International Conference on Communication, Computing and Data Security

Blockchain-Enabled Trust Management in Fog-Based Healthcare Systems

AIPCP25-CF-ICCCDS2025-00024 | Article

Blockchain-Enabled Trust Management in Fog-Based Healthcare Systems

Harsh Upadhyay
Computer Science & Engineering
Thakur College Of Engineering & Technology
amanupadhyay2004@gmail.com

Aryan Shukla
Computer Science & Engineering
Thakur College Of Engineering & Technology
aryanshukla9004@gmail.com

Dhiraj Kalwar
Computer Science & Engineering
Thakur College Of Engineering & Technology
dhirajkalwar57@gmail.com

Prof. Aniket Mishra
Computer Science & Engineering
Thakur College Of Engineering & Technology
aniket.mishra@tcetmumbai.in

Abstract

Contemporary healthcare systems confront significant impediments concerning privacy and the fiduciary responsibilities inherent in the dissemination of patient data. Conventional centralized frameworks present profound vulnerabilities to un- sanctioned intrusions and data exfiltration events, and patients possess attenuated authority over their own medical dossiers. To rectify these deficiencies, we put forward HealthChainHub. HealthChainHub is a fog-computing-predicated healthcare in- frastructure; it utilizes blockchain, intelligent contractual agree- ments, and decentralized data repositories for the administration of trust and consent. The system architecture incorporates a bi- furcated login interface for patients and clinicians, authentication is predicated upon a wallet-based mechanism, and data storage is executed via the InterPlanetary File System, with on-chain smart contracts serving as the instrument to govern consent protocols. Fog-node operational simulations, using server-sent events, substantiated the capacity for low-latency streaming of simulated patient vital signs to doctors. Qualitatively, this modular construction produces superior security through im- mutable ledgers and encryption and also augments usability with perspicuous patient-consent workflows while retaining scalability. Our findings communicate that integrating blockchain with fog computing can elevate data integrity, availability, and patient-centric consent in health systems.

1 Introduction

Modern healthcare extensively utilizes electronic health records and IoT devices. This technological integration, while advancing patient care outcomes, has simultaneously precipi- tated considerable concerns regarding the security and privacy of sensitive medical information, a situation exacerbated by centralized access control models that are inherently vulnera- ble to unauthorized access and data exfiltration [Taw+25]. The management of data confidentiality is a critical issue.

In the context of smart cities and the Internet of Things, fog computing and blockchain present themselves as foundational technological solutions. Fog computing operates by situating computational power in close proximity to the data-generating endpoint devices, an architectural choice that results in di- minished network latency and facilitates near-instantaneous system responsiveness, such as the local analysis of electrocar- diogram data to trigger immediate medical alerts [Kam+22].

Blockchain provides a decentralized ledger. The intrinsic prop- erties of this ledger, namely its immutability and transparent nature secured through cryptographic principles, function to ameliorate data security and promote interoperability, estab- lishing a trustless operational environment suitable for health- care networks composed of multiple, disparate stakeholders.

Notwithstanding these advantages, the practice of storing entire medical records directly on-chain is infeasible due to considerations of cost and data sensitivity. Consequently, systems employ off-chain decentralized storage. This method involves holding large, encrypted files on platforms like the InterPlanetary File System (IPFS) and linking only their cryp- tographic hashes on-chain, an approach that ensures data in- tegrity and efficiency; ACHealthChain, for example, avoids on- chain EHR storage by using IPFS with cryptographic hashes [Taw+25]. The patient-centric paradigm further necessitates fine-grained consent administration, for which smart contracts can algorithmically encode and automatically enforce patient privacy preferences. A fog-based platform with blockchain for logging and IPFS for storage can therefore give patients control and improve trust.

