10.48047/jocaaa.2025.34.05.35

A Secure Hybrid Architecture for Electronic Health Records Using Blockchain and Decentralized Storage

Ravi Kota[1*], G. Ashish Reddy[2], J. Bharath Goud[2], P. Surya[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering-Cyber Security,
[1,2]Malla Reddy Engineering College and Management Sciences, Kistapur, Medchal, 501401, Telangana, India
*Corresponding author: ravikota@mrem.ac.in

Received: 02.03.2025 Revised: 15.04.2025 Accepted: 25.05.2025

ABSTRACT

Centralized storage of electronic health records (EHRs) exposes healthcare systems to vulnerabilities such as data breaches, tampering, and single-point failures. This research proposes a decentralized EHR management framework that integrates blockchain with the InterPlanetary File System (IPFS) to securely handle appointments, medical reports, prescriptions, and patient feedback. A permissioned Ethereum-based smart contract ("Healthcare") maintains immutable on-chain records for user information, appointment details, ratings, and prescription references, while sensitive documents are encrypted using AES-CTR with a PBKDF2-derived key and stored as encrypted binaries in IPFS to preserve confidentiality. Patients can register, authenticate, upload encrypted reports, schedule appointments, and later retrieve decrypted prescriptions, whereas doctors access uploaded records, issue encrypted prescriptions, and update corresponding blockchain entries. Patient feedback is also recorded as on-chain transactions. An in-memory cache supports efficient data retrieval without frequent blockchain queries. Experimental results demonstrate reliable encryption, IPFS storage, and decryption performance. The system strengthens transparency, integrity, and resilience by preventing undetected record modification and ensuring encrypted file availability across nodes, offering a secure and patient-centric approach to EHR management.

Key words: Electronic Health Records (EHR), Patient Privacy, Healthcare Data Security, Cryptography, Tamper-Proof Records

1. INTRODUCTION

Digital healthcare and the use of the Internet of Medical Things (IoMT) are revolutionizing healthcare services by improving both efficiency and accessibility [1, 2]. The most important development is the use of Electronic Medical Records (EMRs) in healthcare, which store a patient's important data, including medical history; treatment plan; and diagnostic images, such as X-rays, MRIs, CT scans, and other DICOM [3]. Recent research reports show that medical images now account for almost 80% of the data produced in EMR systems, posing significant problems for data storage, security, and sharing [4].

10.48047/jocaaa.2025.34.05.35

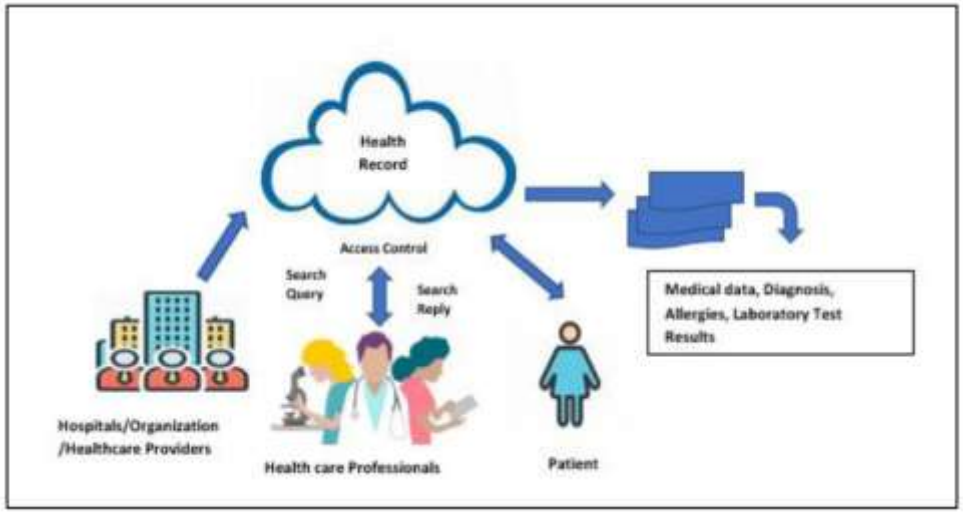


Fig 1. IPFS based Storage of Health Records

The healthcare sector has become highly vulnerable to data breaches, with financial losses up to USD 15 million [5]. In fact, data breaches in healthcare have increased by 19% more compared to in other sectors [6]. Notable incidents such as the WannaCry ransomware attack in 2017, which globally disrupted healthcare institutions, including the UK's National Health Service (NHS), and the Anthem data breach in 2015, which exposed the sensitive information of millions of patients, highlight the weaknesses of current centralized systems [7, 8].

