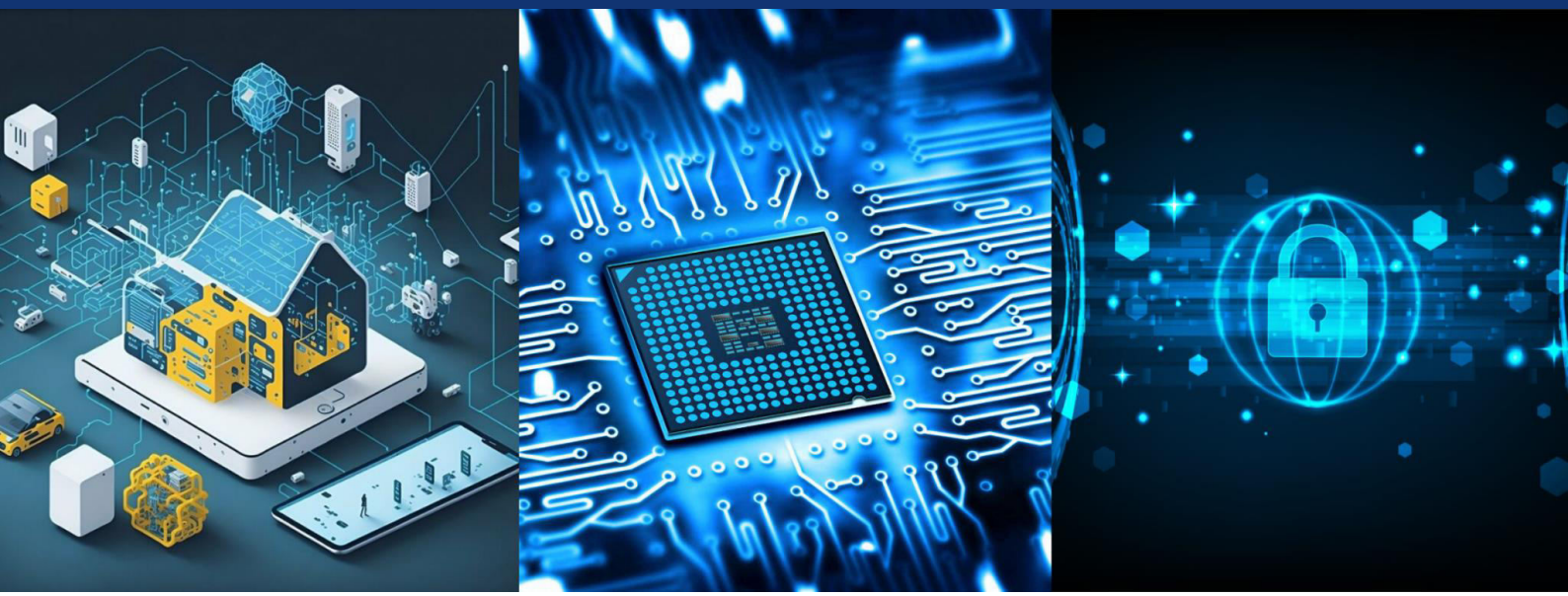
IJIRCCE

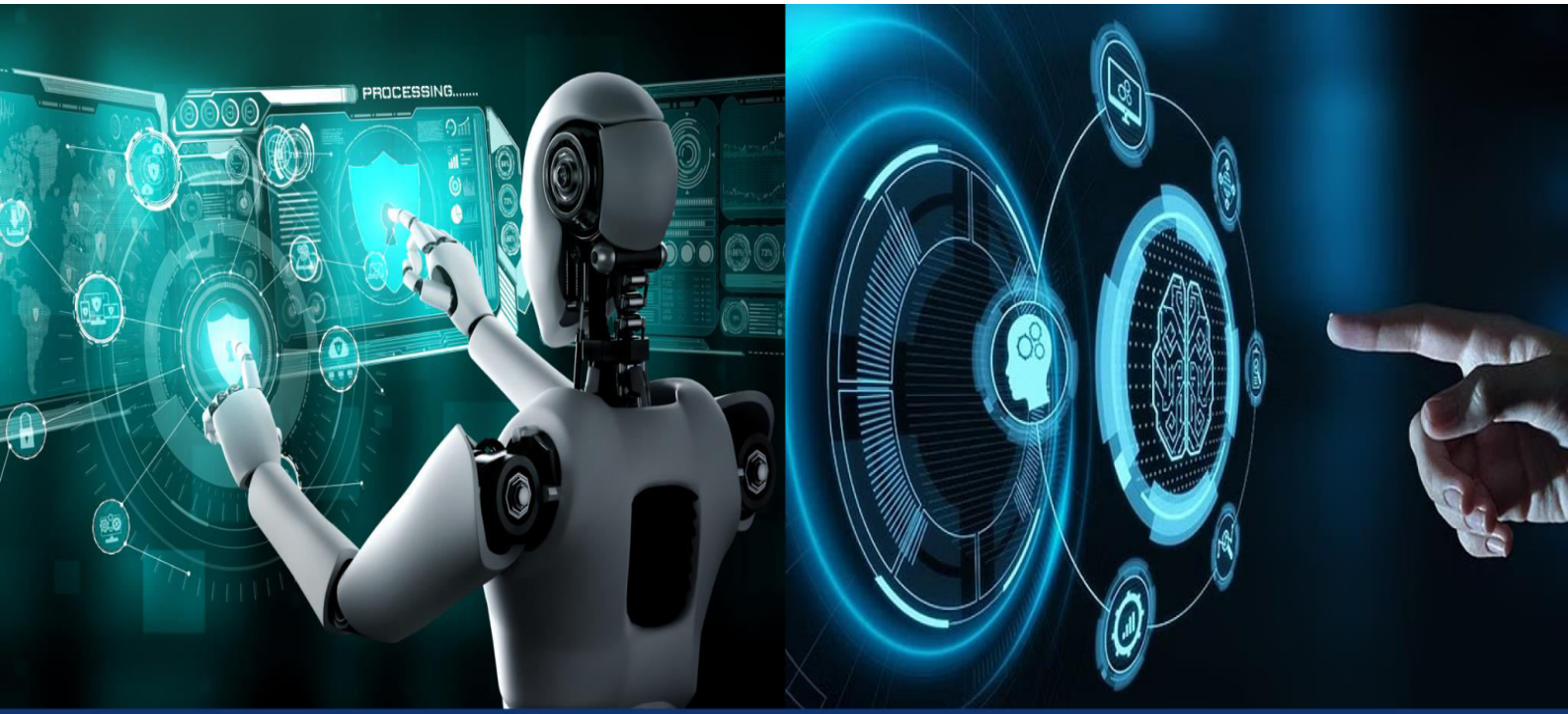
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404111