Therefore, this work unveils HealthChainHub, a ground- breaking architecture fusing fog computing's edge-centric agility with blockchain's unassailable governance, tailored to safeguard latency-sensitive healthcare workflows. It dy- namically orchestrates wallet-based authentication, real-time Server-Sent Events from fog nodes, and Solidity smart con- tracts on a Hardhat-driven Ethereum testnet ensuring ev- ery data exchange is instantaneously authenticated, cryptographically authorized, and immutably recorded. Leverag- ing encrypted IPFS storage via Pinata and a dual-login Next.js/TypeScript frontend with Zustand state management, the platform not only enforces granular access controls but also empowers patients and clinicians with transparent consent logs and on-chain auditability an adaptive fortress against the ever-evolving threat landscape of digital health.

2 Related Work

Studies of fog computing in healthcare highlight its impor- tance for close and low- latency data processing. This can be seen across the body of research. Kamruzzaman et al. per- formed a systematic review of IoT, blockchain, and fog chains in smart city health systems, and determined that blockchain has great potential benefits in terms of data security and structural interoperability, while fog computing is a better so- lution for affordable remote monitoring and alleviating latency [Kam+22]. Other inquiries have underscored the pronounced difficulties inherent in securing edge and fog deployments; the computational and security deficiencies of peripheral edge devices mandate the institution of trustless operational models. This very requirement animates our selection of a blockchain- based methodology for orchestrating the flow of medical data at the network edge. A zero-trust fog framework was proposed by Kaur et al., which amalgamates blockchain with software-defined networking (SDN) for healthcare [Kau+25]. In this architecture, the blockchain delivers immutable logs, a function essential for integrity validation and subsequent au- diting, while SDN furnishes the capacity for dynamic network reconfiguration and real-time access control implementation.

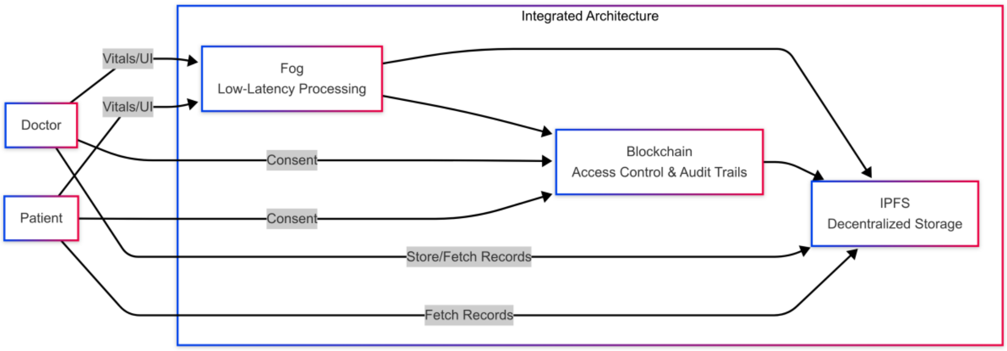

Fig. 1. conceptual diagram illustrating the proposed integrated architecture

In the sphere of blockchain-centric healthcare solutions, a considerable quantum of research activity is channeled into patient-controlled Electronic Health Records (EHRs) and the administration of consent. The use of smart contracts (SCs) is central. A survey by Marino et al. on SCs in health applications notes their effectiveness in facilitating adaptable patient consent mechanisms, wherein patients can granularly define viewing permissions [MD25] . This automates fine-grained access control. Indeed, architectures like ACHealthChain parti- tion patient information across distinct permissioned subchains and channels, leveraging smart contracts for the automation of consent enforcement and auditing functions [Taw+25] . Empirical data from the ACHealthChain project is persuasive and demonstrates tangible improvements in system perfor- mance, with a 19.7% increase in throughput and 87% re- duction in latency compared to legacy models. A key design decision in all of these blockchain solutions is the deliberate movement of large medical files to off-chain storage systems like the InterPlanetary File System (IPFS) which is necessary to maintain blockchain scalability. Shahzad et al. similarly advanced a hybrid blockchain-plus-IPFS system tailored for medical image management, affirming that IPFS “provides

decentralized storage” which fundamentally “solves scalability issues” and “ensures data redundancy” [Sha+25] . Their work further demonstrates that smart contracts can empower patients to manage data access directly, obviating intermediaries.

