# Privacy-Preserving Auditability using AI-enabled Blockchain for Healthcare Registry

Dr. K. Rajesh Khanna[1*], Gone Rushmitha[2], Vontela Chandu[2], Kandika Dikshitha[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi College of Engineering (UGC – Autonomous), Bollikunta, Warangal, Telangana.

*Corresponding author: Dr. K. Rajesh Khanna (khanna.vaagdevi@gmail.com)

## ABSTRACT

This project presents a decentralized, privacy-preserving healthcare registry that leverages client-side encryption and blockchain technology to secure sensitive patient and hospital data. Traditional healthcare systems rely on centralized databases that are vulnerable to single-point failures, insider threats, and large-scale data breaches, and they often lack immutable audit trails. To address these challenges, we implement a Django web application that derives a 256-bit AES key via PBKDF2 from a password and salt and uses AES in CTR mode to encrypt all records before storage. Encrypted data is Base64-encoded and sent to an Ethereum-compatible blockchain through Web3, where smart contracts manage functions for saving and retrieving hospital and patient entries. Upon retrieval, data is Base64-decoded and decrypted on the server, then displayed through role-based interfaces for patients, hospitals, and administrators. The system demonstrates end-to-end confidentiality—plaintext never resides on-chain—while benefiting from blockchain's immutability and transparency. A proof-of-concept evaluation highlights both the feasibility of this hybrid architecture and areas for production enhancement, including authenticated encryption (AES-GCM), randomized nonces, asynchronous transaction handling, and robust key management. By combining client-side cryptography with decentralized storage, this approach offers a blueprint for secure, auditable, and interoperable healthcare data management that can be extended to broader applications in clinical trials, supply-chain tracking, and patient-controlled record sharing.

**Keywords:** Privacy preserving, Healthcare systems, Decentralized mechanism, Blockchain, Artificial Intelligence.

## 1. INTRODUCTION

The initial application of blockchain technology was Bitcoin in 2008. Three characteristics make blockchain different from other solutions: decentralization, transparency, and confidentiality. Its possible application in other data-centric industries, including healthcare, has drawn interest. IBM believes the healthcare sector will be seriously impacted in three areas: the decentralized interchange of electronic health information (EHRs), clinical trial administration, and regulatory compliance. Because it permits data to be transferred between devices via innovative wireless channels, the Internet of Things (IoT) is essential to the healthcare industry.

The IoMT refers to this network's focus on patient care. Thanks to the collection of physiological data by Internet of Medical Things devices, medical experts may make precise diagnoses. Due to its numerous benefits, such as data security and simpler management of Internet of Things devices, blockchain has established itself as a dependable and decentralized platform. Blockchain technology has secure access, data storage, and medical research applications. Attention to patient privacy regulations and data-sharing protocols facilitates accurate data visualization, which is especially helpful during pandemics such as the COVID-19 outbreak. By combining blockchain technology with IoMT

devices, patient privacy and data distribution are improved. Reliability in smart contracts helps to prevent data manipulation. Blockchain's decentralized storage enhances data collection, sharing, and storage transparency The emergence of blockchain technology marked a significant milestone with the introduction of the digital currency Bitcoin in 2008 [1]. Its foundational attributes of transparency, confidentiality, and decentralization set blockchain apart from other technologies. By March 19, 2019, approximately 400 million Bitcoin transactions had been executed successfully, serving as a compelling illustration of the myriad possibilities offered by blockchain technology [2].

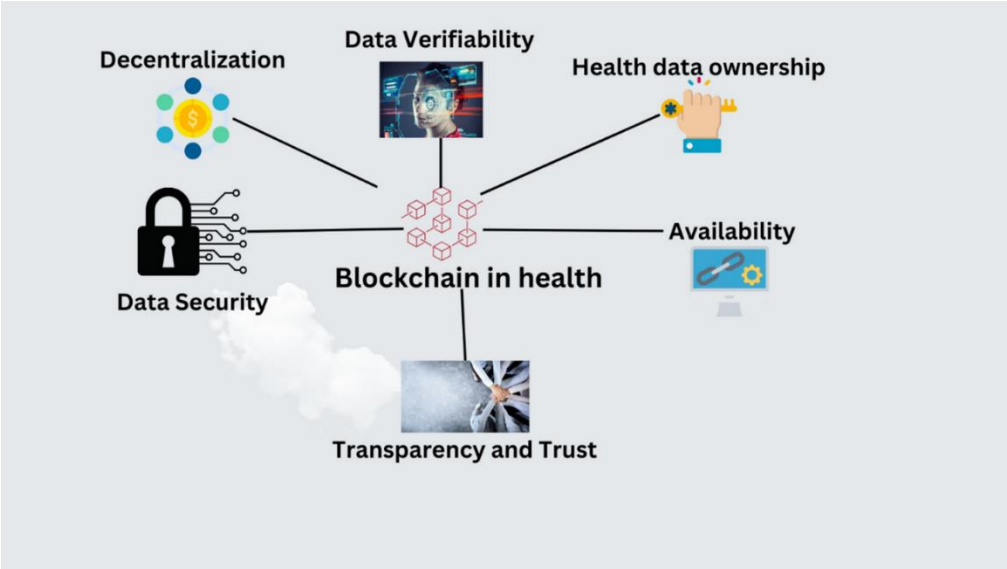



Fig. 1: Advantages of Blockchain.

As a result of this groundbreaking success, there has been a burgeoning interest in exploring the potential applications of blockchain technology across various data-centric industries, notably in the healthcare field [3]. A leading technology company, IBM, has advocated adopting blockchain in healthcare [4]. They anticipate that blockchain technology will substantially influence the healthcare sector, particularly in critical areas such as clinical trial management, regulatory compliance, and creating a decentralized mechanism for the secure exchange of electronic health records (EHRs) [5].

