

HealthVault: Blockchain-Based Electronic Health Record System with Secure Data Sharing and Access Control.

Amogha K Adur

Department of Information Science &
Engineering
amoghaadur@gmail.com
Don Bosco Institute of Technology
Bengaluru, India

Jashith Gowda M C

Department of Information Science &
Engineering
jashithgowdamc@gmail.com
Don Bosco Institute of Technology
Bengaluru, India

Mrs. Pavithra B S

Assistant Professor
Department of Information Science &
Engineering
pavithra.bsl@gmail.com
Don Bosco Institute of Technology
Bengaluru, India

Madhukumar S R

Department of Information Science &
Engineering
madhu2003jr@gmail.com
Don Bosco Institute of Technology
Bengaluru, India

Gurudarshan N

Department of Information Science &
Engineering
guruisse23054@gmail.com
Don Bosco Institute of Technology
Bengaluru, India

***Abstract**– HealthVault is a secure, decentralized electronic health record (EHR) system that utilizes blockchain technology to enable safe storage, sharing, and management of patient medical data. Conventional healthcare systems face challenges such as data breaches, poor interoperability, and limited patient control over personal health information. HealthVault overcomes these issues by employing blockchain’s immutable and transparent ledger, alongside advanced cryptographic methods, to safeguard sensitive medical records effectively.*

Keywords— Blockchain, Electronic Health Record (EHR), Secure Data Sharing, Healthcare Management, Smart Contracts, Cryptography, Patient Data Privacy, Access Control, Decentralized System, Data Security, Healthcare Interoperability, Digital Health Records, Distributed Ledger Technology (DLT), Medical Data Management, Patient Authentication.

I. INTRODUCTION

The healthcare industry is rapidly adopting digital technologies to improve the storage, management and sharing. While traditional Electronic Health Record (EHR) systems are widely used for storing patient data, they suffer from problems including data breaches, unauthorized access, lack of interoperability, and the lack of control of personal medical records by the patient. These issues can affect the security, privacy and reliability of healthcare services.

“HealthVault: Blockchain Based Electronic Health Record System with Secure Data Sharing and Access Control” is designed for providing a secure platform for patients, doctors, hospitals and insurance providers to secure access to and sharing of medical records. The system employs encryption and intelligent contracts to make sure only authorized users to access or change patient information. Patients have full control over their records and can grant and revoke access when needed.

The proposed system improves the efficiency of healthcare, enhances patient privacy, reduces the risk

of tampering with data and allows seamless communication between healthcare providers. Thus, HealthVault is a novel and reliable digital health management solution based on blockchain technology.

TABLE I. Overview of HealthVault: Blockchain-Based Electronic Health Record System with Secure Data Sharing and Access Control.

Technique	Description	Advantages	Applications
Blockchain Technology	A decentralized digital ledger for the secure storage of healthcare records.	Tamperproof storage is transparent and high security.	Medical Data Processing, Electronic Health Records (EHR).
Smart Contracts	Digital contracts for secure access and data sharing automation.	Automated access control, less manual intervention.	Sharing patient-doctor data and insurance verification securely.
Cryptography	Encryption Methods for Protecting Sensitive Medical Data.	Data privacy, safe communication, confidentiality.	Patient authentication Secure records transmission.
Access Control Mechanism	Limits access to health care data to authorized users.	Enhanced privacy and control for patients.	Hospital Management systems, cloud healthcare platforms.
Decentralized Storage	Stores records across multiple nodes instead of a single server.	Eliminates single point of failure, improves reliability.	Distributed Healthcare systems, telemedicine platforms.

I. SYSTEM DESIGN AND IMPLEMENTATION

A. *System Components:*

The system consists of multiple software elements which work together to deliver the services. For example, blockchain technology such as Ethereum or Hyperledger Fabric acts as a distributed ledger where transaction data will be recorded. Intelligent contracts technology will be used for automated authentication and authorization. The Electronic Health Record component stores patient prescription, report and other health related issue data. Encryption algorithm is used to ensure that health care data is secured from any illegal use. Patients and health care providers use Web-based UI built with HTML, CSS, and JavaScript technologies.

