Journal of Science Engineering Technology and Management Science
Volume 02, Issue 08, August 2025 *ISSN: 3049-0952*
www.jsetms.com *DOI: 10.64771/jsetms.2025.v02.i08.602-612*

A BLOCKCHAIN ENABLED TAMPER PROOF APPROACH FOR ENHANCED MEDICAL DATA INTEGRITY AND ACCESS CONTROL

Ch. Aruna[1], T. Varsha[2], C. Shivakumar[2], Mankala Sreeja[2], B. Badri Nath[2]
[1] Assistant Professor, [2]UG Student, [1,2] Department of Computer Science and Engineering
[1,2] Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, 501510, Telangana.

To Cite this Article
Ch. Aruna, T. Varsha, C. Shivakumar, Mankala Sreeja, B. Badri Nath, "A Blockchain Enabled Tamper Proof Approach For Enhanced Medical Data Integrity And Access Control", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 08, August 2025,pp: 602-612, DOI: http://doi.org/10.64771/jsetms.2025.v02.i08.pp602-612
Submitted: 15-07-2025 *Accepted: 21-08-2025* *Published: 28-08-2025*

ABSTRACT
In modern healthcare systems, the centralized storage of electronic health records (EHRs) and associated documents presents significant vulnerabilities, including single points of failure, data tampering, and privacy breaches. This research proposes a decentralized framework that integrates blockchain technology with the InterPlanetary File System (IPFS) to securely manage doctor–patient appointment data, medical reports, prescriptions, and feedback. The system utilizes a permissioned Ethereum-style smart contract, named "Healthcare," to immutably store user profiles, appointment metadata, prescription references, and patient ratings. Sensitive medical files are encrypted using AES-CTR mode, with encryption keys derived via PBKDF2, and pinned to a local IPFS node to ensure both confidentiality and decentralized availability. Patients can register and log in, browse a list of doctors with on-chain average ratings, and book appointments by uploading encrypted medical reports. Later, they can securely download prescriptions in decrypted form. Doctors access the platform to view pending appointments, retrieve patient reports, issue encrypted prescriptions, and publish them on-chain. Patient feedback is also recorded as immutable blockchain transactions. To improve system responsiveness, an in-memory Python cache is synchronized with the blockchain, enabling fast read operations without repeatedly querying the chain. Experimental results demonstrate that the encryption, IPFS pinning, and decryption processes operate within acceptable performance thresholds. The proposed system enhances data integrity, transparency, and fault tolerance: no single authority can alter records without detection, and encrypted files remain retrievable even if specific nodes fail. By combining decentralized metadata storage with secure, off-chain encrypted file handling, this framework offers a robust, patient-centric solution to modern EHR management challenges.

1. INTRODUCTION

The integration of digital healthcare with the Internet of Medical Things (IoMT) has transformed healthcare delivery, particularly through the use of Electronic Medical Records (EMRs), which store vital patient data including diagnostic images that now account for 80% of EMR data—creating major challenges in storage, security, and data sharing. Traditional centralized doctor–patient appointment systems are prone to failures, data tampering, and privacy breaches, as seen in high-profile cyberattacks like the WannaCry ransomware and Anthem data breach. To address these

vulnerabilities, this research proposes a decentralized system combining blockchain, AES-CTR encryption, and IPFS to securely manage user data, appointments, prescriptions, and feedback. The blockchain ensures immutable, time-stamped records of all interactions, while encrypted medical files are stored off-chain in IPFS, ensuring confidentiality and decentralization. The system enables transparent and tamper-proof appointment booking, prescription issuance, and doctor rating submission, all through a Django-based web interface. Research objectives include designing smart contracts for data integrity, implementing robust encryption modules, and ensuring real-time UI updates through synchronized in-memory caches.