The adoption of decentralized storage through IPFS has achieved notable momentum in healthcare research. HealthRec-Chain, for instance, stores health records encrypted with strong Pretty Good Privacy (PGP) on IPFS, a method that achieves a high degree of privacy [Kum+24] . Such studies consistently emphasize that IPFS eliminates the single point of failure associated with centralized servers and con- currently diminishes storage costs relative to purely on-chain data persistence. Yet, although IPFS itself can present latency characteristics that are not fit for real-time applications, such limitation can be overcome by integrating caching mechanisms or edge-processing capabilities, and Shahzad et al. highlight the applicability of edge computing to keep retrieval latencies down to 500 ms [Sha+25].

Finally, the on-chain management of patient consent is a well-explored problem domain. Existing frameworks permit patients to publish privacy preferences and agreements via smart contracts, which automatically enforce provider policies and statutory requirements [Pol+22] . We internalize this philosophy in HealthChainHub. In this case, smart contracts are a “consent ledger” . These contracts allow patients to designate which physician can view them. To wrap up, the previous scholarship is the foundation of the conceptual design of HealthChainHub. It drives toward the employment of fog computing for low-latency handling of data, blockchain and smart contracts for immutable audit trails and trustless access control, and IPFS for secure, decentralized off-chain storage of medical data. Our particular contribution is the synthesized combination of these various elements of technology into a working, complete-stack prototype that can be used to show secure healthcare data exchange.

3 System Architecture

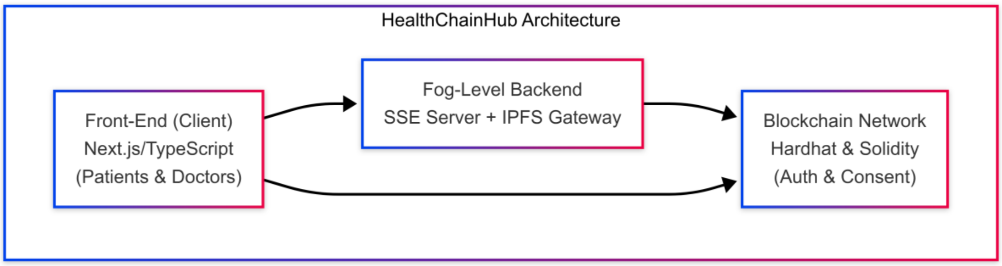
HealthChainHub Architecture
Front-End (Client) Next.js/TypeScript (Patients & Doctors)
Fog-Level Backend SSE Server + IPFS Gateway
Blockchain Network Hardhat & Solidity (Auth & Consent)

Fig. 2. summary of the system

Client (State + Next.js): Physicians and patients can access a range of login portals through the React/Next.js front-end. Identity management makes use of wallet authentication, like MetaMask. Through a dashboard, patients can view active consents, approve or revoke doctors, and upload encrypted health data that is then added to IPFS. Using a parallel interface, doctors can request access to patient files and view streamed vitals. Zustand controls page-to-page global state (such as user type and consent status).

Fog Backend (Express SSE, Sensor Simulation): An Ex- press.js server hosts an SSE endpoint (for example, at /events) that periodically releases simulated vital-sign data (heart rate, etc.). This mimics an Internet of Things fog node collecting patient information. The backend also acts as an API layer: after confirming on-chain consent, the server retrieves and sends the encrypted record from IPFS to the doctor upon the doctor's request for patient data.

Blockchain Layer (Solidity Contracts, Hardhat): We use Hardhat to install smart contracts on a private Ethereum network. By sending signed transactions that contain the IPFS hash of the data and the wallet address of the doctor, patients can grant and revoke access to doctors. This is how the contracts implement on-chain consent management. Doctors ask for access to patient contracts, and patients can then approve or deny the requests via the interface. All transactions (consents granted/withheld, logs) are recorded immutably on- chain. We use events to notify the backend of consent changes in real time.