Similarly, a 2020 ransomware attack on U.S. healthcare institutions significantly interrupted healthcare services by delaying medical procedures and negatively impacting patient care nationwide [9]. These cases show that there is an urgent need for secure, reliable, and decentralized alternatives to existing centralized healthcare data management systems. Traditional doctor–patient appointment systems rely on centralized servers and relational databases to store all user credentials, appointment details, medical reports, and prescriptions. Such centralized architectures suffer several shortcomings These limitations highlight the need for a solution that can (a) decentralize metadata storage to avoid a single point of trust, (b) give patients and doctors an unforgeable audit trail of every action, and (c) ensure that sensitive files (medical reports and prescriptions) are stored securely off-chain in encrypted form.

2. LITERATURE SURVEY

Recent developments in decentralized healthcare systems have incorporated blockchain, the IPFS, and edge computing to address fundamental challenges related to security, scalability, and latency. This section reviews recent studies, highlighting their relevance to our proposed framework.

Blockchain's immutability and transparency have been widely leveraged for secure healthcare data management. Anwar et al. proposed AnonChain, a secure file-sharing system that uses blockchain combined with the IPFS. This approach enhances data security, allowing for user anonymity while ensuring data integrity through encryption and hashing techniques. However, this system may struggle with scalability issues, especially when storing large medical images directly on the blockchain due to the high transaction costs [17]. Similarly, MacBee and Wilcox introduced a blockchain-based system specifically for medical imaging data management. Their work integrates blockchain with existing medical imaging workflows to improve traceability, integrity, and secure sharing among healthcare

10.48047/jocaaa.2025.34.05.35

providers. While this approach directly addresses medical imaging use cases, it does not sufficiently resolve scalability challenges when handling large-scale, high-resolution medical image datasets [18].

Jabarulla and Lee's blockchain-based, patient-centric image management system also uses the IPFS to decentralize access control for medical images. By leveraging Ethereum and smart contracts, the system allows patients to manage permissions effectively. Despite its privacy advantages, their framework faces challenges in terms of latency and the need for more efficient data retrieval mechanisms [16]. However, He et al. proposed a blockchain-based method for secure data offloading in healthcare using mobile edge computing. They utilized deep reinforcement learning to optimize resources and minimize offloading costs. While their approach addresses cost and resource challenges, it overlooks the issue of integrating blockchain and edge computing seamlessly for efficient real-time medical image access [19]. Furthermore, their system may not handle large-scale data efficiently when medical images grow in size.

Finally, Nguyen et al. introduced Federated Healthcare, which uses blockchain and edge computing for decentralized EMR sharing. While the system successfully integrates the IPFS and smart contracts to ensure secure and efficient data sharing among hospitals, the overall performance may degrade when handling high-frequency real-time data access, especially under heavy-load conditions [20].

To address blockchain's storage limitations, the IPFS has emerged as a decentralized alternative for scalable medical image management. For instance, Li et al. explored the IPFS for the low-cost, reliable storage of IoT data, including medical images. They combined blockchain with the IPFS to ensure data integrity and reduce storage costs. However, the IPFS-based solution may not provide the level of access speed required for critical real-time medical applications [21]. Similarly, Qiuyu and Zhao proposed a distributed storage system for encrypted speech data using blockchain and the IPFS. Their method leverages the IPFS's decentralized storage and blockchain's immutability to ensure the secure management of sensitive data. While this approach demonstrates the versatility of the IPFS for healthcare-adjacent use cases (e.g., speech data), it does not address the unique challenges of medical image formats, such as large file sizes and metadata complexity [22].