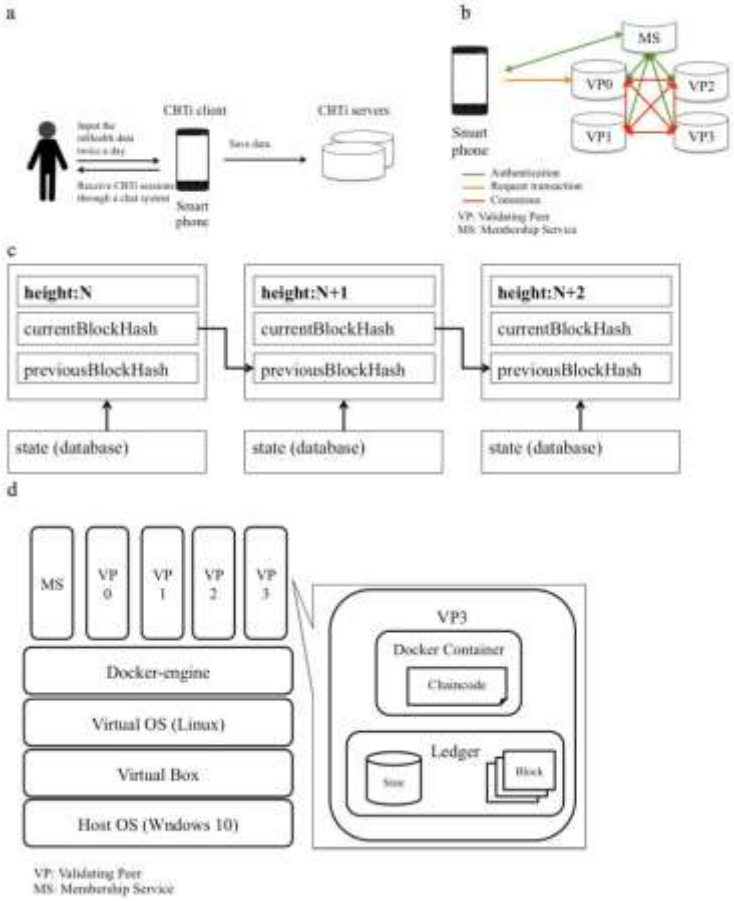


Figure 1: Blockchain based working application

Its significance lies in delivering immutable audit trails, protecting patient privacy, enabling decentralized trust, ensuring resilience and scalability, and serving as a model for future decentralized healthcare applications. The system has wide-ranging applications including appointment and EHR management, secure telemedicine, interoperable health data exchange, pharmacy prescription verification, auditable clinical research, and regulatory compliance—ultimately empowering patients while safeguarding sensitive health information in a transparent and tamper-proof ecosystem.

2. LITERATURE SURVEY

Security in the context of medical data and health information refers to the protection of sensitive patient information from unauthorized access, use, or disclosure. It encompasses various measures to safeguard the confidentiality, integrity, and availability of health data [**9**]. Privacy, on the other hand, is a specific aspect of security that focuses on enforcing rules regarding how private information is stored and shared. Medical data privacy is important because it ensures that patients have control over who can access their health information and how it is used. This helps to maintain confidentiality and prevent the unauthorized use or disclosure of medical data, which can lead to identity theft, discrimination, and other negative consequences [**9**]. Therefore, attempts to create policies and

regulations have been developed in various countries. For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 consists of federal laws that protect the privacy and security of health information in the U.S. These rules ensure that individuals have rights over their health information, and they require specific protections to safeguard electronic health information [**10**]. All companies operating in the healthcare industry in the U.S. must comply with HIPAA regulations. This includes healthcare providers, health plans, healthcare clearinghouses, and their business associates. The HIPAA provides a comprehensive set of guidelines for ensuring the privacy and security of health information [**3**]. The key guidelines comprise a security rule, privacy rule, breach notification rule, and enforcement rule. The security rule outlines the security standards to protect electronic protected health information (ePHI). It includes administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI. The privacy rule establishes national standards for protecting individuals' medical records and other personal health information. It governs the use and disclosure of PHI and grants a patient their rights over their own health information. In the event of a breach involving unsecured PHI, entities that comply with the HIPAA are required to notify affected individuals, the Secretary of Health and Human Services, and, in some cases, the media. Enforcement rules outline procedures for investigating complaints and the penalties for non-compliance with HIPAA regulations [**3**,**11**].

Accordingly, the privacy and security of HISs are crucial to ensure the confidentiality of a patient's personal information and to prevent potential security breaches that may compromise the integrity of the data. Additionally, access control tools and extensive training are essential for securing patient information and protecting confidentiality [**10**]. The organization and implementation of security and privacy in HISs can vary significantly depending on the country and the type of provider or user. This variation is primarily due to differences in legal frameworks, cultural attitudes toward privacy, technological infrastructure, and the specific needs of healthcare providers and users. For example, the European Union's General Data Protection Regulation (GDPR) is one of the most comprehensive and stringent privacy laws, impacting how companies worldwide handle the data of EU citizens [**12**]. In contrast, the United States has a more sector-specific approach, with laws like the HIPAA for healthcare data and the Children's Online Privacy Protection Act (COPPA) for protecting data for children. On the other hand, Australia's approach to health information privacy is outlined in the Privacy Act 1988, which includes the Australian Privacy Principles (APPs) [**12**]. These principles cover a broader spectrum of personal information compared to the U.S.'s HIPAA and apply to a wider range of entities, including all private health service providers [**12**].