### 1.1.1 Recent advances in Blockchain for EHR

HealthChain, an EHR application developed as a permission, private blockchain network, leverages IBM Blockchain's Hyperledger Fabric and is deployed on Bluemix. The modular architecture of Hyperledger Fabric enables HealthChain to ensure health data confidentiality, scalability, and security [6]. Health Chain also incorporates chain codes (smart contracts) to control authorisations and access privileges within the blockchain network [7]. Additionally, Ancile, built on the Ethereum blockchain platform, utilizes smart contracts to achieve access control, data security, privacy, and interoperability of electronic medical records [8]. MedRec and the medical data preservation system (DPS) developed by Li et al. are notable examples that utilize the Ethereum blockchain platform to implement HER [9, 10, 11]. Other blockchain-based EMR applications include MedBlock [12], BlockHIE [13], FHIRChain [14], and MeDShare [15], further illustrating the diversity and potential of blockchain technologies in enhancing EHR systems.

By the year 2022, it is expected that the market for blockchain technology will reach its peak within the healthcare business. This prediction highlights the possible effect that blockchain technology will have on the healthcare industry [16]. This projection reflects the growing recognition of blockchain's potential to revolutionize various facets of healthcare, from enhancing data security to streamlining

administrative processes. In essence, the foundational principles of transparency, confidentiality, and decentralization that underpin blockchain technology have sparked a wave of enthusiasm and exploration across multiple industries, particularly healthcare. The potential to enhance the management of clinical trials, ensure regulatory compliance, and enable secure EHR exchange represents a promising future for blockchain within the healthcare sector as it continues to evolve and mature.

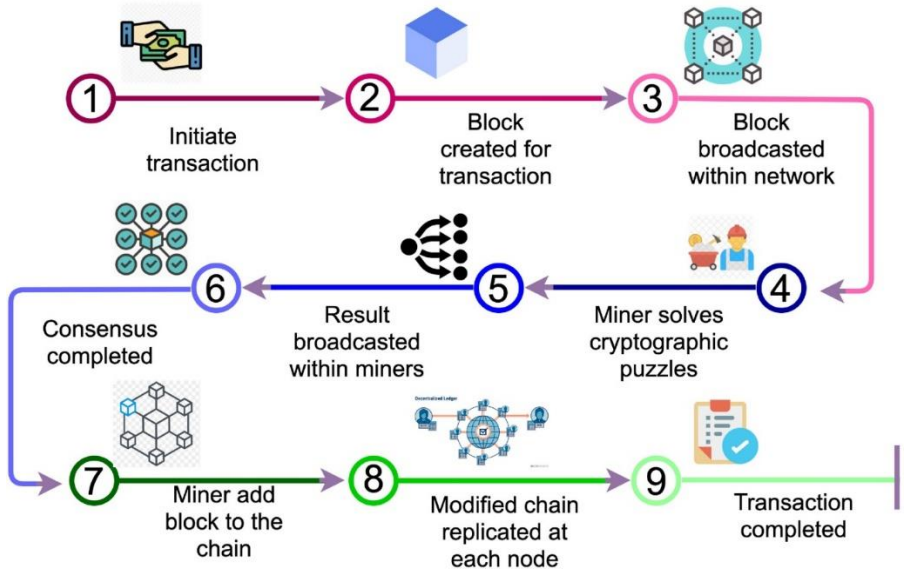



Fig. 2: Blockchain implementation process.

Modern healthcare systems must manage vast amounts of sensitive patient and institutional data. Traditional centralized databases are vulnerable to single-point failures, unauthorized alterations, and breaches. There is a need for a system that ensures data confidentiality, integrity, and availability, while providing transparent auditability and decentralization. This project addresses the challenge of securely storing and retrieving healthcare records—both hospital and patient data—on a tamper-resistant platform without exposing plaintext information on the ledger. The main objectives of proposed system are as follows:

1. Design & Implement a Proof-of-Concept for a blockchain-backed registry that encrypts healthcare data client-side and stores it on an Ethereum-compatible chain.
2. Evaluate Cryptographic Approaches by integrating PBKDF2 for key derivation and AES-CTR for encryption, analyzing their suitability and limitations in this context.
3. Demonstrate End-to-End Workflow through a Django web application that supports multiple user roles (admin, hospital, patient), showcasing secure data submission, retrieval, and presentation.
4. Identify Scalability & Security Gaps by examining in-memory caching, synchronous transaction handling, and cryptographic key management, to guide future production-grade enhancements.

## 2. LITERATURE SURVEY

### 2.1 Blockchain technologies in healthcare

In the context of healthcare and medical data, maintaining the privacy rights of individuals regarding their confidential medical information is paramount. Such sensitive data must be released with meticulous care and attention to ethical and legal considerations. Oversight and regulation are provided by frameworks such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the

United States [17] and analogous international data protection laws. These rules aim to safeguard patient privacy while facilitating the authorized and secure sharing of data that is essential to the healthcare system. Understanding these rules is essential to ensuring that people's medical records are not accessed or disclosed without authorization, protecting the privacy of their personal health information.

In parallel, emerging concepts outlined in literature, such as reference [17], offer innovative ways to facilitate convenient and secure user information sharing. These concepts are particularly relevant in healthcare and IoT medical devices. The utilization of IoT medical devices for monitoring a patient's health has witnessed a growing trend, becoming increasingly common in healthcare settings. These devices, characterized by their ability to provide real-time data on physiological parameters, offer a straightforward assessment of an individual's health status. This includes parameters like temperature, oxygen saturation, heart rate, and the capability to assess internal body temperature [18].