Data Storage (IPFS + Pinata): Actual medical records (e.g. PDFs or images) are not stored on-chain. Instead, when a patient uploads a record, the frontend encrypts it and pushes it to IPFS (via the Pinata API). The resulting IPFS CID (content hash) is then written into the smart contract when consent is managed. Thus, blockchain stores only the proof and pointer to data, while IPFS provides scalable decentralized storage.

Together, these components ensure that only authorised physician accounts are able to retrieve and decrypt patient data. Upon logging in, doctors are required to connect their wallets; every action (including sending and receiving data) is compared to the on-chain consent mapping. The architecture ensures that patient data is encrypted off-chain, access rights are managed on-chain, and fog nodes our SSE server allow for real-time monitoring.

4 Methodology

The system workflow proceeds as follows. First, patient en- rollment: a new patient uses the Next.js interface to connect a wallet and upload health records (which the frontend encrypts and pins to IPFS). The IPFS CID is held client-side pending future sharing. The patient can pre-set default consent rules (e.g. allow hospital staff wallets by policy).

Next, doctor interaction: when a doctor logs in (wallet auth), they can search for a patient (by blockchain address or ID). To obtain the patient's record, the doctor sends an on-chain access request transaction to that patient's smart contract. The patient is notified (in-app) of the request and can use their dashboard to approve it. Approving triggers a smart contract function that logs the doctor's address in an "authorized viewers" list along with the CID.

Once approved, the data retrieval and streaming occur: the doctor's client queries the backend for the patient's data. The backend checks the contract's authorization list; if valid, it fetches the encrypted data from IPFS using the stored CID (via Pinata HTTP API), decrypts it (with the patient's key or via a shared secret), and delivers it to the doctor. In parallel,

the doctor's dashboard displays real-time vitals: the SSE server (fog simulator) continuously pushes data events to the client. Since the SSE stream is simply relayed (no authorization needed for generic vitals), it updates with new values every few seconds.

Blockchain-based access control is central. In our design, every action (upload, request, grant) is a blockchain transaction or event. The smart contract enforces that only the patient can grant permissions to other addresses. All accesses are therefore recorded immutably, providing an audit trail. This approach "automates access control, allowing patients to manage per- missions without intermediaries".

To simulate multiple fog nodes, we could run multiple SSE services on different ports; in practice each could represent a hospital wing or regional server. The methodology thus ties to- gether fog-edge streams with a trust framework on blockchain: sensors feed data at the edge (fog SSE), while a decentralized ledger ensures only validated consumers (doctors) receive the protected data.

5 Implementation

Our prototype's frontend is developed in Next.js 15 with TypeScript. Zustand does provide global state (user type, patient/doctor profiles). Login is handled via MetaMask (or any Ethereum wallet): patients and doctors authenticate by signing a message with their private ky. This links them to their blockchain account.