In the context of HISs, approval and control of whether rules, requirements, and guidelines are followed, including the conducting of audits and inspections, are overseen by various regulatory bodies and government agencies. For instance, the HIPAA sets standards for the storage, sharing, and management of health information, and the Office of the Inspector General is involved in enforcing compliance through audits and investigations [**13**]. Furthermore, validation of HISs increasingly includes aspects of security and privacy. This is essential given the sensitive nature of health data and the evolving cybersecurity threat landscape. Modern validation methodologies for e-health systems focus on ensuring that security and privacy policies are effectively integrated and compliant with relevant regulations and standards. These methodologies typically involve a combination of technological advancements, adherence to legal frameworks, and the application of best practices in data security and privacy management. The goal is to ensure the confidentiality, integrity, and availability of health data throughout its lifecycle, from collection to storage and processing. The validation process often includes rigorous testing and assessment of security measures, privacy protocols, and compliance with laws like the HIPAA in the U.S. or the GDPR in the EU. This approach is crucial to safeguarding patient data against unauthorized access, breaches, and other security incidents [**13**].

In the landscape of Health Information Systems (HISs), regulatory bodies such as the U.S. Food and Drug Administration (FDA) and the European Medicines Agency (EMA) play pivotal roles. These organizations are fundamental in establishing and enforcing standards that ensure the safety, efficacy, and privacy of health technologies. The FDA, in the United States, oversees the regulation of medical devices, which include software and hardware used in HISs. It sets forth guidelines that dictate how these technologies should be developed, tested, and implemented to protect patient data and ensure system integrity. Similarly, the EMA in the European Union performs an analogous function, focusing on the evaluation and supervision of medicinal products, thereby extending its influence to the technologies employed in healthcare settings across Europe [**14**].

These regulatory bodies also have a significant impact on how HIS technologies evolve and are adopted in healthcare practices. By setting stringent requirements for compliance, they influence the design and functionality of HIS technologies, prioritizing patient data security and privacy. Compliance with these regulations is not just a legal obligation but also a critical factor in gaining trust and acceptance among healthcare providers and patients. While these agencies primarily aim to protect public health, their guidelines also spur innovation, as developers and providers strive to create solutions that meet these rigorous standards without compromising on efficiency and user experience. Thus, the function and position of the FDA, EMA, and similar regulatory bodies are integral to the development and deployment of secure and privacy-compliant HIS technologies

3. PROPOSED METHODOLOGY

This research module introduces a blockchain-integrated doctor–patient appointment system that combines AES-CTR encryption, IPFS for decentralized file storage, and Ethereum-style smart contracts via Web3 for secure and transparent data management. When patients upload medical reports or doctors issue prescriptions, the files are encrypted using a derived AES key, stored in IPFS, and their references are recorded on the blockchain for integrity. The system connects to local IPFS and Ethereum nodes, initializing smart contracts and caching user, rating, and appointment data in memory to optimize access and reduce repeated blockchain reads. All user metadata, reviews, and electronic health records (EHRs) are stored on-chain within a “Healthcare” smart contract, ensuring tamper-proof and transparent recordkeeping. AES-CTR encryption safeguards file contents, which remain off-chain in IPFS, ensuring both security and decentralization. This architecture supports various user flows including registration, appointment booking, rating submissions, and EHR updates while ensuring secure, decentralized access control to sensitive healthcare information.