### 2.2 Enhancing security

The use of blockchain technology enhances the security and privacy of the data produced by Internet of Things (IoT) healthcare devices. It guarantees the privacy of sensitive health information while granting authorized parties access to relevant information when needed. This secure and transparent data management technique is by the principles of patient privacy and data protection supported by legal frameworks like HIPAA [19, 20]. Thus, collecting extensive datasets for COVID-19 research necessitates strict adherence to international laws and standards to protect patient privacy and data security. Regulatory frameworks like HIPAA play a crucial role in overseeing the release of medical records. Innovative concepts in information sharing, as outlined in Jerbi et al. [18] further advance secure data-sharing practices. Meanwhile, the increasing prevalence of IoT medical devices underscores the importance of robust data security, which can be achieved through blockchain technology integration.

Utilizing blockchain technology in conjunction with IoMT devices holds significant potential for enhancing patient privacy protections and optimizing the functionality of these devices. This integration offers numerous advantages rooted in blockchain technology's decentralized and secure nature. One of the key benefits of combining blockchain and IoMT is the bolstering of patient privacy. Blockchain's decentralized architecture ensures that sensitive health data remains secure and tamper-proof. Patient records and data can be stored on the blockchain so only authorized individuals or entities can access them. This enhances patient confidentiality and data security, aligning with regulatory requirements and ethical considerations. Furthermore, eliminating centralized intermediaries is a pivotal aspect of blockchain technology. Traditional healthcare systems often involve multiple centralized entities and organizations responsible for data management. The integration of blockchain eliminates the need for these intermediaries, streamlining the process of transmitting patient data and information across global platforms. This not only enhances data accessibility but also reduces the risk of data breaches and unauthorized access.

In a broader context, blockchain technology promotes enhanced and decentralized communication of data and information between healthcare facilities, professionals, and patients. Hospitals and healthcare providers can securely share patient records, test results, and treatment plans with patients, ensuring transparency and fostering trust in the healthcare ecosystem. Integrating blockchain with IoT-enabled devices further facilitates the seamless distribution of a patient's medical records to individuals worldwide. This means authorized parties can access relevant medical information securely and efficiently, regardless of geographical location. This is particularly valuable in emergency medical care or remote consultations, where quick access to accurate medical data is critical. A vital component of blockchain technology in IoMT is using reliable smart contracts to transfer IoMT data to the blockchain. Smart contracts automate and enforce predefined rules, ensuring data integrity and authenticity. This

enhances the system's resilience against data manipulation and fabrication, safeguarding the accuracy of medical records and treatment histories.

The inherent security features of blockchain, including cryptographic encryption and decentralized consensus mechanisms, contribute to establishing mutual trust among all participating parties in the healthcare ecosystem. Patients can trust that their data is protected, while healthcare providers can rely on the integrity of the information they access.

Alsemmeari et al. [21] focus on the implementation of a comprehensive evaluation system designed to analyze web-based healthcare apps effectively. The authors used the AHP and TOPSIS methods to compare and rank different options based on things like data integrity, auditing standards, resilience, authentication, encryption, and the ability to revoke access. Particularly, our research is consistent with the computational methodology suggested by Ahmad et al. [22] to perform an empirical inquiry into the best security practices for medical equipment. Similarly to that, the subsequent study employed AHP, hesitant fuzzy, and AHP techniques to assess several options related to criteria characteristics. Passwords, version control, software recovery, access control, biometric authentication, security tokens, backups, and error detection were among these features. In this subject, the work of Alsemmeari et al. [21] is regarded as unique. To improve the security of IoMT, they developed a robust architecture in their study that utilizes TNN and blockchain technologies. In contrast, this paper offers a brand-new framework that uniquely combines the core features and advantages of blockchain technology with artificial intelligence. To increase the number of IoT devices, IoMT systems will be provided with an automated process. This methodology aids in both the detection of ongoing cyberattacks and the process of learning from them to anticipate and predict new threats.

## 3. PROPOSED METHODOLOGY

This project offers a detailed proof-of-concept for a secure, blockchain-backed healthcare registry. It illustrates end-to-end encryption on the client side, immutable on-chain storage, and a web interface for interacting with that data. Its core architecture revolves around three pillars: AES encryption, Web3 smart-contract interaction, and Django view logic for a simple user interface. Together, these components showcase how sensitive healthcare records can be encrypted on the client side, stored immutably on an Ethereum-compatible blockchain, and then retrieved and displayed through familiar web forms.

At startup, the application establishes its cryptographic foundation by deriving a 256-bit AES key via PBKDF2 from a hard-coded password and salt. This key is used in AES-CTR mode (with a zeroed counter) to encrypt and decrypt all hospital and patient data. Although this approach ensures that plaintext never touches the blockchain, it has notable security shortcomings—namely the use of fixed credentials, lack of an initialization vector (IV) randomness, and absence of message authentication—which would need to be addressed in a production system.

Simultaneously, the module initializes a Web3 connection to a local blockchain node (for example, Ganache running at http://127.0.0.1:9545). It loads the compiled smart contract's ABI and deployed address from a JSON file and binds it to a contract object. This contract exposes functions for saving and retrieving encrypted records: saveHospital, getHospitalCount, getHospital, savePatient, getPatientCount, and getPatient. By calling these functions, the application can push new records on-chain and fetch existing ones.