B. *System Implementation:*

The process starts with patient, doctor, and health care provider account creation and authentication. The medical data is captured, encrypted, and securely stored through blockchain technology. Smart contract is used to ensure that users have permission to access the system and exchange the data with other permitted users. Patients are able to control their data by allowing or denying access anytime they choose. All transactions on the platform are recorded using blockchain technology to ensure transparency.

C. *Working process:*

HealthVault's operation flow starts with user account creation, in which patients, physicians, and healthcare organizations establish their credentials. Once authenticated, the system receives the patient's health information, including prescription details, reports, and diagnostic information. The patient information is stored in the HealthVault system, with encryption and blockchain used for storing the information securely. Smart contracts facilitate authentication and permissions, permitting only authorized users to view the information. Patient information belongs to the patients themselves, who have the right to authorize or deny access to the patient data by any physician or organization at any time.

D. *System Design:*

The system is designed using a distributed blockchain approach whereby the patient's health data will be stored and managed using several nodes. The patients will be allowed to submit and manage their health records using the interface provided. Smart contracts will dictate the authentication process and permission levels to ensure only the authorized parties have access to the health care data.

E. *Security and Access Control:*

HealthVault has developed strong security measures and access control methods to secure sensitive data about health conditions. Encryption mechanisms that use cryptography

are applied to ensure patient data is secured before uploading on the blockchain network. The smart contract manages the authentication and authorization process for patients and users through verification of identity and access permissions. Patients maintain complete ownership over their medical records and determine which doctor, hospital, or insurance organization has access to the patient's files.

III. LITERATURE SURVEY

G. Gupta and R. K. Verma (2026) proposed a blockchain-based framework for secure multi-institutional electronic health record sharing using zero-knowledge proof and differential privacy techniques. The study focused on improving the privacy and security of healthcare data while enabling secure sharing among hospitals and healthcare organizations. The authors emphasized that traditional EHR systems suffer from data breaches, privacy leakage, and unauthorized access. Their proposed framework enhanced confidentiality, secure authentication, and decentralized access control through blockchain technology. The study concluded that integrating blockchain with advanced privacy-preserving techniques significantly improves secure healthcare data sharing and patient trust [1].

S. Patil. (2025) introduced "Medsecurechain," which is a blockchain architecture for privacy-preserving medical data exchange and decentralized personal health records. In this architecture, blockchain technology and smart contracts were used for secure storing, authentication, and access control of the healthcare record. The authors stressed the significance of a patient-centric approach in which the patients would have control over permissions to share their medical data. According to experimental analysis, the proposed framework increased transparency, integrity, and security against any unauthorized modifications in data, with less dependence on central healthcare servers [2].

M. Salwadkar et al. (2025) suggested blockchain-based electronic health records system for secure exchange of healthcare data. The work was aimed at ensuring interoperability between hospitals and healthcare organizations with the help of a decentralized blockchain framework. Smart contracts were used for automatic validation and authorization for access to medical records. According to the research by Salwadkar et al., blockchain technology increased data traceability and minimized data manipulation risks [3].

A. Rajasekharan and R. Koshy (2024) proposed "EMRChain," an electronic medical records management system based on blockchain technology to deliver secure and transparent storage of healthcare information. They used blockchain technology for maintaining patients' records and logging the transactions immutably. This research work focused on secure communication among patients, doctors, and healthcare organizations through encryption and authentication mechanisms. The results revealed that the inclusion of blockchain technology enhanced security, restricted unauthorized access, and made effective healthcare record management possible [4].

S Ballal. (2023) suggested blockchain-powered decentralized system for management of electronic health records. The paper examined problems associated with centralized healthcare systems, including the problem of single point of failure, manipulation of data, and lack of interoperability. Decentralized system suggested by the authors utilized blockchain technology to provide secure storage and transparent data sharing between different healthcare organizations. According to the authors, decentralized healthcare systems are more reliable, secure, and ensure patient privacy compared to traditional EHRs [5].

