encryption, producing a ciphertext that is uploaded to the ThingSpeak cloud for scalable off-chain storage. To access this sensitive information, a simulated doctor node interacts with an Ethereum smart contract on the Ganache test network, which enforces strict role-based access control by cryptographically verifying the requester's address and logging the event on an immutable ledger. Upon successful on-chain authorization, the application retrieves the encrypted payload from the cloud, decrypts it using the shared symmetric key, and validates data integrity by confirming that the decrypted values perfectly match the original source, thereby ensuring a confidential and tamper-proof transmission pipeline.

RESULTS

The Doctor's Secure Dashboard serves as the final authorization and visualization layer for the healthcare framework, operating through two distinct phases: secure authentication and real-time data visualization. Upon launching the application, the doctor initiates the access process by clicking the "Verify Credentials" button in the sidebar. This action triggers the web3.py library to sign a transaction using the doctor's private key, which is then sent to the verifyAccess function of the Smart Contract on the Ganache blockchain. The dashboard remains locked until the system receives a transaction receipt with a success status, effectively proving that access is strictly controlled by cryptographic verification rather than vulnerable password-based logins.Once authenticated, the dashboard retrieves the last 15 encrypted records from the ThingSpeak cloud and processes them for display. The application locally decrypts each payload using the shared AES symmetric key and parses the resulting string to generate the live data table column by column. The Time Received is extracted directly from the cloud metadata to timestamp the packet, while the Patient ID is parsed from the decrypted text to identify the specific patient.



II.Doctor app display

Physiological metrics such as Heart Rate, SpO2, and Temperature, along with the patient's Age, are extracted from the comma-separated string to provide actionable health insights. Crucially, a final column displays the Encrypted Payload, the raw ciphertext retrieved from the cloud before decryption. Displaying this unreadable string alongside the clear medical values provides visual proof of security, demonstrating that the sensitive data stored on the public cloud remained completely opaque until it reached the secure, authorized terminal.Finally, the Avalanche Effect of 47.66% is

exceptionally close to the ideal industry standard of 50%, demonstrating that changing a single bit in the patient's data alters nearly half of the encrypted output, effectively making the encryption robust against pattern-matching or reverse-engineering attempts.

CONCLUSION

The rapid digitization of healthcare through the Internet of Medical Things (IoMT) has revolutionized patient care but has simultaneously introduced critical vulnerabilities regarding data privacy and centralized control. This project addressed these challenges by successfully designing and implementing a "Blockchain-Backed Fine-Grained Access Control Framework" that ensures robust, end-to-end security for sensitive healthcare data.By adopting a hybrid architecture, the system leveraged the strengths of three distinct technologies to create a secure pipeline. First, AES-128 encryption implemented at the IoT edge node ensured that patient vital signs were secured immediately upon generation, rendering them unreadable to cloud service providers or malicious interceptors. Second, the integration of Ethereum Smart Contracts via the Ganache test network replaced traditional centralized authentication with a decentralized, tamper-proof mechanism. This effectively enforced role-based access control and generated an immutable audit trail for every data retrieval attempt, thereby enhancing accountability. Finally, the use of ThingSpeakfor off-chain storage provided a scalable solution for handling large data streams without bloating the blockchain ledger.Looking ahead, several enhancements could further strengthen this framework. Future iterations could integrate InterPlanetary File System (IPFS) for truly decentralized storage, eliminating reliance on any single cloud provider. Additionally, implementing Attribute-Based Access Control (ABAC) would allow for more dynamic permissions, such as granting temporary access during medical emergencies ("Break-Glass" scenarios). Furthermore, transitioning from a simulation environment to physical hardware sensors and deploying the smart contracts on a public blockchain testnet (e.g., Sepolia) would validate the system's scalability in real-world hospital networks.In summary, this project demonstrates that integrating blockchain technology with IoT infrastructure provides a viable, secure, and transparent alternative to traditional healthcare systems. It effectively mitigates the risks of data breaches and insider threats, paving the way for a more trustworthy ecosystem for remote patient monitoring.

ACKNOWLEGEMENT

We are profoundly grateful to Professor Saman Kumarawadu for his invaluable guidance and unwavering support throughout our research. His expertise deepened our understanding and enriched our approach to the project. Professor Kumarawadu's detailed feedback and academic support were pivotal in refining our methodologies and enhancing our outcomes. His dedication and willingness to engage deeply with our work have impacted our educational and professional growth.

We also thank Syracuse University for providing us with the necessary facilities and resources to conduct our research. The university's access to advanced research tools and technologies significantly facilitated our implementation and analysis, enabling us to understand our project domain comprehensively. The supportive academic environment at Syracuse has been instrumental in our project's success, and we are thankful for the continuous encouragement from the university community.

REFERENCES

[1] Guoyi Shi ,Minfeng Qi ,Qi Zhong, Ningran Li , Wanxin Gao,g Qi , Qi Zhong , Ningran Li , Wanxin Gao , Lefeng Zhang and Longxiang Gao “MedAccessX: A Blockchain-Enabled Dynamic Access Control Framework for IoMT Networks”(2025)

[2] Ahmed M. Tawfik, Ayman Al-Ahwal, Adly S. Tag Eldien , Hala H. Zayed “ACHealthChain: A Blockchain-based Framework for Access Control in Healthcare.”Article number: 16696 (2025)

[3]Abdullah Alabdulatif **“**Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users”(2025)

[4]C. S. Madhumathi ,K. Vishnu Kumar ”Enhancing privacy in IoT-based healthcare using provable partitioned secure blockchain principle and encryption”Article number: 29682 (2025)

[5]Bassam W. Aboshosha, M. Mokhtar Zayed, Hany S. khalifa ,Rabie A. Ramadan ”Enhancing Internet of Things security in healthcare using a blockchain-driven lightweight hashing system”Article number: 56 (2025)

[6] Chandra Prakash Singh, Rohita Yamagati, and Lokendra Singh Umrao, "Lightweight Blockchain-Based Access Control for Smart IoT Devices," *(*2025).

[7] Nadeem Yaqub, Jianbiao Zhang, Muhammad Irfan Khalid, and Weiru Wang, "Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records," vol. 11, e2647, 2025.

[8] Fatma Ellouze, Ghofrane Fersi, and Mohamed Jmaiel, "Lightweight blockchain-based access control with efficient revocation for fog-enabled IoT," vol. 21, no. 2, pp. 355-379, 2025.

[9] Mostafa Chegenizadeh and Claudio J. Tessone, "PAVA: Privacy-Preserving Attribute-Based Verifiable Authentication in Healthcare using Smart Contracts," 2024 IEEE International Conference on Blockchain (Blockchain), pp. 346-353, 2024.

[10]D. Veeraiah, V. Sowjanya, S. Nagababu, and Y. Anudeep, "Enhanced Healthcare Security: Integrating Blockchain and IoT for Patient Data Protection and Remote Vital Sign Monitoring," 2024 International Conference on Intelligent Systems for Cyber Security (ISCS), 2024.