Peng Kang's approach to private file storage and sharing with the IPFS is another example of utilizing decentralized storage for healthcare data. By combining blockchain's immutability with the IPFS's decentralized storage, Kang's system ensures privacy and reliability. However, like other IPFS-based solutions, its scalability and performance could become limiting factors as the number of stored medical images increases significantly [23]. Furthermore, N. Sangeeta also used the IPFS and blockchain to manage data in vehicular networks, showing how this can enhance decentralized data retrieval. While this system improves data security and retrieval efficiency, it does not address the potential delays in retrieving large images or real-time access challenges [24].

Finally, Ben Letaifa, Rachedi, and Makina proposed a system that integrates the IPFS, blockchain, and edge computing for eHealth. While it ensures real-time data processing and confidentiality, their solution faces challenges in scaling up for large healthcare datasets. The IPFS's performance may degrade as the system scales, impacting its ability to handle time-sensitive medical data efficiently [25]. Edge computing helps address the latency challenges inherent in centralized healthcare systems. Gao et al. explored a fine-grained searchable encryption system for EHRs, combining blockchain and edge computing to enhance data privacy and integrity. Their system reduces the computational burden on users and ensures secure access to medical images. However, this system still faces the challenge of effectively managing high throughput in real-time scenarios, particularly when large datasets are involved [26]. Similarly, Dongjun Na et al. proposed a federated blockchain architecture to minimize latency and improve reliability for IoT DApp services. By using IoT devices as blockchain nodes, their

10.48047/jocaaa.2025.34.05.35

system optimizes upload and download times for decentralized applications. While this approach addresses latency challenges in IoT environments, its applicability to medical image sharing requires further validation, particularly in scenarios demanding ultra-low latency for urgent healthcare workflows [27].

Mahadev and Patil designed a blockchain-based framework for secure data sharing in edge computing, leveraging fog nodes to enhance privacy and reduce computational overhead. Their work demonstrates efficient decentralized management of sensitive data, but its adaptation to healthcare systems would require addressing regulatory compliance and interoperability with existing medical devices [28]. Expanding on medical imaging, Liu et al. developed a secure medical image transmission and storage system that uses blockchain and the IPFS for off-chain storage. Edge computing is incorporated to enhance real-time access and reduce latency. Although the system shows promise in localizing data access, it may not scale well in a network with multiple hospitals requiring simultaneous access to large volumes of medical images [29].

Bingcheng and He proposed a blockchain-based secure video-sharing system for vehicular edge computing, emphasizing decentralized access control via smart contracts. While they focused on real-time data sharing, the system's design for vehicular networks may not fully account for the stringent privacy requirements of healthcare data [30]. Similarly, Gao's collaborative edge computing framework aims to improve resource sharing and efficiency in decentralized systems. While it enhances trust and reduces latency by bringing computation closer to the users, it still needs to be optimized for high-demand scenarios such as real-time medical image sharing between hospitals [31].

Cryptographic techniques are crucial in ensuring the confidentiality and integrity of medical images. Wenying and Jian proposed a blockchain-based medical image-sharing framework that integrates QR codes for data integrity and security. While their solution is effective in protecting image data, it may face difficulties in scalability when dealing with larger datasets or more complex medical imaging systems [32]. Similarly, Muhammad and Migliorini suggested a secure approach for storing and retrieving data in a decentralized manner using blockchain and the IPFS. Their system leverages cryptographic mechanisms, including the AES, to protect data during storage and transmission. However, their approach still faces challenges in efficiently managing data retrieval times, especially when dealing with large medical images [33].

Finally, Li et al. proposed a similar system using blockchain and the IPFS for the secure, reliable storage of IoT data. They employed the AES and RSA encryption to enhance security. While their encryption methods are robust, their solution does not adequately address the scalability challenges when scaling up to handle high volumes of medical image data [21].