IV.COMPARITIVE ANALYSIS OF THE LITERATURE SURVEY

TABLE II. COMPARISON OF TECHNIQUES AND RESULTS

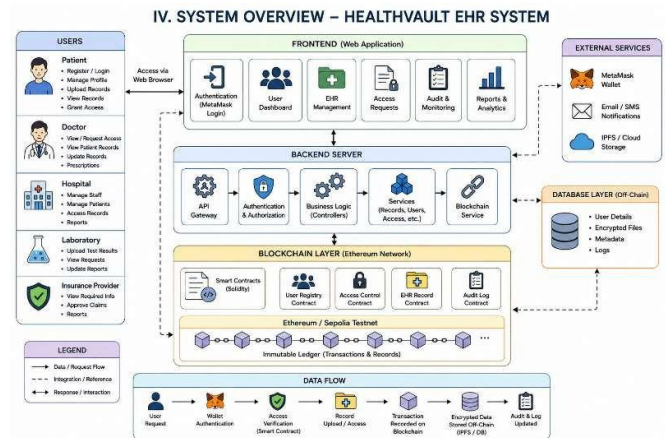
Authors	Techniques Used	Results
G. Gupta & R. K. Verma, 2026	Blockchain + Zero-Knowledge Proof + Differential Privacy	Improved privacy and secure multiinstitutional EHR sharing
S. Patil, 2025	Blockchain + Smart Contracts + Decentralized Personal Health Records	Enhanced secure medical data sharing and access control
M Salwadkar, 2024	Blockchain-Enabled Electronic Health Record System	Improved interoperability and secure healthcare communication
A. Rajasekharan & R. Koshy, 2024	EMR Chain Blockchain Framework + Encryption	Increased transparency and prevention of unauthorized access
S. Ballal, Y. Chandre, 2023	Decentralized Blockchain-Based EHR Platform	Reduced data tampering and improved patient privacy
V. Sharma, 2024	Blockchain + Smart GuardianChain Security Framework	Enhanced security for electronic health records
G. Xu et al., 2023	Blockchain-Based Healthcare Data Security System	Improved confidentiality and secure healthcare data management

III. SYSTEM OVERVIEW

HealthVault is a blockchain based Electronic Health Record (EHR) system that aims to provide secured storage, management and sharing of health care data. The system uses blockchain technology, intelligent contracts, encryption techniques and decentralized authentication mechanisms to ensure privacy, transparency and protection of patient medical records.

The system provides a web-based platform for patients, doctors, hospitals, laboratories, and insurance providers to access and manage healthcare information securely. MetaMask wallet integration and Ethereum blockchain technology are used to provide secure user authentication and decentralized access control. Smart agreements automate the permissions, authentication, and secure sharing of healthcare data among authorized users.

The health records uploaded by patients are encrypted and securely stored using the blockchain and database technologies. The blockchain network keeps transaction logs that are immutable, so unauthorized changes are impossible and data integrity is guaranteed. The system enhances healthcare security, promotes transparent data sharing, and minimizes risks associated with centralized healthcare record systems.



IV. COMPONENTS REQUIRED

Ethereum Blockchain Network

Ethereum blockchain is used to securely store transaction records and manage decentralized healthcare data sharing. It provides transparency, immutability, and protection against unauthorized modifications.

MetaMask Wallet

MetaMask Ethereum blockchain is used to securely store transaction records and manage decentralized healthcare data sharing. It provides transparency, immutability, and protection against unauthorized modifications.

Smart Contracts

Smart agreements are developed using Solidity for the automation of processes such as authentication, access control, and sharing of healthcare data in the blockchain network

Web Application Interface

The frontend web application developed using HTML, CSS, and

JavaScript provides an interactive platform for patients doctors hospitals, and healthcare providers to manage healthcare records.

Backend Server

The backend server developed using Python or Node.js handles user requests, data processing, blockchain communication, and system management functionalities.

Database Storage

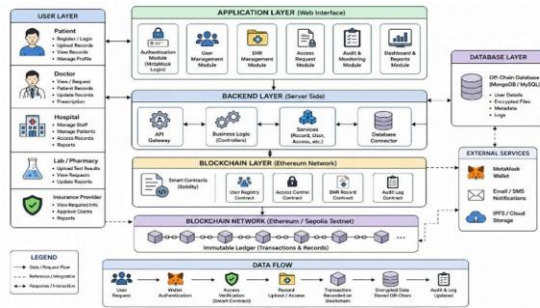
For effective data management, healthcare records, user information, metadata and system logs are securely stored in an encrypted off chain database.