Once the contract is set up, the application fetches all existing hospital and patient entries in two one-time loops at module load. For each index, it calls the contract's "get" function, Base64-decodes the returned ciphertext, decrypts it with AES-CTR, and splits the resulting string on a $ delimiter into structured Python lists (hospitalList and patientList). These in-memory lists serve as the application's

data cache, enabling quick lookups and filtering during HTTP requests—albeit at the cost of thread-safety and scalability.

The Django view layer then provides a series of simple GET and POST handlers to support three user roles: Admin, Hospital, and Patient/User. GET views render HTML templates for login screens, "add record" forms, and dashboard pages. POST views process form submissions: they authenticate users by comparing submitted credentials against the cached lists (or hard-coded admin credentials), and they allow new records to be added by concatenating form fields with $, encrypting and Base64-encoding the result, and sending it to the blockchain via a transaction. Upon mining, the transaction receipt is displayed back to the user, and the local cache is updated.

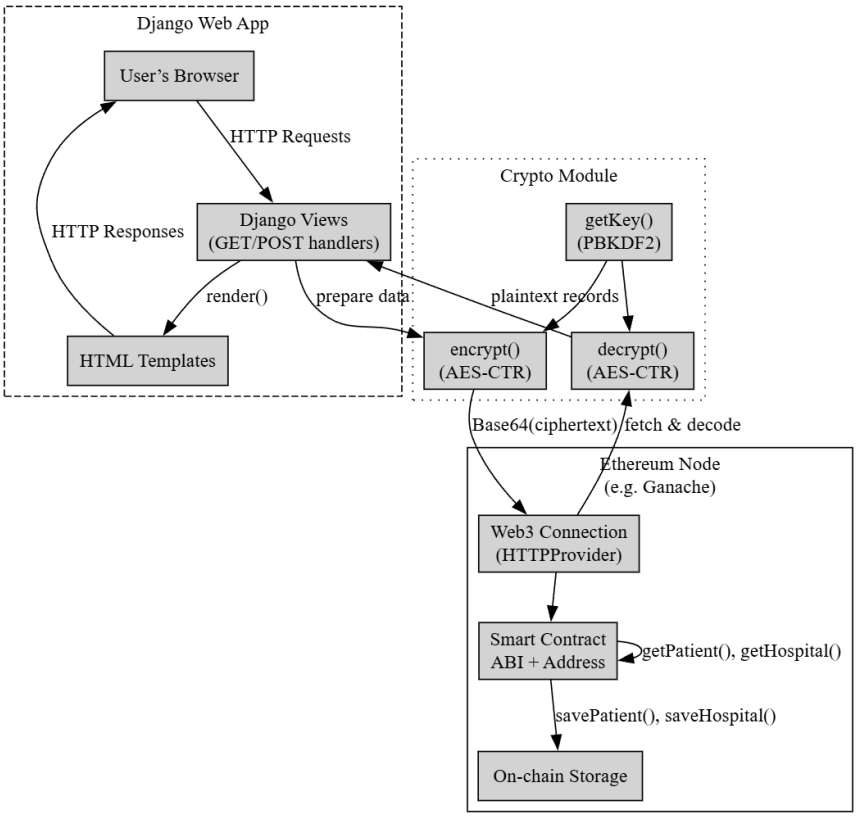



Fig. 3: System architecture of proposed AI-enabled blockchain system for securing medical data.

For data display, the application builds HTML tables via Python string concatenation, embedding each record's fields in table rows. Users can view only their own records: Patients see their own healthcare visits, Hospitals see patients associated with their facility, and Admins see the full list of registered hospitals. While this approach keeps the UI code minimal, it bypasses Django's templating safeguards and would need refactoring to prevent injection vulnerabilities.

### 4.1 Ethereum Blockchain

In this project, the "blockchain server" is really your local Ethereum-compatible node (e.g., Ganache or a geth/parity instance) together with the Web3 client code that runs in your Django app. Its role is to provide an RPC endpoint for sending transactions and querying on-chain data. Internally, the system begins by running a local Ethereum node at http://127.0.0.1:9545, which maintains the blockchain state, processes new blocks, and exposes JSON-RPC methods such as eth_sendTransaction, eth_call, and eth_getTransactionReceipt. The Django application then establishes a connection to this node via Web3's HTTPProvider, setting web3.eth.defaultAccount to the first unlocked account so that all

subsequent transact() calls automatically use that account. Next, the compiled contract JSON (Governance.json) — containing ABI and bytecode metadata — is loaded and paired with its deployed address to create a Web3 contract object whose methods mirror the smart contract's functions. When data needs to be read, calls like contract.functions.getPatientCount().call() and contract.functions.getPatient(i).call() issue eth_call RPCs, causing the node to execute the contract code locally (without changing state) and return the stored Base64-encoded ciphertext. Finally, writing data involves invoking methods such as contract.functions.savePatient(encrypted).transact(), which creates and signs a transaction using the default account, sends it via eth_sendTransaction, and then, in development mode, waits for the node to mine the transaction into a block; web3.eth.waitForTransactionReceipt(tx_hash) polls eth_getTransactionReceipt until mining is complete and then returns a receipt detailing gas usage and status.