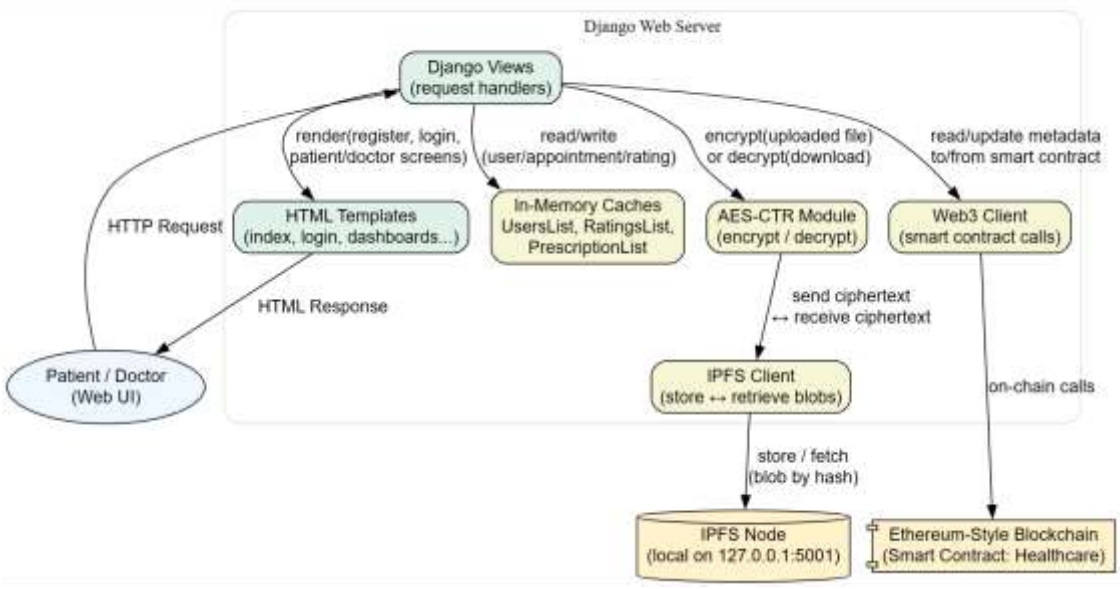


Figure 2: Proposed block diagram of blockchain-based medical data integrity and access control.

Registration and Login

registration page where new visitors can sign up by entering details such as username, password, contact number, email, address, a brief description, government ID, and their role as either "Patient" or "Doctor." Upon submission, the server verifies that the chosen username is not already registered on the blockchain; if it's unique, a saveUser transaction is submitted to permanently store the user's details on-chain, and the in-memory user list is updated accordingly. A confirmation message is then displayed, optionally including the transaction receipt. For authentication, the system offers two distinct login pages for patients and doctors, each requiring a username and password. Upon login, the server checks the in-memory user list for a matching credential pair and validates the role. If the credentials are correct, the system stores the username in a module-wide "current user" variable (without using sessions or cookies) and redirects the user to the appropriate dashboard; otherwise, an error message is shown and the login form is reloaded.

Patient Dashboard

Once a patient logs in, they are presented with a dashboard offering options such as booking a new appointment or viewing past appointments and prescriptions. To book an appointment, the patient fills out a form pre-filled with their name, inputs disease details, uploads a medical report, and selects a doctor. Upon submission, the system encrypts the report using AES-CTR, uploads the ciphertext to IPFS to obtain a unique content hash, and creates a new blockchain transaction to store an Electronic Health Record (EHR) containing the patient and doctor names, disease description, IPFS hash with filename, a placeholder for prescription, and a timestamp. The new entry is also added to the in-memory appointment list for immediate visibility, and the patient receives a confirmation with an appointment ID. When viewing their appointment history, patients see a table listing all EHR entries associated with their username, including patient and doctor names, disease details, truncated IPFS hashes, report filenames, prescription details (if issued), and booking dates. If prescriptions are available, download links for both the report and prescription appear, which invoke a backend function that retrieves the encrypted file from IPFS, decrypts it using AES, and delivers the original file as a downloadable response.

Doctor Dashboard

Once a doctor logs in, they are presented with a dashboard offering options such as viewing appointments, generating prescriptions, and checking their ratings. By selecting "View Appointments," the doctor sees a table populated from the in-memory list of Electronic Health Records (EHRs) where their username matches the doctor field. Each entry includes the appointment ID, patient name, disease description, a truncated IPFS hash with the report filename, any existing prescription details (or "None" if not yet issued), and the booking timestamp. Actionable options include viewing the patient's report (decrypted and downloaded from IPFS) and, if no prescription exists, generating one via a form that allows the doctor to enter prescription instructions and upload a file. Upon submission, the prescription file is encrypted using AES, uploaded to IPFS, and a blockchain transaction updates the appointment record with the prescription text, filename, and IPFS hash. The in-memory list is updated immediately to reflect the change, and a confirmation message is displayed. Additionally, the dashboard allows doctors to view their ratings, which are computed as the average of all numeric review scores from patients stored in memory, with a default of five stars shown if no reviews exist.

Proposed Workflow

The blockchain-based medical data integrity and access control system operates through a seamless workflow beginning with user registration, where visitors provide their personal details and role (Patient or Doctor); the server checks for duplicates in the in-memory list and, if unique, stores the information on-chain via a smart contract and updates the in-memory users list. During login, patients

and doctors authenticate using their credentials, and upon successful validation, are redirected to their respective dashboards. Patients can view doctors and book appointments by submitting disease details and uploading encrypted medical reports, which are stored on IPFS, with metadata saved on the blockchain. Doctors, upon logging in, can view their appointments and either access the encrypted medical reports or generate prescriptions by submitting encrypted files and associated details, which are similarly stored in IPFS and updated on-chain. Patients can later view and download both medical reports and prescriptions from their dashboard, with all files being decrypted securely by the server. Additionally, patients can provide feedback by submitting reviews and ratings for doctors, which are saved on-chain and dynamically reflected in future appointment views. Throughout the system, user session state is maintained via a global variable, and in-memory lists are updated in real-time and persist until the server is restarted, after which data is reloaded from the blockchain, ensuring continuity and decentralized data integrity.