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure Organ Donation and Healthcare Data Sharing Through Blockchain Interoperability

Devulapelli Ganesh[1], Duddala Reva Sree[2], K. Sunitha[3], Dr. V. Subba Ramaiah[4], Dr. K. Rajitha[5]

Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, India[1, 2]

Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, India[3,4,5]

ABSTRACT: Organ donation systems require secure, transparent, and efficient coordination among healthcare institutions. However, traditional healthcare infrastructures rely on centralized databases that suffer from limited interoperability, lack of transparency, and vulnerability to unauthorized data manipulation. This paper proposes a blockchain-based system for secure organ donation management and healthcare data sharing. The proposed framework utilizes Ethereum smart contracts to automate processes such as donor registration, patient organ requests, and organ allocation while maintaining a transparent and immutable transaction record. Sensitive electronic health records (EHR) are encrypted using AES-256 encryption and stored in off-chain storage, while cryptographic hashes generated using SHA-256 are anchored on the blockchain to ensure data integrity. A compatibility-based donor-patient matching mechanism is implemented to identify suitable donors based on medical parameters such as blood type compatibility, donor age, and urgency level. Furthermore, Zero-Knowledge Proof (ZKP) techniques enable privacy-preserving verification of patient eligibility without revealing sensitive medical information. The proposed architecture improves transparency, security, and interoperability in healthcare systems while supporting trustworthy organ donation and transplantation workflows across multiple hospitals.

KEYWORDS: Blockchain; Organ Donation; Healthcare Interoperability; Electronic Health Records; Zero Knowledge Proof; Data Security.

I. INTRODUCTION

Organ failure is a major global health concern, and organ transplantation remains one of the most effective treatments for patients with end-stage organ diseases. However, the demand for organ transplants significantly exceeds the availability of donors, leaving many patients on waiting lists and resulting in numerous preventable deaths each year. Efficient management of organ donation systems is therefore essential to ensure fairness, transparency, and timely allocation of available organs.

Traditional organ donation and healthcare record management systems rely on centralized databases maintained by hospitals or national health organizations. Although these systems support basic record management, they often face challenges such as limited interoperability between hospitals, vulnerability to data tampering, lack of transparency in organ allocation processes, and concerns regarding patient data privacy.

Medical records and donor information are frequently stored in isolated databases, making secure information exchange across institutions difficult. Previous studies have also highlighted interoperability and security limitations in centralized healthcare infrastructures [17], [20].

Blockchain technology has emerged as a promising solution to address these challenges by providing a decentralized and immutable ledger where transactions are cryptographically verified and permanently recorded. This enables secure data sharing between healthcare institutions while preventing unauthorized modification of records. In addition to transparency and integrity, protecting patient privacy is critical in healthcare applications.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Techniques such as Zero-Knowledge Proofs (ZKP) allow verification of medical eligibility without revealing sensitive patient information [19]. In this work, a blockchain-based framework is proposed for secure organ donation management and healthcare data sharing. The system integrates Ethereum smart contracts to automate donor registration, organ request submission, and organ allocation processes, while electronic health records are encrypted and stored off-chain with blockchain-based integrity verification. A compatibility-based donor–patient matching mechanism further evaluates potential donors using medical parameters such as blood type compatibility, donor age, and urgency level.