Encryption Algorithms

Encryption techniques are used to safeguard sensitive patient data in healthcare and to ensure confidentiality during storage and data sharing processes.

V. SOFTWARE SYSTEM DESIGN

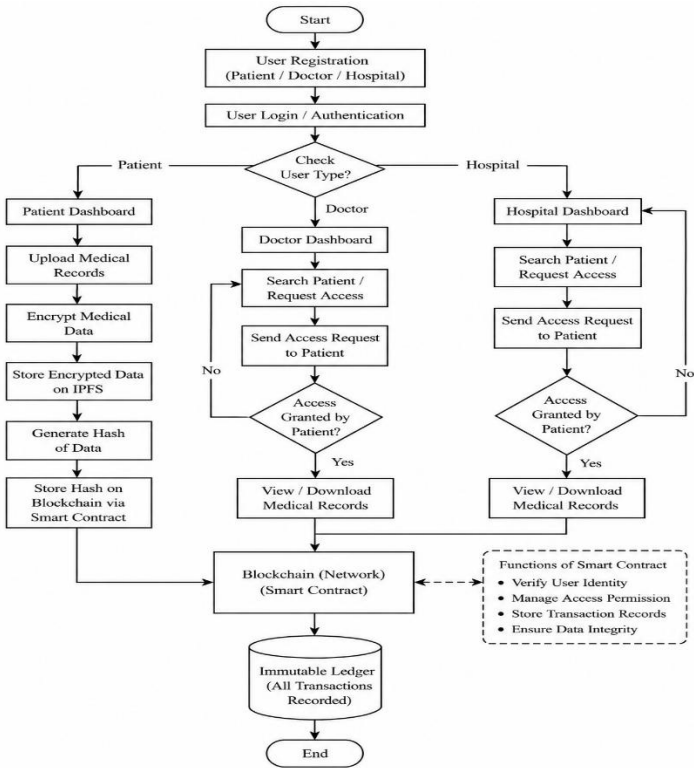
As shown in the figure below, this is the software design of the blockchain-based EHR system named HealthVault. The figure shows how the interaction takes place between patients, doctors, hospitals, laboratories, and insurance providers with the help of the HealthVault software via the secure web interface. The front-end application is connected to the back-end server where user requests, authentication, and management of healthcare data take place.



Smart contracts written using Solidity programming language are integrated with the Ethereum blockchain network for secure access control, transaction validation, and data recording purposes. Decentralized user authentication and login facility can be provided with the help of MetaMask wallet integration. The healthcare records and transaction data can be stored using blockchain and encrypted database technologies.

FLOW CHART

The flowchart shows overall operations of the HealthVault blockchain-based electronic health record system



VI. RESULTS

a. Output Results

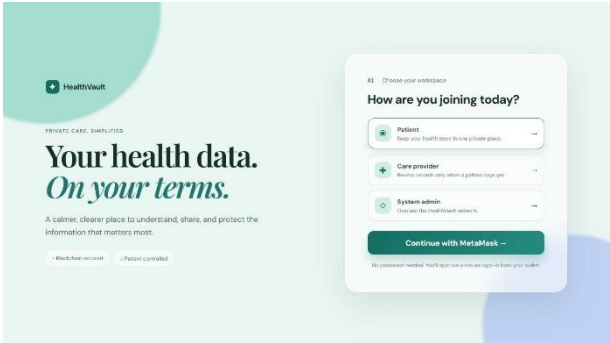


Figure: 9.1 Snapshot of the HealthVault User Workspace Selection and Secure Authentication Interface

Figure 9.2 illustrates The HealthVault web app onboarding screen, wherein the user chooses their role from among the three options (Patient, Care provider, and System admin). The app allows for secure and decentralized access authentication using a Web3 wallet (MetaMask).