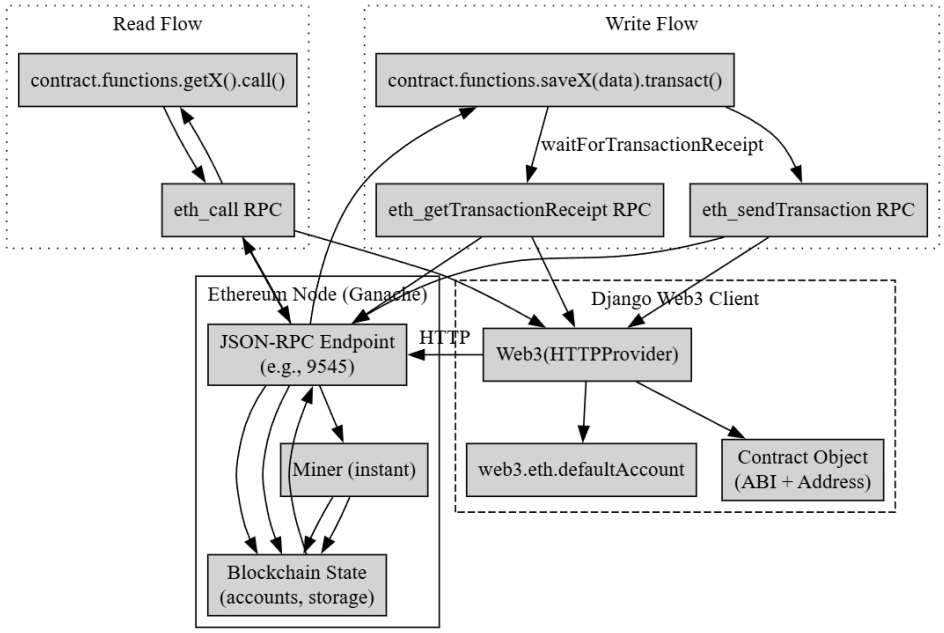



Fig. 4: Proposed AI-enabled blockchain system internal operation.

## 4. RESULTS AND DISCUSSION

Upon successful login, Fig. 5 demonstrate the admin page greeted with a dashboard that lists available tasks: "Add Hospitals," "View Hospitals," and "Logout." These tasks are presented as large, clearly labeled buttons or cards. The dashboard also displays a welcome message (e.g., "Welcome, admin") and include a sidebar with navigation links for quick access. This form allows the admin to register a new hospital on the blockchain. It contains labeled fields for Hospital Name, Specialty, Contact Number, Email, Address, Username, and Password. A "Submit" button at the bottom encrypts the input data and invokes the smart contract to store it on-chain. Mandatory fields are marked with an asterisk. After submitting the "Add Hospital" form, Fig. 6 displays a success message along with transaction details from the blockchain receipt—transaction hash, block number, and gas used. A "Back to Dashboard" button allows the admin to return to the main menu.

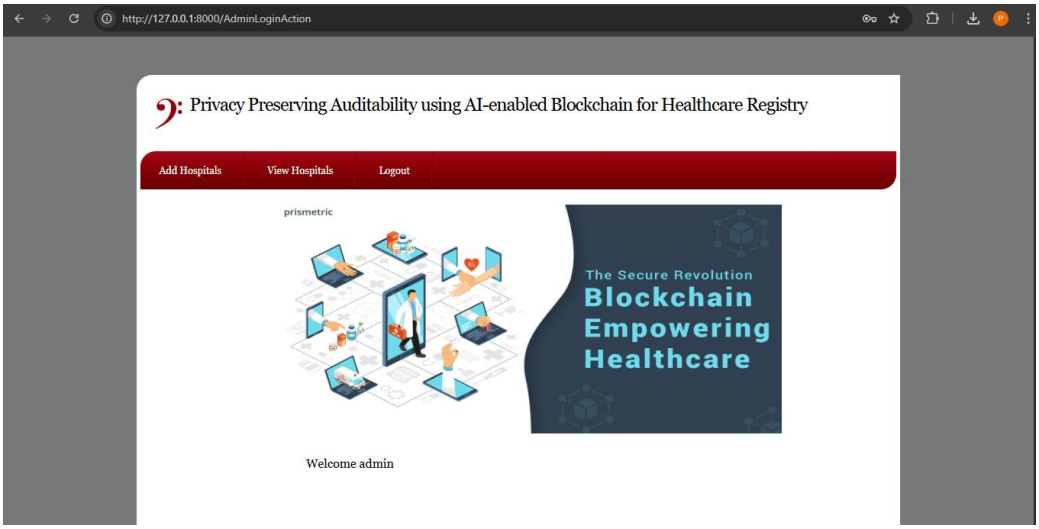



Fig. 5: Admin dashboard with tasks (add hospitals, view hospitals, and logout).

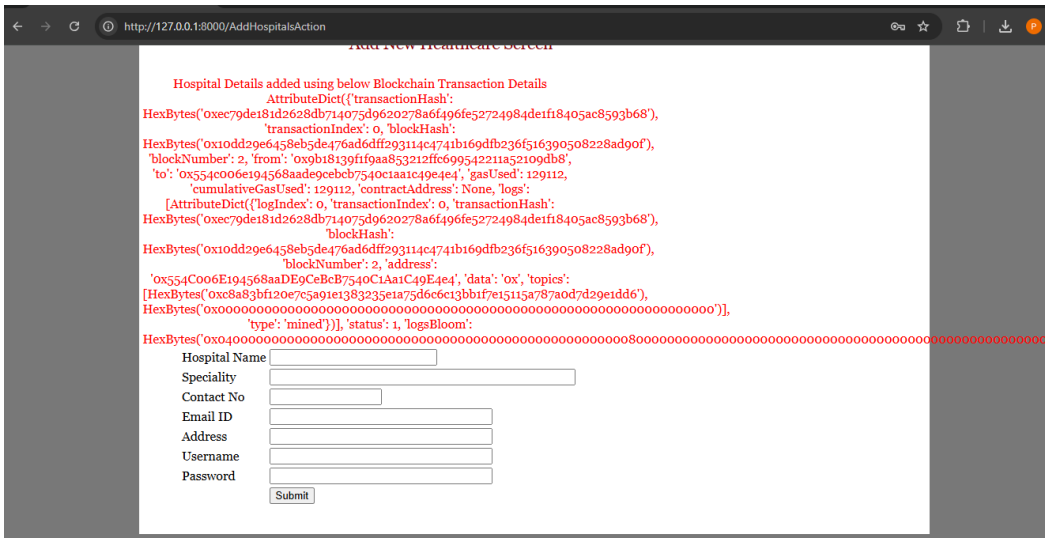



Fig. 6: Successful signup of hospital details into Blockchain server.