II. RELATED WORK

A. Blockchain-Based Organ Donation Systems

In [3] authors proposed a smart contract-based organ donation system to ensure secure donor–recipient matching and transparent allocation. In [9] a decentralized end-to-end transplantation system was developed to automate the donation workflow and improve traceability. In [11] blockchain was used to enhance transparency in donor matching, reducing manipulation risks. In [12] authors introduced BOMS, a privacy-aware matching system that enables secure verification without exposing sensitive data. In [14] an Ethereum-based framework (Organ Harbour) was designed to improve traceability and fairness in organ allocation, while in [15] a private Ethereum system was proposed to automate donor verification and transplantation processes. Although these systems improve transparency and automation, they mainly focus on matching and record management, and lack privacy-preserving verification and interoperability across healthcare institutions.

B. Blockchain-Based Healthcare Systems

In [1] authors proposed a hybrid blockchain architecture integrated with federated learning and quantum encryption to secure distributed healthcare data. In [2] a comprehensive survey highlighted blockchain-based access control and privacy preservation mechanisms in healthcare systems. In [4] a blockchain-enabled framework was introduced for secure healthcare data management, ensuring integrity and confidentiality. In [5] a hybrid blockchain model was proposed to support secure data sharing across institutions. In [7] blockchain was used to protect electronic patient data from unauthorized access, while [8] explored innovations in privacy, security, and interoperability using distributed ledgers. In [10] authors investigated blockchain-based interoperability for secure communication between healthcare systems, and in [13] a public blockchain framework was proposed for cross-organizational health data sharing. In [16] and [17] survey studies analyzed interoperability, security challenges, and adoption barriers in blockchain-based healthcare systems. In [20] a blockchain-based EHR framework (MyBlockEHR) was proposed to improve secure data exchange. In [6] integration of blockchain with emerging technologies such as IoT and AI was explored for next-generation healthcare systems, while [19] discussed Zero-Knowledge Proofs for privacy-preserving blockchain applications. In [18] authors proposed a blockchain-based organ donation and healthcare management system to ensure transparency and automation, though scalability remains a challenge.

III. PROPOSED BLOCKCHAIN-BASED SOLUTION

The proposed system presents a blockchain-based framework for secure organ donation and healthcare data sharing across institutions. Ethereum smart contracts manage donor registration, organ requests, allocation, and verification, ensuring transparency and automation. Sensitive health records are stored off-chain with blockchain-based hash references for integrity. Additionally, Zero-Knowledge Proofs (ZKP) enable privacy-preserving medical verification, supporting secure and interoperable organ donation workflows.

A. System Architecture

The architecture of the proposed blockchain-based organ donation and healthcare data sharing system is illustrated in Fig. 1.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404111

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

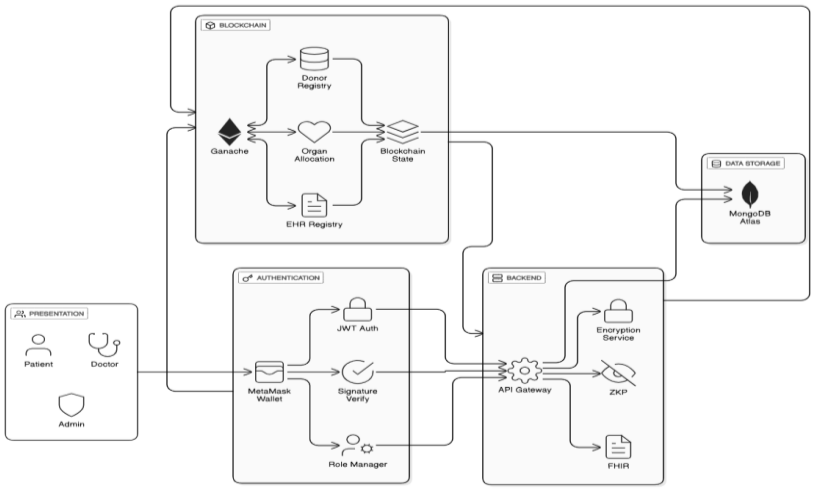


Fig.1. System Architecture of Secure Organ Donation and Healthcare Data Sharing System

The system follows a layered architecture that integrates blockchain technology, authentication mechanisms, backend services, and secure data storage to support transparent and secure healthcare operations.

The architecture consists of five main components: Presentation Layer, Authentication Layer, Backend Services Layer, Blockchain Layer, and Data Storage Layer. The Presentation Layer provides the user interface for administrators, doctors, and patients through a decentralized web application where users authenticate using MetaMask. The Authentication Layer manages secure access control using JWT-based authentication and role-based permission management. The Backend Services Layer processes application requests through an API gateway and provides services such as AES-based encryption for medical records and privacy-preserving verification using Zero-Knowledge Proof mechanisms. The Blockchain Layer, implemented on the Ethereum platform, manages smart contracts responsible for donor registration, organ allocation, and electronic health record references. Finally, the Data Storage Layer stores encrypted off-chain medical records using MongoDB, while blockchain stores hash references to ensure data integrity and tamper-proof verification.