Figure 3: Proposed workflow of blockchain-based medical data integrity and access control system.

Key Derivation & AES-CTR Encryption/Decryption

To securely encrypt and decrypt uploaded files, the system first derives a 256-bit AES key using PBKDF2 (Password-Based Key Derivation Function 2) with a fixed password and salt. Once the key

is generated, AES in Counter (CTR) mode is employed: plaintext bytes are XORed with a stream generated by encrypting successive counter values. Decryption simply reverses that process using the same key and counter. This ensures that both encryption and decryption share identical steps—differing only in the direction of the data flow through the AES-CTR engine.

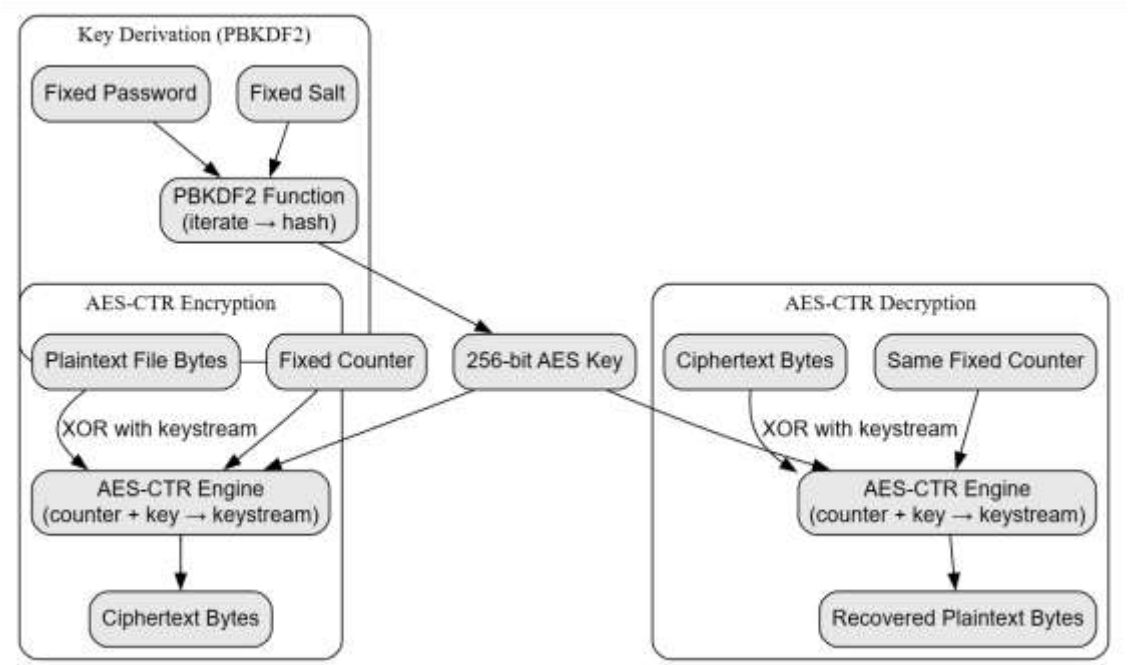


Figure 4: Key derivation and AES-CTR workflow.

IPFS Storage and Retrieval

Once a file has been encrypted, it must be stored in a decentralized, content-addressable manner. The IPFS client takes encrypted bytes, pins them to a local IPFS node, and returns a unique content hash. Later, when retrieving the file, the IPFS client fetches the ciphertext using that hash. Finally, the ciphertext is handed back to the AES decryption module so the original bytes can be recovered. This workflow abstracts away local filesystem storage and relies entirely on IPFS's distributed hash table.