Fig. 7: View hospitals page.

Fig. 7 renders an HTML table listing all registered hospitals. Columns include Hospital Name, Specialty, Contact Number, Email, Address, Username, and Password (if stored). The data is fetched from the blockchain, decrypted, and displayed in a paginated, sortable table for easy browsing. Similar in layout to the admin login,

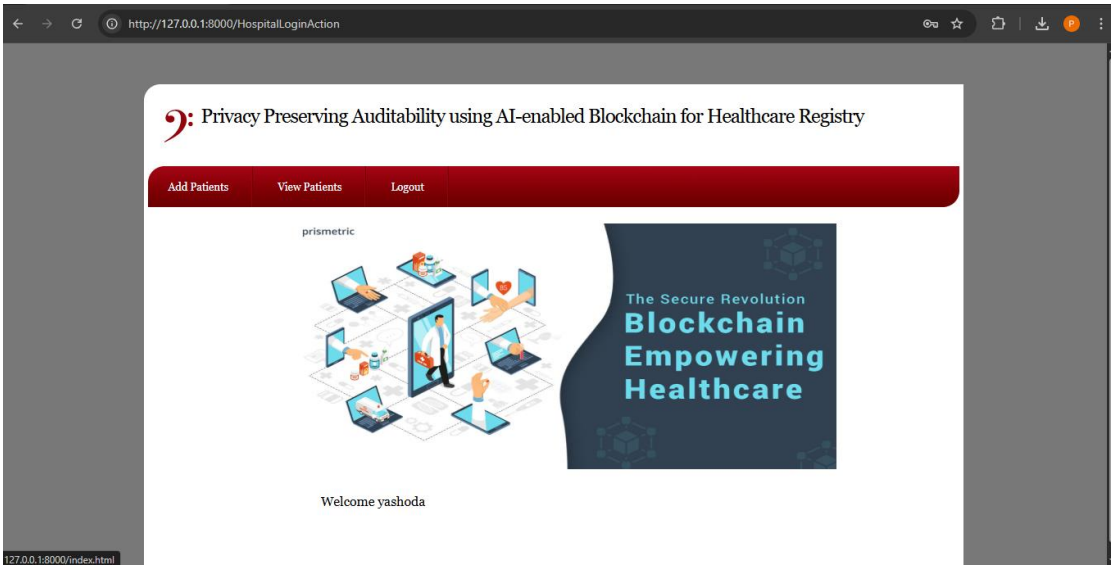



Fig. 8: Hospital dashboard with add patients, view patients and logout.

Upon logging in, Fig. 8 shows hospital users dashboard with three main actions: “Add Patients,” “View Patients,” and “Logout.” Each action is represented by a button or tile. A personalized greeting (e.g., “Welcome, [HospitalName]”) appears at the top. After submitting the “Add Patient” form—which captures Patient Name, Disease, Gender, Contact, Doctor, Prescription, Address, Visit Date, and Patient Username— Fig. 9 shows the blockchain transaction receipt. It confirms that the patient record has been encrypted and successfully committed to the ledger.