B. Sequence Diagram

The sequence diagram shown in Fig. 2 illustrates the interaction between system entities such as Patient, Doctor, and Administrator, and components including the frontend interface, authentication layer, application layer, blockchain network, and database. It shows how user requests are processed through authentication, encrypted data handling, and blockchain transactions to support secure healthcare workflows.

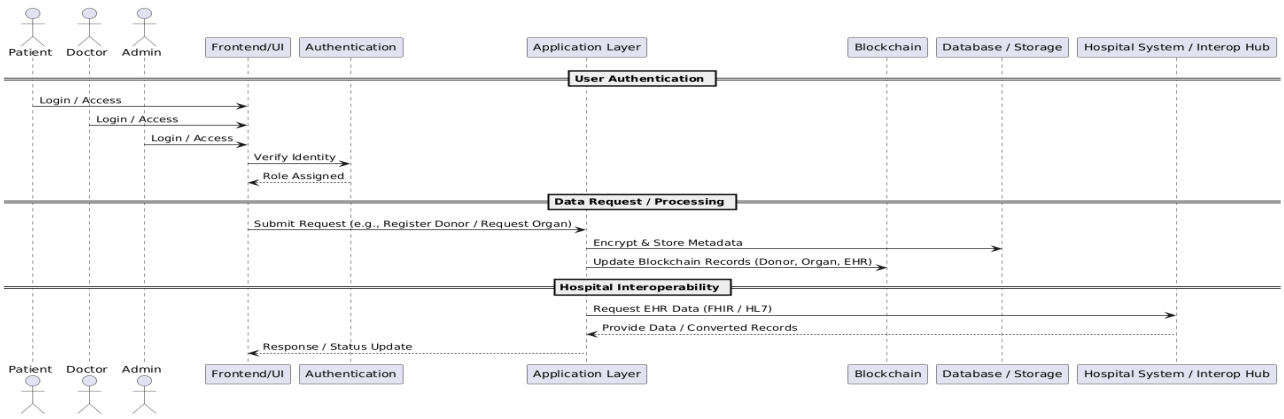


Fig.2. Sequence Diagram of Secure Organ Donation and Healthcare Data Sharing System

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404111

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Users first authenticate through the frontend using MetaMask or JWT, after which the authentication module verifies identities and assigns roles. Requests such as donor registration, organ allocation, and medical record verification are processed in the application layer. Medical data is encrypted using AES, while hash references and transactions are stored on the blockchain to ensure integrity. Encrypted records are stored off-chain, and interoperability standards such as FHIR/HL7 enable secure data exchange between healthcare institutions.

IV. IMPLEMENTATION

The system is implemented using a full-stack blockchain architecture. The frontend is developed using React.js and Tailwind CSS for a responsive user interface, with Ethers.js enabling interaction with Ethereum smart contracts. The backend is built using Node.js and Express.js to handle APIs and business logic, with MongoDB Atlas for secure off-chain data storage and JWT for authentication. The blockchain layer utilizes Solidity for smart contract development, Ganache for local deployment, and MetaMask for transaction signing. Cryptographic mechanisms such as AES-256 encryption, SHA-256 hashing, and Zero-Knowledge Proofs (ZKP) are integrated to ensure data security, integrity, and privacy.

A. Algorithms

The proposed system employs several cryptographic and verification algorithms to ensure secure healthcare data management and reliable organ donation operations. These algorithms support functions such as encryption of medical records, integrity verification of healthcare data, secure authentication of system users, donor-patient compatibility evaluation, and privacy-preserving eligibility verification. Algorithm 1 presents the AES-256-GCM encryption process used to secure electronic health records before storage. Algorithm 2 describes the Zero-Knowledge Proof generation process used to verify patient eligibility without revealing sensitive medical data. Algorithm 3 introduces the donor-patient compatibility matching algorithm used to identify suitable donors based on medical parameters such as blood type, donor age, and urgency level.

Algorithm 1: AES-256-GCM Encryption

Input: plaintext record M, 256-bit encryption key K, context label aad
1: Decode K into a 32-byte binary key buffer
2: Generate a 12-byte cryptographically random initialization vector IV
3: Initialize AES-256-GCM cipher using K and IV
4: Bind aad as additional authenticated data to the cipher context
5: **if** M is not a string **then**
6: | Convert M to a canonical serialized string representation
7: **end**
8: Encrypt M to produce ciphertext C
9: Extract 128-bit authentication tag T from cipher10: **return** { IV, authentication tag T, ciphertext C, algorithm identifier }
Decryption sub-procedure:
11: **function** DECRYPTS (payload, K)
12: | Recover IV and T from payload
13: | Initialize AES-256-GCM decipher using K, IV, and T
14: | Bind same aad context label
15: | **if** authentication tag T does not match **then** Revert - Tamper Detected
16: | **return** decrypted plaintext M
17 **end**