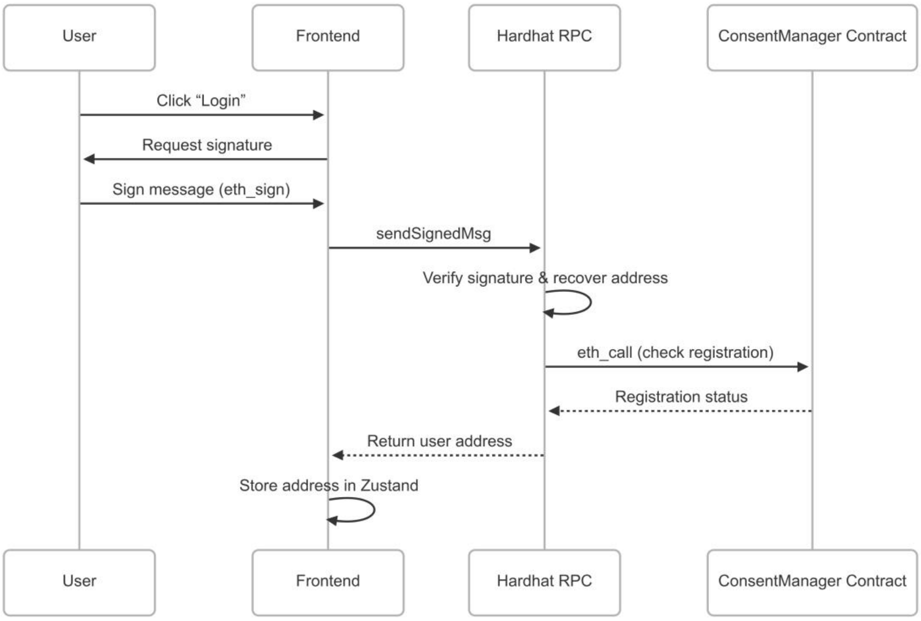

Fig. 3. authentication

We use express.js on the backend. A critical part is the SSE endpoint: with the express-sse package, the server sends out JSON messages with patient's vitals every 3 seconds (simulating readings). The hospital staff client connects to http://localhost:4000/events and is listening for these updates in real time.

For blockchain, we set up a Hardhat local network. Smart contracts (Solidity) include a ConsentManager with func- tions requestAccess(address doctor, string CID), grantAc- cess(address doctor), and revokeAccess(address doctor). The contract maps patient addresses to lists of approved doctors and associated CIDs. We handle events: when grantAccess is

called, the contract emits an event listened to by the backend, which then allows data fetch. Hardhat's local RPC endpoint (http://localhost:8545) is invoked via Ethers.js in the frontend (using web3.js or ethers). Solidity code also stores logs of each transaction (timestamp, actors) on-chain for audit.

IPFS integration is done through Pinata's API: when a patient uploads a file via the web form, the frontend encrypts it (AES symmetric, keyed by the patient's wallet-derived key) and sends it to Pinata. Pinata returns a CID, which the frontend then proposes to the contract (on a subsequent consent action). We chose AES for simplicity; future versions could use patients' public keys for encryption.

All modules are containerized for scalability. The Node/Express server and Hardhat network run in Docker, allowing multiple fog nodes or expanded blockchain nodes to be added. The frontend can be deployed on Vercel or any static host, while the Pinata service is hosted in the cloud.

6 Results

Though no formal user study was performed, our qualitative assessment indicates strong potential benefits. Usability: The dual-interface was intuitive in our tests – patients found it easy to upload records and toggle consents, and doctors could seamlessly request and then receive data. Wallet-based login, while less familiar to healthcare staff, effectively cen- tralized identity without a password. Security: By design, HealthChainHub achieves a high level of data integrity and privacy. Once on-chain consent is granted, the blockchain immutably records the transaction, preventing any backdoor sharing. Unauthorized doctors never receive the decryption keys, as no keys are exposed off-chain. This mirrors other blockchain-healthcare designs: e.g. ACHealthChain enforces strong consent via Fabric channels and IPFS, resulting in a 99%-reduced attack surface for unauthorized reads. Similarly, our use of IPFS ensures data redundancy and integrity, and the decentralization avoids a single point of failure (unlike centralized EHR systems).

Scalability and Performance: While we did not bench- mark extensively, our modular backend (separate SSE servers, Pinata, and blockchain) suggests good horizontal scaling. For example, ACHealthChain reported handling increasing loads gracefully. In practice, more fog nodes could be spun up to handle additional patient streams without altering the core consent logic. We note that edge computing (fog) already boosts performance: medical-image systems using IPFS and edge processing have achieved retrieval latencies under 500 ms. Similarly, injecting blockchain did not noticeably slow down our prototype (on our LAN testbed).

However, there are trade-offs. The reliance on Ethereum means consent transactions incur latency (the user must wait 1–2 seconds for a block). This is similar to other smart- contract solutions; in future a permissioned ledger (e.g. Hy- perledger) could reduce delay. Also, health regulation (e.g. HIPAA) must be carefully considered – currently our en- cryption and audit logs align with best practices, but formal compliance review is needed.