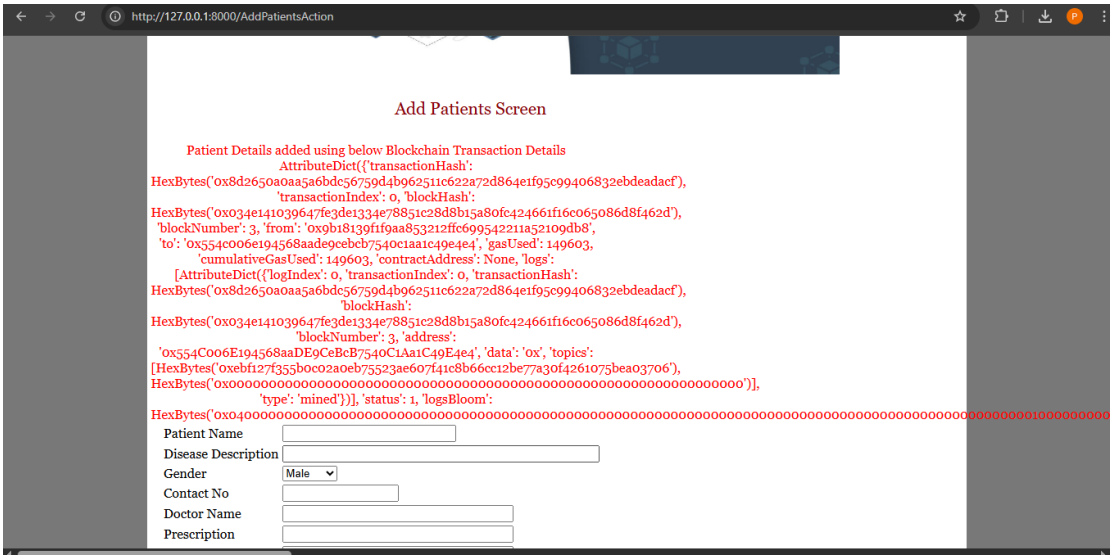
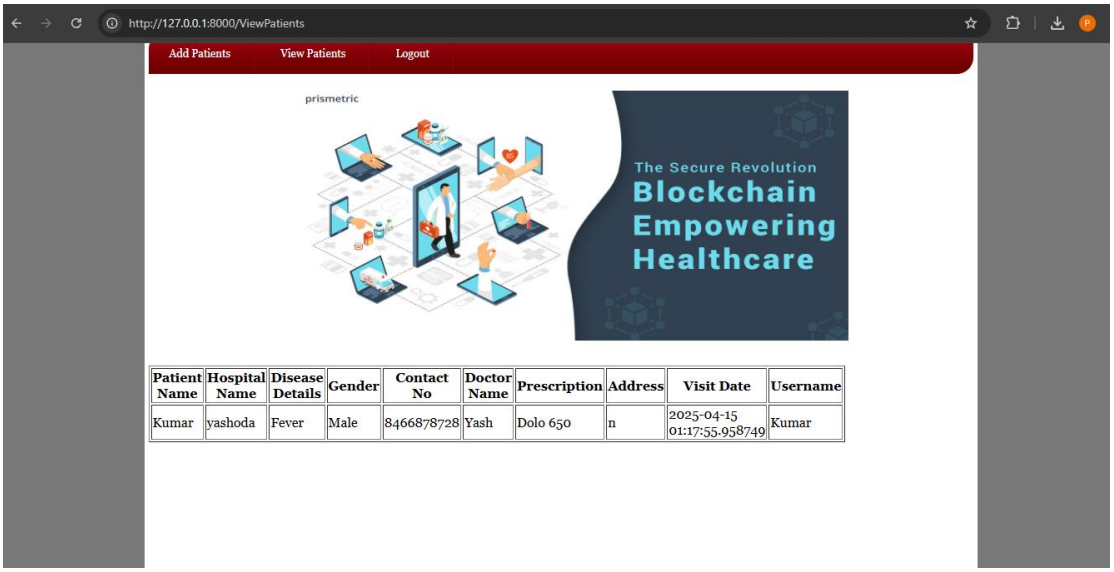


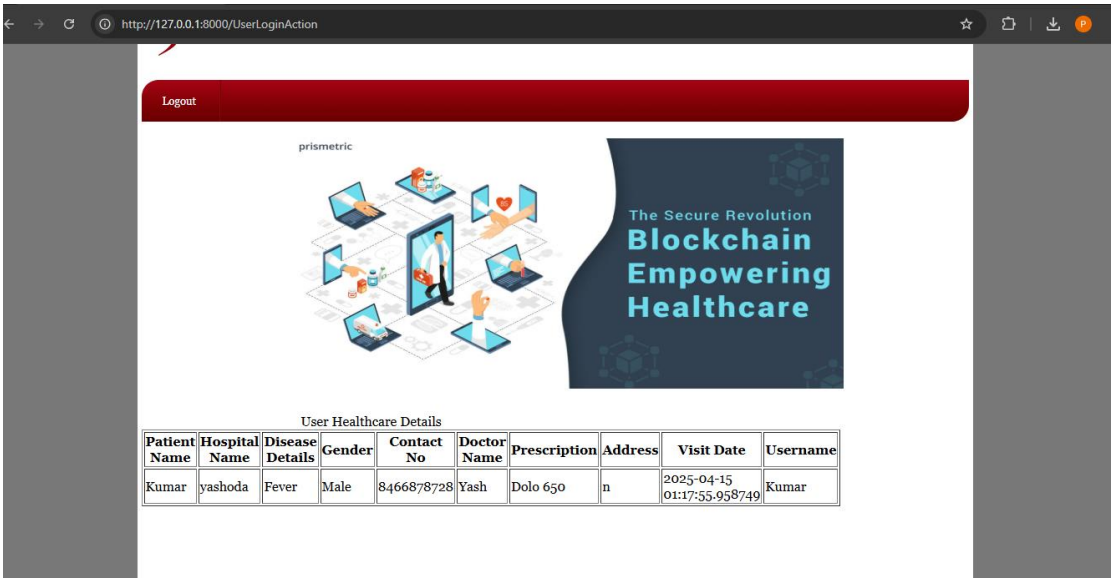

Fig. 9: Added patient and details are stored in Blockchain server.




| Patient Name | Hospital Name | Disease Details | Gender | Contact No | Doctor Name | Prescription | Address | Visit Date | Username |
|---|---|---|---|---|---|---|---|---|---|
| Kumar | yashoda | Fever | Male | 8466878728 | Yash | Dolo 650 | n | 2025-04-15 01:17:55.958749 | Kumar |

Fig. 10: View patient's page.

Fig. 10 displays a decrypted, tabular list of all patients associated with the logged-in hospital. Columns include Patient Name, Disease, Gender, Contact, Doctor, Prescription, Address, Visit Date, and Patient Username. Pagination controls allow navigating large record sets. Fig. 11 shows the upon login, patients see their own medical history in a clean table, mirroring the "View Patients" interface but filtered to their username. Each record row shows Date of Visit, Hospital Name, Disease Details, Doctor, Prescription, and Contact Information. A "Logout" button allows the patient to end the session.




| Patient Name | Hospital Name | Disease Details | Gender | Contact No | Doctor Name | Prescription | Address | Visit Date | Username |
|---|---|---|---|---|---|---|---|---|---|
| Kumar | yashoda | Fever | Male | 8466878728 | Yash | Dolo 650 | n | 2025-04-15 01:17:55.958749 | Kumar |

Fig. 11: Patient information page after successful login.