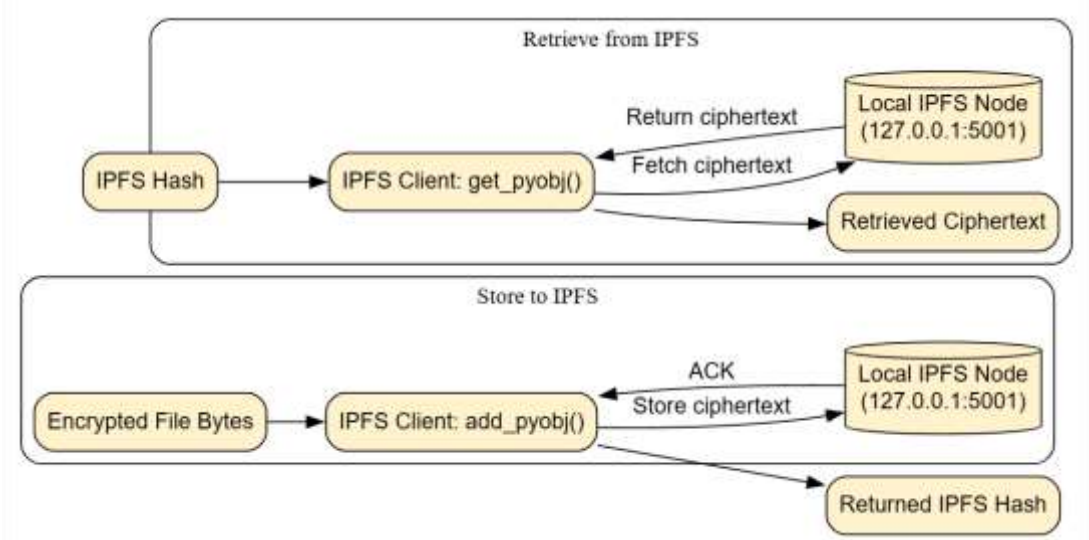


Figure 5: IPFS workflow.

Smart Contract Data Operations

All user, appointment, prescription, and rating metadata is stored on the Ethereum-style "Healthcare" smart contract. Four primary operations occur: registering a new user (saveUser), adding an appointment/EHR (saveEhr), updating a prescription (updatePrescription), and saving a rating

(saveRating). Each involves packaging relevant fields into a transaction, waiting for the blockchain to confirm it, then mirroring the update in the server's in-memory list. This ensures the server always reflects the on-chain state without re-fetching all data on every request.

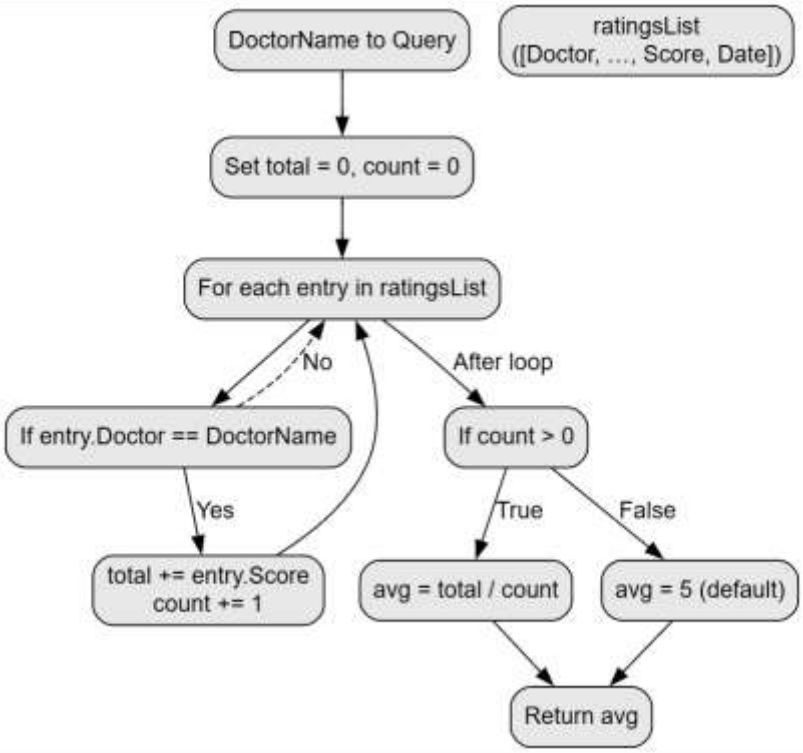


Figure 6 : Rating calculation algorithm.

Rating Calculation Algorithm

To display each doctor's average rating, the system iterates through the in-memory list of all rating entries. For a given doctor name, it sums up every numeric rating where the doctor matches and counts how many entries were found. If no ratings exist, a default value (e.g., 5) is returned. Otherwise, the average is calculated as total ÷ count. This procedure runs each time the "Book Appointment" page lists all doctors, allowing patients to see up-to-date average scores.