Algorithm 2: Zero-Knowledge Proof Generation for Patient Eligibility

Input: Private medical data W = {age, bloodType, weight, height, conditionFlags, secret}, Public parameters P = {reqBloodType, organType, requestId}
1: Check age eligibility: ageValid ← (W.age ≥ 18) ∧ (W.age ≤ 75)
2: Check weight range: weightValid ← (W.weight ≥ 40 kg) ∧ (W.weight ≤ 150 kg)
3: Check height range: heightValid ← (W.height ≥ 140 cm) ∧ (W.height ≤ 220 cm)
4: Check blood type match: bloodMatch ← (W.bloodType = P.requiredBloodType)

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404111

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

5: Check no disqualifying conditions: noCondition ← (W.conditionFlags = 0)
6: Combine physical checks: physicalValid ← weightValid ∧ heightValid
7: eligible ← ageValid ∧ bloodMatch ∧ noCondition ∧ physicalValid
8: **if** eligible = 0 **then** Revert - Patient does not meet eligibility criteria
9: **end**
10: Compute a ZK-friendly cryptographic commitment C over all private inputs in W
11: Generate proof π using the proving key, private witness W, and commitment C
12: Assemble public signals σ ← [P.organType, P.requestId, eligible, C]
13: **return** proof π, public signals σ, commitment C
Verification sub-procedure:
14: **function** VERIFY (π, σ, verification key)
15: | Validate π against σ using the verification key
16: | **if** proof is valid **then return** Eligible - no private data revealed
17: | **else** Revert - Proof verification failed
18: **end**

Algorithm 3: Donor-Patient Organ Matching

Input: organ RequestId, active donor registry, blood compatibility matrix B, required OrganType, patient UrgencyLevel, patient BloodType
1: Retrieve organ request details for RequestId
2: Fetch all active donors registered for the required organ type
3: Initialize empty ranked result list result
4: **for** each donor d in active donor pool **do**
5: | Retrieve donor age age_d and blood type BT_d from registry
6: | **if** B[BT_d][patient blood type] is not compatible **then**
7: | Skip donor and continue to next
8: | **end**
9: | Assign base compatibility score ← 100
10: | **if** donor blood type exactly matches patient blood type **then** score ← score + 20
11: | **if** age_d ≤ 30 **then** score ← score + 15
12: | **else if** age_d ≤ 45 **then** score ← score + 10
13: | **else if** age_d ≤ 60 **then** score ← score + 5
14: | **if** urgency level is CRITICAL **then** score ← score + 25
15: | **else if** urgency level is HIGH **then** score ← score + 15
16: | **else if** urgency level is MEDIUM **then** score ← score + 10
17: | Add donor with computed score to result
18: **end**
19: **return** result sorted in descending order of compatibility score

B. Smart Contracts

The proposed system utilizes Ethereum smart contracts deployed on the Ganache blockchain to automate organ donation and healthcare data operations. The **DonorRegistry** contract manages donor registration by storing details such as age, blood type, pledged organs, and medical record hashes, ensuring transparency and traceability. The **EHRRegistry** contract maintains cryptographic hash references of off-chain electronic health records to enable secure data verification while preserving privacy. The **OrganAllocation** contract performs donor–recipient matching based on factors such as blood type and urgency level, ensuring fair and immutable allocation decisions. Additionally, the **AccessControl** contract enforces role-based permissions for administrators, doctors, and patients, restricting system operations to authorized users and enhancing overall security.

C. Mathematical Model

The donor-patient compatibility is computed using a weighted scoring function based on blood match, donor age, and patient urgency.

$$\text{Score} = 100 + 20\text{M}_{\text{exact}} + \text{A}_{\text{score}} + \text{U}_{\text{score}}$$

Here, M_{exact}indicates exact blood match, while $\text{A}_{\text{score}}$and U_{score}represent age and urgency factors, respectively.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404111

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

$$A_{score} = \{15,10,5,0\}$$
$$U_{score} = \{25,15,10,0\}$$

Donors are ranked based on the computed score, and the highest score is selected for organ allocation.

V. RESULTS & DISCUSSION

This section presents the implementation results of the proposed system, highlighting key functionalities and workflows. The results demonstrate successful integration of system components, with screenshots illustrating user interactions and blockchain transactions.

A. Admin Dashboard

As shown in Fig. 3, the admin dashboard provides a comprehensive overview of system activities, including total users, verified donors, and completed allocations. It also includes analytical visualizations such as user registration trends and donor distribution by blood type, enabling efficient monitoring and management of the organ donation system.