## 5. CONCLUSION

This project demonstrates a comprehensive proof-of-concept for a secure, decentralized healthcare registry that combines client-side encryption with blockchain immutability. By deriving a 256-bit AES key through PBKDF2 and encrypting all hospital and patient data in AES-CTR mode, the system ensures that only ciphertext is ever stored on-chain, preserving confidentiality even in a transparent ledger environment. The integration of Web3.py and a local Ethereum node illustrates how smart contracts can manage encrypted records—supporting functions to add, retrieve, and count entries—

while Django provides a familiar web interface for patients, hospitals, and administrators. Throughout development, the design highlighted critical trade-offs: the simplicity of in-memory caching versus the need for scalable data stores, the performance benefits of synchronous transaction handling versus the desirability of non-blocking, asynchronous patterns, and the security implications of a fixed AES counter versus best practices around randomized nonces and authenticated encryption. While the current implementation effectively showcases end-to-end encryption, on-chain storage, and role-based data access, it also surfaces areas for hardening. Production readiness will require externalizing and rotating cryptographic secrets, adopting AES-GCM or HMAC for data integrity, replacing globals with a robust database or cache layer, and implementing asynchronous transaction workflows to improve responsiveness. Moreover, smart contract security audits and operational governance—covering node redundancy, key management, and compliance reporting—are essential to meet real-world regulatory standards. By addressing these enhancements, this architecture can evolve into a scalable, secure platform that empowers patients with privacy controls and institutions with verifiable audit trails, ultimately fostering greater trust in digital healthcare ecosystems.

Extend the system to support patient-controlled consent management via smart contracts and integrate a permissioned blockchain for scalable, low-cost operations. Incorporate off-chain indexing and zero-knowledge proofs to enable selective data sharing without revealing sensitive details.

## REFERENCES


[1] Gugueoth, V., Safavat, S., Shetty, S. & Rawat, D. A review of iot security and privacy using decentralized blockchain techniques. *Comput. Sci. Rev.* **50**, 100585 (2023).

[2] Peres, R., Schreier, M., Schweidel, D. A., & Sorescu, A. Blockchain meets marketing: Opportunities, threats, and avenues for future research (2023).

[3] Khang, A., Rana, G., Tailor, R., & Abdullayev, V. Data-centric ai solutions and emerging technologies in the healthcare ecosystem (2023).

[4] Villarreal, E. R. D., Garcia-Alonso, J. & Moguel, E. Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access* **11**, 5629–5652 (2023).

[5] Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K. & Siddique, A. H. Blockchain application in healthcare systems: A review. *Systems* **11**(1), 38 (2023).

[6] Androulaki, E. et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference; EuroSys '18; Association for Computing Machinery*, pp. 30:1–30:15 (New York, NY, USA, 2018).

[7] Ahram, T. *et al.* Blockchain Technology Innovations. In *Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA*, 8–10 June 2017; pp. 137–141.

[8] Dagher, G. G., Mohler, J., Milojkovic, M. & Marella, P. B. Ancile: Privacy-preserving frame work for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **39**, 283–297 (2018).

[9] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. MedRec: Using blockchain for medical data access and permission management. In *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria*, 22–24 August 2016; pp. 25–30 (2016).

[10] Li, H. *et al.* Blockchain-based data preservation system for medical data. *J. Med Syst.* **42**, 141 (2018).

[11] Li, R. *et al.* Blockchain for large-scale internet of things data storage and protection. *IEEE Trans. Serv. Comput.* **12**(5), 762–771 (2018).

[12] Fan, K., Wang, S., Ren, Y., Li, H. & Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **42**, 1–11 (2018).

[13] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. In *Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Sicily, Italy*, 18–20 June 2018, pp. 49–56 (2018).

[14] Zhang, P., White, J., Schmidt, D. C., Lenz, G. & Rosenbloom, S. T. FHIRChain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **16**, 267–278 (2018).

[15] Xia, Q. *et al.* MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **5**, 14757–14767 (2017).

[16] McGhin, T., Choo, K.-K.R., Liu, C. Z. & He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **135**, 62–75 (2019).

[17] O'Donoghue, O., Vazirani, A. A., Brindley, D. & Meinert, E. Design choices and trade-offs in health care blockchain implementations: Systematic review. *J. Med. Internet Res.* **21**(5), 1 (2019).

[18] Jerbi, W., Cheikhrouhou, O., Guermazi, A., Hamam, H., & Trabelsi, H. A blockchain based authentication scheme for mobile data collector in iot. In *2021 International Wireless Communications8 and Mobile Computing (IWCMC)*, pp. 929–934 (IEEE, 2021).

[19] Abbas, S., Al Hejaili, A., Sampedro, G. A., Abisado, M., Almadhor, A., Shahzad, T., & Ouahada, K. A novel federated edge learning approach for detecting cyberattacks in iot infrastructures. *IEEE Access* (2023).

[20] Shachar, C., Cadario, R., Cohen, I. G. & Morewedge, C. K. Hipaa is a misunderstood and inadequate tool for protecting medical data. *Nat. Med.* **1**, 1–3 (2023).

[21] Alsemmeari, R. A., Dahab, M. Y., Alsulami, A. A., Alturki, B. & Algarni, S. Resilient security framework using tnn and blockchain for iomt. *Electronics* **12**(10), 2252 (2023).

[22] Ahmad, M. *et al.* Healthcare device security assessment through computational methodology. *Comput. Syst. Sci. Eng.* **41**(2), 1 (2022).