Patient-centric access control is a key aspect of maintaining privacy and trust in healthcare data management. Jabarulla and Lee's system allows patients to manage permissions for their medical images through smart contracts on a blockchain. Although this approach ensures privacy, it may suffer from performance issues as the number of patients and healthcare providers grows, impacting real-time access to medical images [16]. Muhammad and Migliorini's framework also offers patient-controlled access to medical data using blockchain and the IPFS. Their system enables patients to manage access permissions, ensuring data confidentiality. However, the system may face challenges in ensuring real-time access during emergencies, especially in high-demand healthcare environments [33].

Similarly, Nguyen et al.'s Federated Healthcare system uses blockchain and smart contracts to enable the decentralized sharing of medical records. Although their system allows patients to control access to

10.48047/jocaaa.2025.34.05.35

their EMRs, it may struggle with scaling to handle a large number of healthcare providers and patients, especially in large hospital networks [20].

3. PROPOSED SYSTEM

This research module implements a compact doctor–patient appointment system that integrates AES-CTR encryption for securing uploaded medical files, IPFS for decentralized storage of those encrypted files, and an Ethereum-style smart contract (via Web3) to manage all user, appointment, rating, and prescription metadata on-chain. When a patient uploads a medical report or a doctor issues a prescription, the file is first encrypted locally, uploaded to IPFS, and only its IPFS hash is stored on the blockchain, while all user credentials and interaction data are also maintained on-chain and accessed through Django view functions. At startup, the system initializes by connecting to a local IPFS node and a blockchain node (such as Ganache), loading the contract ABI, and designating a default transaction account, after which it fetches and caches users, ratings, and electronic health records in in-memory Python lists to avoid repeated blockchain reads. These cached records include user details, doctor–patient ratings, appointment and prescription metadata, IPFS file references, and timestamps, and are updated in tandem with the blockchain whenever new entries are added so that subsequent lookups always reflect the current application state.

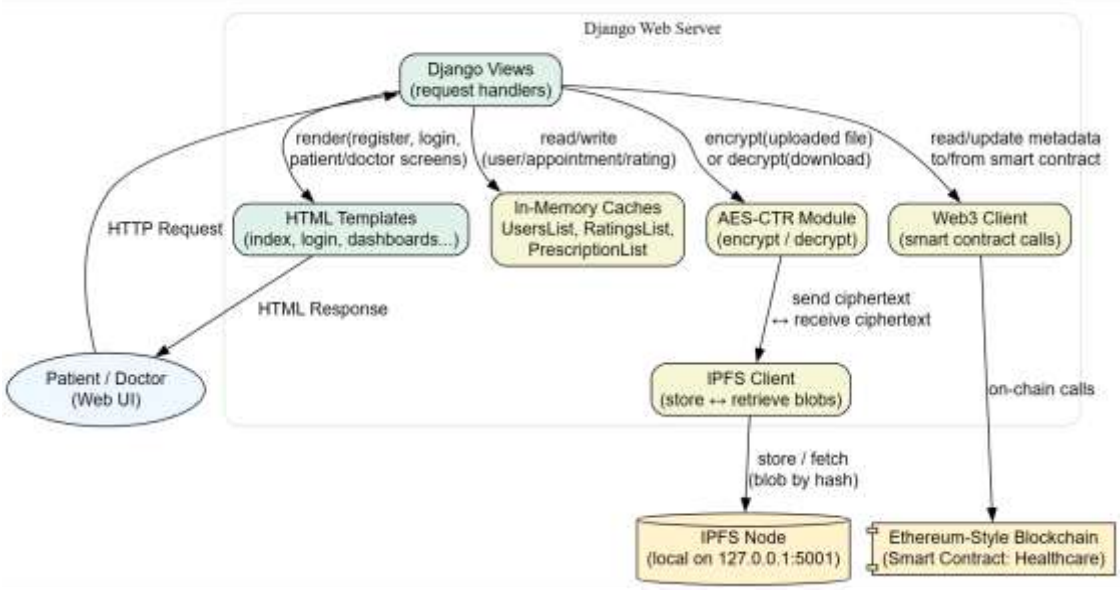


Fig. 2. Proposed block diagram of blockchain-based medical data integrity and access control.