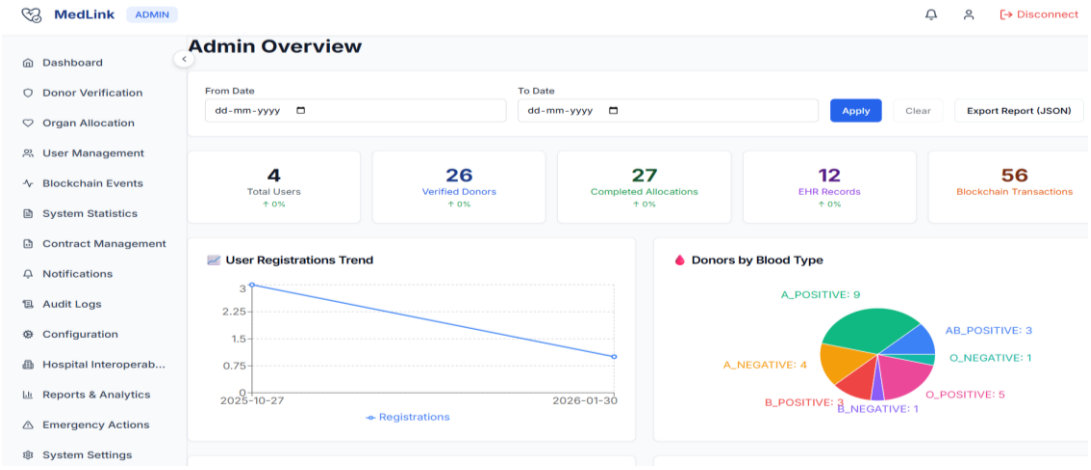


Fig.3. Admin Dashboard of Secure Organ Donation and Healthcare Data Sharing System

B. Doctor Dashboard

As shown in Fig. 4, the doctor dashboard provides functionalities for managing patient records, uploading EHR data, and verifying ZeroKnowledge Proofs. It also displays key metrics such as total patients, EHR uploads, and verified proofs, along with recent activity logs to assist doctors in monitoring and decision-making processes.

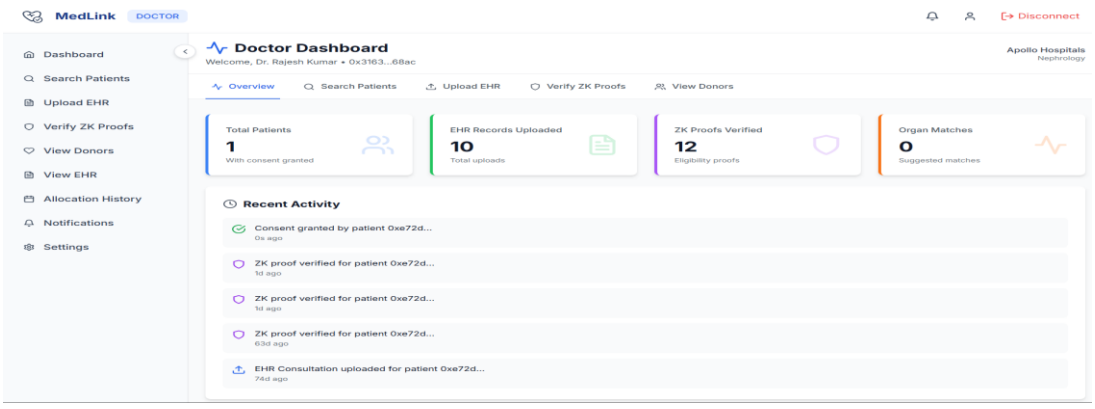


Fig.4. Doctor Dashboard of Secure Organ Donation and Healthcare Data Sharing System

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404111

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C. Patient Dashboard

As shown in Fig. 5, the patient dashboard enables users to manage organ donation pledges, submit organ requests, and view their medical records. It also displays key information such as active requests, uploaded EHR data, and recent activity, allowing patients to monitor and control their participation in the organ donation system.