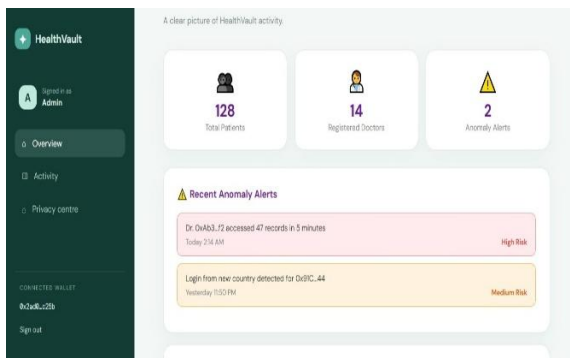


Figure: 9.2 Snapshot of The HealthVault Administrative Overview and Anomaly Monitoring Dashboard

Figure 9.2 illustrates The Admin dashboard of the HealthVault software, showing live system statistics like Total Patients (128), Registered Doctors (14), and Number of Anomaly Alerts (2). The admin console shows the software's capabilities in terms of security surveillance through alerting users about suspicious system access patterns such as high-speed access to data records (High Risk) and location-based access (Medium Risk).

VII. ADVANTAGES

Secure Data Storage:

Blockchain technology contains an opportunity where it will be possible to store the electronic health record safely through data encryption and storing in a decentralized environment. There will be no chance of data breaches taking place.

Patient-Centered Access Control:

The system gives the patients full control over their health records. The patients have the choice to either grant access to their doctor, hospitals, or even insurance companies when required.

Transparent and Traceable Transactions:

The ledger contains all the transactions and changes happening within the system. This helps ensure that everything is transparent and makes it easy for monitoring to be done.

Efficient Data Sharing:

The HealthVault enables the secure transfer of medical records of patients among various healthcare organizations. The physicians and the hospitals, once permitted, get immediate access to the medical records of the patients.

Reduced Risk of Data Tampering:

The information input in the blockchain cannot be altered without authorization since it is immutable. Therefore, there is a higher degree of integrity when using the blockchain technology for information storage.

Improved Healthcare Management:

This system helps to manage the patient records of the hospital in an effective way. This is due to the digital storage and access control that results in less paperwork and fewer errors in the healthcare process management.

VIII. APPLICATIONS

Hospital Management: Usage of HealthVault In hospitals, the software is utilized to store patient information such as records, prescriptions, diagnoses and treatments. The software employs the use of blockchain technology to ensure data protection, prevent any tampering and facilitate sharing of medical records by authorized practitioners.

Telemedicine Services: The system supports secure sharing of patient data between doctors and patients during online consultations, improving remote healthcare services and virtual treatment.

Health Insurance Management: Insurance companies can securely access verified medical records with patient permission, helping in faster claim verification and reducing fraudulent activities.

Emergency Healthcare Access: In emergency situations, authorized healthcare providers can quickly access patient medical history and treatment details, enabling faster and more accurate medical care.

Medical Research and Analysis: Researchers and healthcare organizations can use anonymized healthcare data for medical research, disease analysis, and healthcare improvements while maintaining patient privacy.

Multi-Hospital Data Sharing: The system enables secure interoperability between different hospitals and healthcare providers, allowing seamless sharing of patient records without compromising security.

CONCLUSION

HealthVault is an EHR system that applies Blockchain technology to revolutionize health data management. This system ensures secure storage, transparency, privacy, and selective sharing of the medical information of patients using encryption and smart contracts. Patients are able to control access permissions with the use of this system, thus adding to the trustworthiness of healthcare services.

The adoption of blockchain technology helps avoid the problem of accessing the information illegally, manipulating it, and relying on centralized databases. Moreover, blockchain technology facilitates interoperability between hospitals, physicians, and insurance companies because of the effective exchange of data. Thus, the HealthVault system represents an efficient, open, and patient-oriented approach to managing digital health care systems.