This module, a fixed password and salt are processed through PBKDF2 to derive a 256-bit AES key that is reused for all files, allowing the server to encrypt and decrypt data under a single secret. Using this key along with a fixed counter, the system applies AES-CTR mode to convert any uploaded medical report or prescription into ciphertext before storing it in IPFS, and later uses the same key and counter to deterministically decrypt the file when it is retrieved. As a result, IPFS only ever stores encrypted binaries, and the confidentiality of patient files depends entirely on keeping the server-side encryption key secure. All application metadata—users, ratings, appointments, and electronic health records is stored inside a single “Healthcare” smart contract on the blockchain, while only the encrypted file binaries reside in IPFS. User registrations record full profile details and roles on-chain, ratings store reviews, scores, and timestamps for each doctor, and every appointment creates an EHR entry containing patient and doctor details, disease description, IPFS references to encrypted reports, and later an updated prescription field when the doctor issues one. By keeping all metadata on-chain and only

10.48047/jocaaa.2025.34.05.35

files off-chain, the system ensures tamper-proof transparency while preserving encrypted file privacy. During registration, a new user submits their profile details and selected role, after which the system checks for duplicate usernames and, if unique, writes the new record to the blockchain and updates its in-memory cache before confirming successful signup. For login, separate patient and doctor forms validate credentials against the cached user list and, when correct, store the active username in a shared variable and redirect the user to the appropriate dashboard, while invalid attempts simply reload the login page with an error message.

4. RESULTS DESCRIPTION

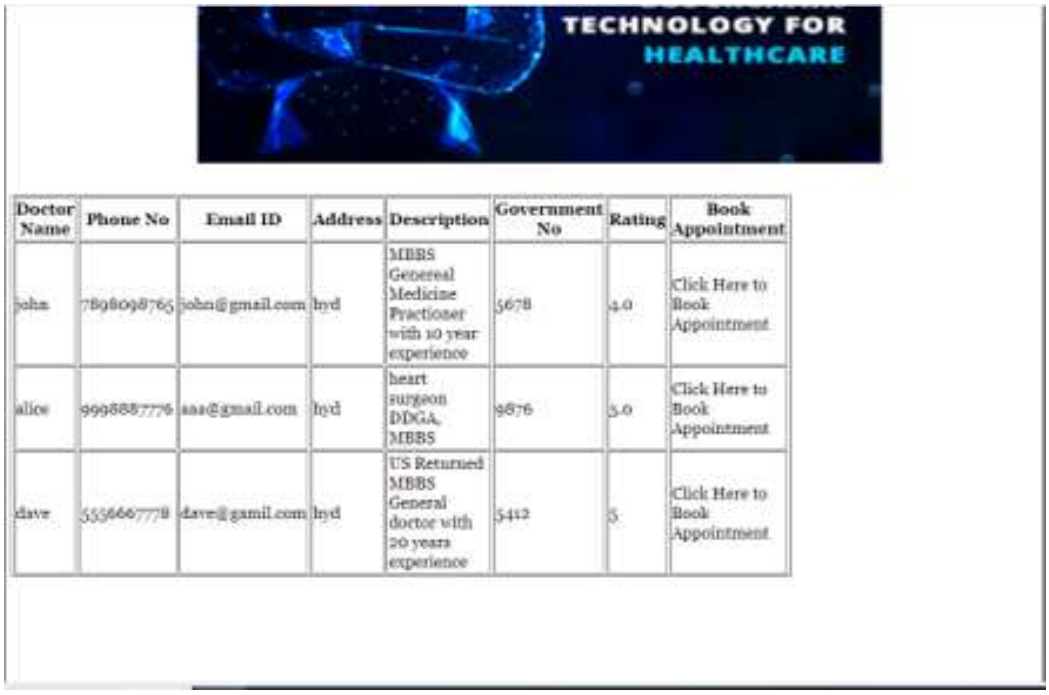
The home page of the Healthcare platform in Fig. serves as the first point of entry. At the very top, a horizontal navigation bar presents three clickable links:

When a patient clicks “View Doctors List,” the system renders a table with the following columns (each column header in bold) as shown in Fig. 3:

- **Doctor Name:** The doctor’s username (e.g., “John,” “Alice,” “Dave”).
- **Phone No:** The doctor’s contact telephone number.
- **Email ID:** The doctor’s email address.
- **Address:** The doctor’s location (e.g., “hyd” for Hyderabad).
- **Description:** A short biography (e.g., “MBBS General Medicine Practitioner with 10 years experience”).
- **Government No:** The doctor’s license or registration number.
- **Rating:** The computed average rating (e.g., “4.0” or “5.0”), calculated by summing all numeric scores in ratingsList where doctorName matches and dividing by the count (defaulting to 5 if none exist).
- **Book Appointment:** A link or button labeled “Click Here to Book Appointment.” When clicked, it passes the chosen doctor’s username as a query parameter to the Appointment view.

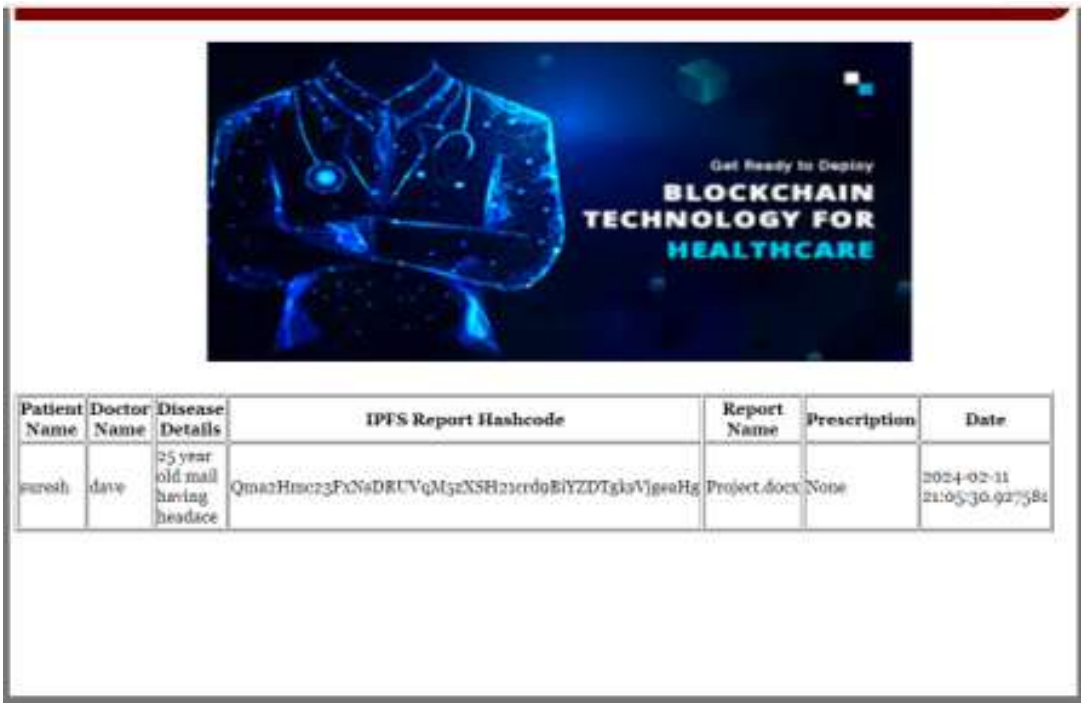
Clients can sort or filter (if implemented) by rating or specialization. Once a patient selects “Click Here to Book Appointment,” they proceed to a form where they confirm the doctor and upload their report.

10.48047/jocaaa.2025.34.05.35



Doctor Name	Phone No	Email ID	Address	Description	Government No	Rating	Book Appointment
john	7898098765	john@gmail.com	hyd	MBBS Genereal 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

Fig. 3. 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	QmazHmc23PxNsDRUVqM5zXSH21crd9BiYZDTgksVjgeaHg	Project.docx	None	2024-02-11 21:05:30.927582

Fig. 4. Patient booking appointment history of proposed blockchain-based EHR management system.