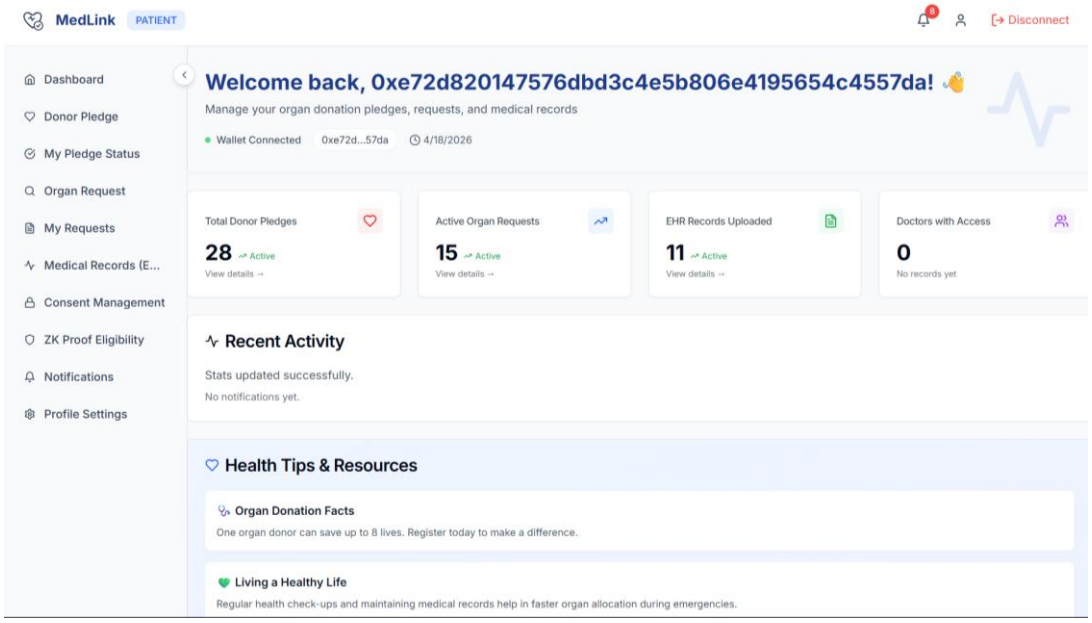


Fig.5. Patient Dashboard of Secure Organ Donation and Healthcare Data Sharing System

D. Smart Contract Deployment Gas Cost

The Fig. 6 illustrates the estimated gas consumption required to deploy the smart contracts in the proposed system. The OrganAllocation contract consumes the highest deployment gas due to its complex allocation logic and additional storage structures. In contrast, DonorRegistry and AccessControl require lower gas as they mainly handle registration and access control operations. Since deployment occurs only once, the cost does not significantly affect regular system usage.

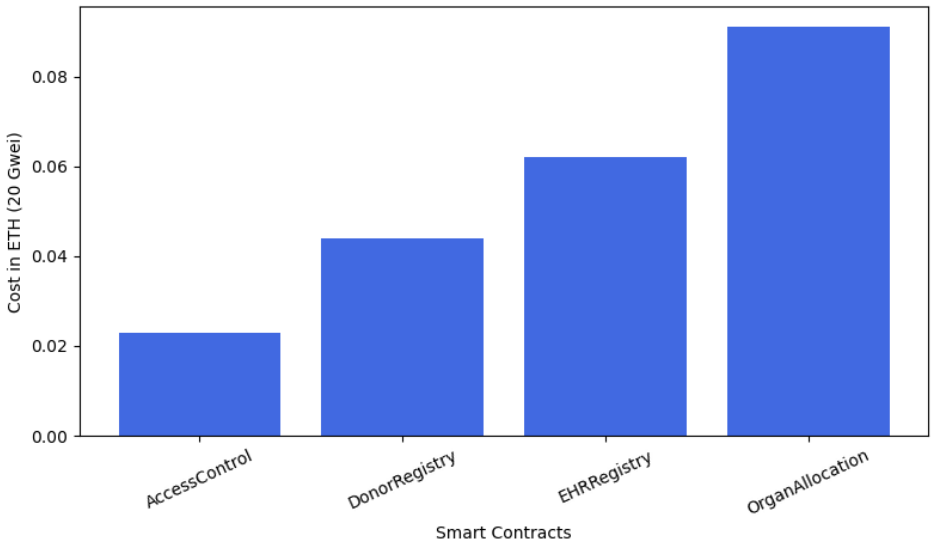


Fig.6. Smart Contract Deployment Gas Cost

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION AND FUTURE SCOPE

A. Conclusion

The proposed system presents a secure and decentralized solution for organ donation and healthcare data sharing by leveraging blockchain technology, smart contracts, and cryptographic mechanisms. It effectively addresses the limitations of traditional systems, such as lack of transparency, data tampering, and inefficient allocation processes. The implementation demonstrates the use of Ethereum-based smart contracts for automating donor registration, organ allocation, and access control, while sensitive medical data is securely stored off-chain using AES-256 encryption with SHA-256 hashing for integrity verification. This off-chain storage approach significantly enhances system scalability by reducing on-chain data load and transaction costs. The integration of Zero-Knowledge Proofs enables privacypreserving eligibility verification without exposing confidential patient data. Additionally, role-based access control using JWT and intuitive dashboards for Admin, Doctor, and Patient ensure efficient system interaction. Overall, the system achieves enhanced security, transparency, scalability, and efficiency, making it a reliable solution for modern healthcare data management and organ donation systems.

B. Future Scope

The proposed system can be further enhanced by implementing several improvements to support real-world deployment. Future work includes deploying the system on public or consortium blockchain networks to enable wider adoption and interoperability across multiple hospitals and healthcare institutions. Advanced AI or machine learning-based algorithms can be integrated to improve the accuracy and efficiency of donor-recipient matching. Additional security mechanisms such as multi-factor authentication and advanced cryptographic techniques can be incorporated to strengthen data protection. Furthermore, the system can be extended by integrating decentralized storage solutions 55 such as IPFS to efficiently manage large-scale medical data. The development of a mobile application can also be implemented to provide users with real-time access, notifications, and improved usability for patients, doctors, and administrators.