REFERENCES

- [1] G. Gupta and R. K. Verma, "A Zero-Knowledge Proof and Differential Privacy-Enhanced Blockchain Framework for Secure Multi-Institutional Electronic Health Record Sharing," in 2026 6th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2026.
- [2] G. Shanmugapriya, A. S. Shanthi, A. N. Abilasha, D. T. S. Dharanisankaran, and T. K. Saravanan, "MedGuardChain: Blockchain-Based Intelligent Cyber Defense Framework for Secure Electronic Health Records," in 2026 Second International Conference on Intelligent Systems for Communication, IoT and Security (ICISCOIS), 2026.
- [3] S. Patil, J. Katti, R. Pise, S. Shinde, S. Gavkare, and A. Pathan, "Medsecurechain: A Blockchain-Based Framework for Privacy-Preserving Medical Data Sharing and Decentralized Personal Health Records," in 2025 9th International Conference on Computing, Communication, Control and Automation (ICCCBEA), 2025.
- [4] M. Salwadkar, R. Balamurugan, L. H. Jasim, V. A. Narayana, J. Karpagam, K. Sravani, and Sh.B. To-Rayeva, "Blockchain-Enabled Electronic Health Records for Secure Data Sharing," in 2025 IEEE 2nd International Conference on Green Industrial Electronics and Sustainable Technologies (GIEST), 2025.
- [5] G. K. Chouhan, S. Singh, A. Jaduvansy, P. Rai, and A. Rath, "A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records," in 2025 International Conference on Intelligent and Cloud Computing (ICoICC), 2025.
- [6] M. A. Farin, S. Sikder, A. Y. Raad, M. T. Ahmed, and T. Tahlil, "HealthChain: A Blockchain-Based Framework for Electronic Health Record Management System," in 2025 IEEE/ACM 7th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2025.
- [7] U. U. Tariq, F. Sabrina, M. M. Rashid, S. Gordon, Y. Lin, Z. Wang, and S. Azad, "Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review," *IEEE Access*, vol. 13, 2025.
- [8] V. Jaiswal, R. Singh, S. B. V, and S. Kumar, "HealthGuard: A Blockchain-Based Framework for Secure EHR Management," in 2025 International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF), 2025.
- [9] R. R. Gope, N. Thapa, A. Padhi, S. K. Sharma, and D. Muduli, "MedBlock: A Blockchain-Based Framework for Secure and Decentralized Medical Record Management," in 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3), 2025.
- [10] A. Kumar, A. S. Yadav, R. K. Sachan, A. Kishor, R. Yadav, and P. K. Singh, "EHRShare: A Blockchain-Based Electronic Health Record Sharing System with Zero-Knowledge Proof," in 2025 Seventeenth International Conference on Contemporary Computing (IC3), 2025.
- [11] V. Sharma, K. Aseri, R. R. Palle, A. Agrawal, K. Tallapneni, and S. K. Jain, "Smart GuardianChain: A Solution Based on Blockchain Technology for Ensuring Security of E-Health Records in a Smart Environment," in 2023 International Conference on Smart Devices (ICSD), 2024.
- [12] S. Nekkalapudi, R. K. Mishra, and M. Pandey, "BlockchainBased Healthcare Outcome Improvement: A Decentralized Method of Patient Care," in 2024 First International Conference on Data, Computation and Communication (ICDCC), 2024.
- [13] M. Pethuraj, L. Vatchala, and S. Gayathri, "Securing Healthcare Data: Leveraging Blockchain for Electronic Health Records," in 2024 International Conference on Electronic Systems and Intelligent Computing (ICESIC), 2024.
- [14] H. Zode, V. Nawghare, S. Thete, and P. Rani, "MedyEth: Blockchain Based Electronic Healthcare Records System," in 2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2024.
- [15] A. Rajasekharan and R. Koshy, "EMRChain: Electronic Medical Records Management System using Blockchain," in 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 2024.
- [16] D. Sahu, N. Tiwari, and M. Chawla, "Blockchain as a Solution for Electronic Health Record Management: A Comprehensive Review," in 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2024.
- [17] A. Giri, R. Sandhu, M. Rakhra, and G. S. Cheema, "Blockchain Framework for Secure Patient Data Management," in 2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS), 2024.
- [18] S. Ballal, Y. Chandre, R. Pise, B. Sonare, and S. Patil, "Blockchain-Based Decentralized Platform for Electronic Health Records Management," in 2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 2023.
- [19] X. He and W. Gao, "Research on Blockchain-Based Data Sharing and Access Control Model," in 2023 IEEE International Conference on Image Processing and Computer Applications (ICIPCA), 2023.
- [20] Y. Yao, X. Cen, Y. Liu, J. Yuan, and Y. Ye, "Blockchain-based Electronic Medical Record Security Sharing Scheme," in 2023 45th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), 2023.