Fig. 4 shows the screen that is the logged-in patient's **Booking History** page (accessed by choosing "View Prescriptions" or a similarly labeled link). It displays a table whose rows correspond to every EHR (electronic health record) in prescriptionList where patientUsername matches the logged-in user. For each record, the columns include:

- **Patient Name:** The patient's username (same as global username).
- **Doctor Name:** The doctor assigned at booking time.

10.48047/jocaaa.2025.34.05.35

- **Disease Details:** The text the patient entered describing their symptoms or condition.
- **IPFS Report Hashcode:** The first 10 characters of the IPFS content hash for the encrypted medical report (i.e., before the "@" separator).
- **Report Name:** The original filename of the medical report.
- **Prescription:** If the doctor has already issued a prescription, this column shows the textual prescription; otherwise, it displays "None."
- **Prescription File Name:** The name of the prescription file (if uploaded) or a hyphen ("–") if none exists.
- **Download Prescription:** If a prescription file exists, a "Click Here" link appears. That link points to ViewReport?pid=<fileHash>&file=<filename>, which fetches the encrypted prescription from IPFS, decrypts it, and forces a browser download. If no prescription has been issued yet, this column shows "Pending."
- **Date:** The timestamp string when the appointment was originally booked.

Below the table, the patient can still provide feedback (if not already provided) or simply log out. This comprehensive booking history view ties together on-chain EHR metadata and off-chain encrypted file retrieval.

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] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, and A. A. Alabdulatif, "A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data," *Comput. Biol. Med.*, vol. 167, p. 107630, 2023.

[2] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Comput. Biol. Med.*, vol. 150, p. 106019, 2022.

10.48047/jocaaa.2025.34.05.35

[3] B. W. Genereaux, D. K. Dennison, K. Ho, R. Horn, E. L. Silver, K. O'Donnell, and C. E. Kahn, "DICOMweb™: Background and application of the web standard for medical imaging," *J. Digit. Imaging*, vol. 31, pp. 321–326, 2018.

[4] "Deep Learning Market: Focus on Medical Image Processing, 2020–2030," Yahoo Finance, 2024. [Online]. Available: https://finance.yahoo.com/news/deep-learning-market-focus-medical-090600695.html. [Accessed: 15-May-2025].

[5] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. A. Khan, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, p. 133, 2020.

[6] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[7] Wikipedia contributors, "WannaCry Ransomware Attack," Wikipedia, 2017. [Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack. [Accessed: 15-May-2025].

[8] Wikipedia contributors, "Anthem Medical Data Breach," Wikipedia, 2015. [Online]. Available: https://en.wikipedia.org/wiki/Anthem_medical_data_breach. [Accessed: 20-May-2025].

[9] "UHS Ransomware Attack Cost $67M in Lost Revenue, Recovery Efforts," TechTarget HealthTech Security, 2020. [Online]. Available: https://www.techtarget.com/healthtechsecurity/news/366595382/UHS-Ransomware-Attack-Cost-67M-in-Lost-Revenue-Recovery-Efforts. [Accessed: 20-May-2025].

[10] S. Uppal, B. Kansekar, S. Mini, and D. Tosh, "HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system," *Healthc. Anal.*, vol. 3, p. 100175, 2023.

[11] B. A. A. Al-Ahmadi, "Blockchain based remote patient monitoring system," *J. King Abdulaziz Univ. Comput. Inf. Technol. Sci.*, vol. 8, pp. 111–118, 2019.

[12] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[13] L. Ante, C. Fischer, and E. Strehle, "A bibliometric review of research on digital identity: Research streams, influential works and future research paths," *J. Manuf. Syst.*, vol. 62, pp. 523–538, 2022.

[14] "Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda," *Inf. Manag.*, vol. 61, p. 104026, 2024.

[15] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, pp. 4298–4311, 2020.