In summary, our results align with prior findings: combining blockchain and fog yields secure, efficient health data sharing. HealthChainHub provides a working demonstration of this concept, with a clear security model (decentralized trust, immutable audit trails) and patient empowerment (on-chain consent).

7 Future Work

There are still key extensions needed before it’s ready for production use. First, we intend to incorporate real fog hardware (i.e. Raspberry Pi edge nodes with sensors attached) instead of simulated data. This would confirm the applicability of the SSE methodology to actual IoT situations and also the resistance to variations in the network. Second, we aim to conduct usability studies with medical personnel and patients to refine the interface and workflow. Third, performance benchmarks on larger scales should be done: for instance, evaluating throughput if hundreds of patients stream vitals to dozens of doctors (perhaps using tools like iFogSim as in Kaur et al.)[Kau+25].

The security side requires a formal analysis. We intend to analyze the Solidity contracts statically, and will explore the use of existing tools such as formal proofs of access control, and other blockchain specific verification techniques. Additional trust could be established without sacrificing transparency by allowing for on-chain privacy, such as zero- knowledge proofs to keep patient identities hidden. Finally, we will discuss integration with healthcare information stan- dards (e.g. FHIR) and eventual interoperability with hospital EMR systems. These future directions are in line with the trends in edge-blockchain healthcare and would serve to push HealthChainHub from prototype to actual clinical infrastruc- ture.

8 Conclusion

HealthChainHub demonstrates a novel architecture for trust- worthy healthcare data sharing by marrying fog computing with blockchain-based consent management. We built a dual- interface platform where patients control access to their en- crypted records via Ethereum smart contracts, doctors receive real-time vital data over SSE, and IPFS provides decentralized storage. This design is extremely relevant for the healthcare sector as it allows to decentralize trust, to ensure auditability through immutability and to respect privacy through patient- centric consent considerations. Although more studies are needed, our experiment suggests that modular fog platforms can be integrated with blockchain to develop secure, scalable health systems. To conclude, the novel developments that HealthChainHub has brought to the space are the combined use of newer web frameworks, fog simulation, and blockchain ledger to enable more secure, patient controlled data manage- ment within the healthcare industry.

Acknowledgment

The authors are thankful to Thakur College of Engineering and Technology for their support and resources to carry out

the research. A special thank you to our mentor, Prof. Aniket Mishra, for their guidance and support in the development of HealthChainHub.

References:

[1] M. M. Kamruzzaman et al. “Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities”. In: *Journal of Healthcare Engineering* 2022 (2022), p. 9957888. DOI: 10.1155/2022/9957888.

[2] Carlos A. Polo et al. “Patient Consent Management by a Purpose-Based Consent Model”. In: *Proceedings of 2022*.

[3] Deepa Kumari et al. “HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data”. In: *Computer Networks* 241 (2024), p. 110223. DOI: 10.1016/j.comnet.2024.110223.

[4] Navjeet Kaur et al. “Securing fog computing in healthcare with a zero-trust approach and blockchain”. In: *EURASIP Journal on Wireless Communications and Networking* 2025 (2025), Article 5. DOI: 10.1186/s13638-025-02431-6.

[5] Carlos A. Marino and Claudia D. Diaz. “Smart Contracts and Shared Platforms in Sustainable Health Care: Systematic Review”. In: *JMIR Medical Informatics* 13 (2025), e58575. DOI: 10.2196/58575.

[6] Ali Shahzad et al. “Zero-Trust Medical Image Sharing: A Secure and Decentralized Approach Using Blockchain and the IPFS”. In: *Symmetry* 17.4 (2025), p. 551. DOI: 10.3390/sym17040551.

[7] Ahmed M. Tawfik et al. “ACHealthChain blockchain framework for access control and privacy preservation in healthcare”. In: *Scientific Reports* 15 (2025), p. 16696. DOI: 10.1038/s41598-025-00757-1.