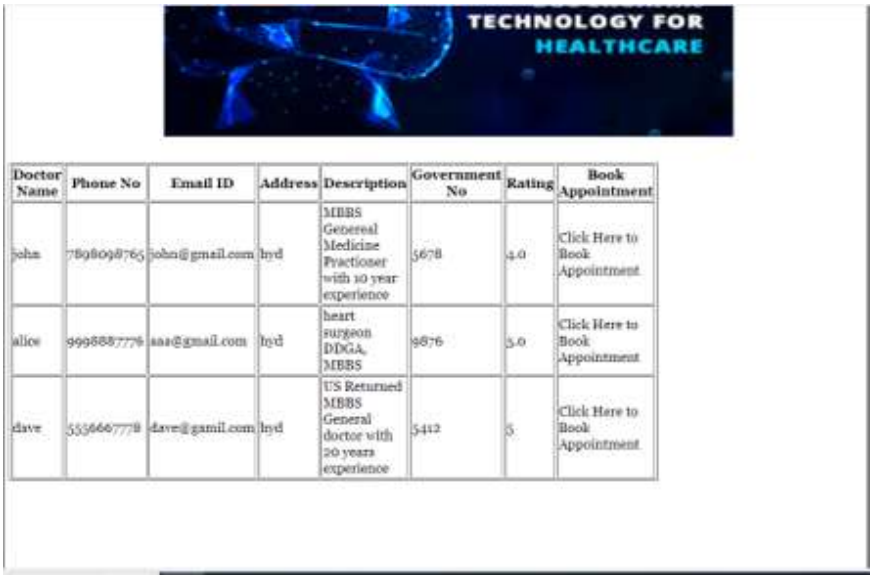
4. RESULTS

When the "New User Signup" link is clicked, the system presents a vertically structured registration form (as shown in Fig. 9.2) designed to collect all essential user details for storing in the on-chain "Users" array. The form includes fields such as Username (with a placeholder like "___"), Password (masked input), Contact Number (e.g., " "), Email ID (e.g., " ____@gmall.com"), Address (free-text input), Self Description (a multiline field, e.g., "25 years suffering from headache"), Identification Number (e.g., a government-issued ID like "#####"), and User Type (a dropdown menu with "Doctor" or "Patient," where "Doctor" is selected by default in the example). Upon clicking the "Signup" button, the backend system uses PBKDF2 to derive an AES key, encrypts any applicable uploaded data, and invokes the saveUser(...) function on the smart contract to store all entered attributes on-chain. If the username is already taken, the form returns an error message; otherwise, the user is added to the in-memory usersList cache, and a success message is displayed on the interface, confirming successful registration.

Figure 7: Signup page of proposed blockchain-based EHR management system.

Figure 8: Patient login page of proposed blockchain-based EHR management system.

Figure 8 illustrates the Patient Login Screen, where registered patients authenticate by entering their username and password—fields include a plain-text username input (e.g., "suresh") and a masked password field, with a clearly labeled "Login" button beneath. Upon clicking "Login," the Django function PatientLoginAction verifies the entered credentials against the in-memory user list, ensuring the username exists, the password matches, and the user type is "Patient." If valid, the system sets the global username variable and redirects the user to the patient dashboard (Fig. 9.4); otherwise, an "Invalid login details" error appears, prompting the patient to retry. The patient dashboard presents four main options: (1) "View Doctors List" displays all doctors (from usersList) alongside their average ratings (calculated from ratingsList), (2) "View Prescriptions" links to the patient's complete appointment history with options to decrypt/download prescription files via IPFS and AES decryption, (3) "Feedback & Ratings" enables patients to select a doctor from a dropdown, write a review, assign a numeric rating, and store this data on-chain using saveRating(...), and (4) "Logout" ends the session by clearing the global username and returning to the home screen. When "View Doctors List" is selected, a sortable table appears (as seen in Fig. 9.5) containing columns such as Doctor Name, Phone No, Email ID, Address, Description, Government No, Rating (default 5 if unrated), and a "Click Here to Book Appointment" link. Clicking this link redirects to an appointment form, passing the selected doctor's name as a parameter, where patients can finalize their booking and upload encrypted medical reports.



Doctor Name	Phone No	Email ID	Address	Description	Government No	Rating	Book Appointment
john	7898098765	john@gmail.com	hyd	MBBS General Medicine Practioner with 10 year experience	5678	4.0	Click Here to Book Appointment
alice	9998887776	aaa@gmail.com	hyd	heart surgeon DDGA, MBBS	9876	5.0	Click Here to Book Appointment
dave	5556667778	dave@gamil.com	hyd	US Returned MBBS General doctor with 20 years experience	5412	5	Click Here to Book Appointment

Figure 9: Web page showing the list of doctors along with appointment booking.