[16] M. Y. Jabarulla and H. N. Lee, "Blockchain-based distributed patient-centric image management system," *Appl. Sci.*, vol. 11, p. 196, 2020.

[17] S. Anwar, R. Tulsyan, S. Saha, and S. K. Sahana, "AnonChain: A secure file sharing framework using IPFS integrated blockchain," *Int. J. Math. Eng. Manag. Sci.*, vol. 7, pp. 844–858, 2022.

[18] M. P. McBee and C. Wilcox, "Blockchain technology: Principles and applications in medical imaging," *J. Digit. Imaging*, vol. 33, pp. 726–734, 2020.

10.48047/jocaaa.2025.34.05.35

[19] Q. He, Z. Feng, H. Fang, X. Wang, L. Zhao, Y. Yao, and K. Yu, "A blockchain-based scheme for secure data offloading in healthcare with deep reinforcement learning," *IEEE/ACM Trans. Netw.*, vol. 32, pp. 65–80, 2024.

[20] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain and edge computing for decentralized EMRs sharing in federated healthcare," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Cape Town, South Africa, 8–12 Dec. 2024.

[21] L. Li, D. Jin, T. Zhang, and N. Li, "A secure, reliable and low-cost distributed storage scheme based on blockchain and IPFS for firefighting IoT data," *IEEE Access*, vol. 11, pp. 97318–97330, 2023.

[22] Q. Zhang and Z. Zhao, "Distributed storage scheme for encryption speech data based on blockchain and IPFS," *J. Supercomput.*, vol. 79, pp. 897–923, 2023.

[23] P. Kang, W. Yang, and J. Zheng, "Blockchain private file storage-sharing method based on IPFS," *Sensors*, vol. 22, p. 5100, 2022.

[24] N. Sangeeta and S. Y. Nam, "Blockchain and Interplanetary File System (IPFS)-based data storage system for vehicular networks with keyword search capability," *Electronics*, vol. 12, p. 1545, 2023.

[25] H. Makina, A. B. Letaifa, and A. Rachedi, "Leveraging edge computing, blockchain and IPFS for addressing eHealth records challenges," in *Proc. IEEE Int. Conf. Security Inf. Netw. (SIN)*, Sousse, Tunisia, 11–13 Nov. 2022.

[26] H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-enabled fine-grained searchable encryption with cloud-edge computing for electronic health records sharing," *IEEE Internet Things J.*, vol. 10, pp. 18414–18425, 2023.

[27] D. Na, J. Kim, J. Jeon, and S. Park, "A federated blockchain architecture for file storage with improved latency and reliability in IoT DApp services," *Sensors*, vol. 23, p. 8569, 2023.

[28] M. Gawas, H. Patil, and S. S. Govekar, "An integrative approach for secure data sharing in vehicular edge computing using blockchain," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 2840–2857, 2021.

[29] Y. Li, Y. Tu, J. Lu, and Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the Internet of Things," *Sensors*, vol. 20, p. 916, 2020.

[30] B. Jiang, Q. He, P. Liu, S. Maharjan, and Y. Zhang, "Blockchain empowered secure video sharing with access control for vehicular edge computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, pp. 9041–9054, 2023.

[31] Q. Gao, J. Xiao, Y. Cao, S. Deng, C. Ouyang, and Z. Feng, "Blockchain-based collaborative edge computing: Efficiency, incentive and trust," *J. Cloud Comput.*, vol. 12, p. 72, 2023.

[32] W. Wen, Y. Jian, Y. Fang, Y. Zhang, and B. Qiu, "Authenticable medical image-sharing scheme based on embedded small shadow QR code and blockchain framework," *Multimed. Syst.*, vol. 29, pp. 831–845, 2023.

[33] M. Bin Saif, S. Migliorini, and F. Spoto, "Efficient and secure distributed data storage and retrieval using Interplanetary File System and blockchain," *Future Internet*, vol. 16, p. 98, 2024.

[34] "Blockchain Facts: What Is It, How It Works, and How It Can Be Used," Investopedia. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed: 01-June-2025].