REFERENCES

1. S. Samantray and K. H. K. Reddy, “A Federated Learning Approach Towards Hybrid Blockchain, Quantum-Key-Encryption based Distributed System: A Futuristic Healthcare Architecture for Smart Cities,” Blockchain Research and Applications, 2025, DOI: https://doi.org/10.1016/j.bcra.2025.100385
2. M. Tawfik, A. Al-ahwal, A. S. T. Eldien, and H. H. Zayed, “Blockchain-based Access Control and Privacy Preservation in Healthcare: A Comprehensive Survey,” Cluster Computing, 2025, DOI: https://doi.org/10.1007/s10586-025-05308-x
3. S. D. J., S. M., T. S. V. Naik, V. S. Abhijith, and V. C. Doddamani, “Smart Blockchain-Based Organ Donation System for Secure Donor-Recipient Matching,” IJRIAS, 2025, DOI: https://doi.org/10.51584/IJRIAS.2025.100500092
4. S. K. Sharma et al., “Blockchain-Enabled Secure Data Management in Healthcare,” Blockchains, vol. 2, 2025, DOI: https://doi.org/10.3390/blockchains2020008
5. S. K. Sharma and F. Parwej, “Design and Implementation of a Blockchain-Based Secure Data Sharing Framework to Enhance the Healthcare System,” Blockchains, vol. 3, 2025, DOI: https://doi.org/10.3390/blockchains3030010
6. O. Cheikhrouhou, K. Mershad, M. Laurent, and A. Koubaa, “Blockchain and Emerging Technologies for Next Generation Secure Healthcare,” Blockchain Research and Applications, 2025, DOI: https://doi.org/10.1016/j.bcra.2025.100305
7. K. Maithili et al., “Securing Electronic Patient Data Using Blockchain,” in Proc. IEEE ICEPE, 2025, DOI: https://doi.org/10.1109/ICEPE65965.2025.11139450
8. Bhupendra Kumar et al., “Enhancing Healthcare with Blockchain,” in Proc. IEEE ICDT, 2025, DOI: https://doi.org/10.1109/ICDT63985.2025.10986335
9. S. Rangarajan et al., “An End-to-End Decentralized Organ Donation and Transplantation System Using Blockchain,” IEEE TENSYMP, 2024, DOI: https://doi.org/10.1109/TENSYMP61132.2024.10752292
10. Jayapreethi Manoharan, Abdulrahman H Ali, Marwan M Aljohani, Anita Soni, Gowrishankar V, and Shrikant Upadhyay, “Experimental Possibilities of Decentralized Health Information System Interoperability Using Blockchain Technology,” Proc. IEEE, 2024, DOI: https://doi.org/10.1109/ICSCNA63714.2024.10863833
11. Divya Priya, M. Naga Sreeya, A. Sanjana, P. Sarayu, and M. Kista Swamy, “Enhancing Organ Donor Matching and Transparency with Blockchain Technology,” Proc. IEEE, 2024,

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

DOI: https://doi.org/10.1109/BITCON63716.2024.10985709

12. S. Igboanusi, C. A. Nnadiekwe, J. U. Ogbede, D.-S. Kim, and A. Lensky, "BOMS: Blockchain-enabled Organ Matching System," Scientific Reports, 2024, DOI: https://doi.org/10.1038/s41598-024-66375-5
13. G. Lax, R. Nardone, and A. Russo, "Enabling Secure Health Information Sharing among Healthcare Organizations by Public Blockchain," Multimedia Tools and Applications, 2024,
DOI: https://doi.org/10.1007/s11042-024-18181-4
14. N. Bansal, and K. Pandey, "Organ Harbour: A Blockchain Solution for Organ Donation and Transplantation," ACM IC3, 2024, DOI: https://doi.org/10.1145/3675888.3676050
15. V. Sitharamulu, G. Sucharitha, S. N. Mohanty, S. Janbhasha, and D. Kothandaraman, "A Private Ethereum Blockchain for Organ Donation and Transplantation Based on Intelligent Smart Contracts," Egyptian Informatics Journal, 2024, DOI: https://doi.org/10.1016/j.eij.2024.100542
16. H. Taherdoost, "Blockchain and Healthcare: A Critical Analysis of Progress and Challenges in the Last Five Years," Blockchains, 2023, DOI: https://doi.org/10.3390/blockchains1020006
17. D. Villarreal, J. García-Alonso, E. Moguel, and J. A. Hurtado, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," IEEE Access, 2023, DOI: https://doi.org/10.1109/ACCESS.2023.3236505
18. Hawashin, K. Salah, I. Yaqoob, M. C. E. Simsekler, and S. Ellahham, "Blockchain-Based Management for Organ Donation and Transplantation," IEEE Access, 2022, DOI: https://doi.org/10.1109/ACCESS.2022.3180008
19. Konkin and S. Zapechnikov, "Privacy Methods and Zero-Knowledge Proof for Corporate Blockchain," Science Direct (Procedia Computer Science), 2021, DOI: https://doi.org/10.1016/j.procs.2021.06.055
20. Rahul Ganpatrao Sonkamble, Shraddha P. Phansalkar, Vidyasagar M. Potdar, "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR," IEEE Access, 2021, DOI: https://doi.org/10.1109/ACCESS.2021.3129284

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details