Patient Name	Doctor Name	Disease Details	IPFS Report Hashcode	Report Name	Prescription	Date
suresh	dave	25 year old mail having headace	Qma2Hmc23FxNsDRUVqM3zXSH21crdoBiYZDTgk3VJgeaHg	Project.docx	None	2024-02-11 21:05:30.927584

Figure 10 : Patient booking appointment history of proposed blockchain-based EHR management system.

presents the Booking History screen for a logged-in patient, accessible by selecting the "View Prescriptions" link on the dashboard. The page displays a comprehensive table in which each row corresponds to an electronic health record (EHR) from the prescriptionList where the patientUsername matches the logged-in user. The table includes the following columns: Patient Name (reflecting the global username), Doctor Name (associated with the appointment), Disease Details (as entered by the patient), IPFS Report Hashcode (first 10 characters of the encrypted report's IPFS hash, preceding the "@" symbol), Report Name (original file name of the uploaded report), Prescription (shows the doctor's issued instructions or "None" if not yet available)

5. CONCLUSION

This project has demonstrated a robust, decentralized approach to electronic health record (EHR) management by integrating blockchain and IPFS technologies within a Django-based web application. By moving all metadata—user profiles, appointments, prescriptions, and ratings—onto a permissioned smart contract, the system achieves immutable audit trails, tamper resistance, and transparent verification. Simultaneously, sensitive medical reports and prescription files are encrypted with AES-CTR and pinned to IPFS, ensuring that file contents remain confidential while benefiting from distributed storage resilience. In practice, patients can book appointments by uploading

encrypted reports, and doctors can securely download those reports, generate encrypted prescriptions, and store references on-chain. Real-time average rating calculations and immediate synchronization of in-memory caches ensure that the user experience remains responsive without incurring repeated blockchain queries. Performance testing confirmed that encrypting, pinning, fetching, and decrypting multi-megabyte files meets acceptable latency constraints (under two minutes for a 10 MB file), and that on-chain transactions can be processed promptly in a local Ethereum environment. Compared to traditional centralized systems, this architecture removes the single point of failure inherent in a standalone database, drastically reduces the risk of undetected data tampering, and provides a trustless environment where stakeholders—patients, doctors, and auditors—can independently verify all actions.

REFERENCES

1. Yusof, M.M.; Papazafeiropoulou, A.; Paul, R.J.; Stergioulas, L.K. Investigating Evaluation Frameworks for Health Information Systems. *Int. J. Med. Inform.* **2008**, *77*, 377–385.
2. Vora, J.; Italiya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Hsiao, K.F. Ensuring Privacy and Security in E-Health Records. In Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS), Colmar, France, 11–13 July 2018.
3. Mbonihankuye, S.; Nkunzimana, A.; Ndagijimana, A. Healthcare Data Security Technology: HIPAA Compliance. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1927495.
4. Qayyum, A.; Qadir, J.; Bilal, M.; Al-Fuqaha, A. Secure and Robust Machine Learning for Healthcare: A Survey. *IEEE Rev. Biomed. Eng.* **2020**, *14*, 156–180.
5. Agbo, C.C.; QMahmoud, H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56.
6. Mohamad Jawad, H.H.; Bin Hassan, Z.; Zaidan, B.B.; Mohammed Jawad, F.H.; Mohamed Jawad, D.H.; Alredany, W.H.D. A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations. *Electronics* **2022**, *11*, 3223.
7. Katarahweire, M.; Bainomugisha, E.; Mughal, K.A.; Ngubiri, J. Form-based security in mobile health data collection systems. *Secur. Priv.* **2021**, *4*, e155.
8. Ullah, I.; Amin, N.U.; Khan, M.A.; Khattak, H.; Kumari, S. An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System. *J. Med. Syst.* **2020**, *45*, 4.
9. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183.
10. Harman, L.B.; Flite, C.A.; Bond, K. Electronic Health Records: Privacy, Confidentiality, and Security. *Am. Med. Assoc. J. Ethics* **2012**, *14*, 712–719.
11. Basil, N.N.; Solomon, A.; Chukwuyem, E.; Ekokobe, F. Health Records Database and Inherent Security Concerns: A Review of the Literature. *Cureus* **2022**, *14*, e30168.
12. Fathima Shah, W. Preserving Privacy and Security: A Comparative Study of Health Data Regulations—GDPR vs. HIPAA. *Int. J. Res. Appl. Sci. Eng. Technol.* **2023**, *11*.
13. Amato, F.; Casola, V.; Cozzolino, G.; De Benedictis, A.; Mazzocca, N.; Moscato, F. A Security and Privacy Validation Methodology for e-Health Systems. *ACM Trans. Multimed. Comput. Commun. Appl.* **2021**, *17*.
14. Joppi, R.; Bertele, V.; Vannini, T.; Garattini, S.; Banzi, R. Food and Drug Administration vs European Medicines Agency: Review times and clinical evidence on novel drugs at the time of approval. *Br. J. Clin. Pharmacol.* **2020**, *86*, 170–174.