International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Secure Medical Image Sharing

SHAIK SHABANA[1], Dr S V Sivanagaraju[2], Dr.D.Venkatesh[3] Dr.M.Mallikarjuna Rao [4]

[1] *M.Tech Scholar Department of Computer Science & Engineering, PVKK Institution of Technology, Anantapur*

[2]*Associate Professor Department of Computer Science & Engineering, PVKK Institution of Technology, Anantapur*

[3]*Professor & HOD of CSE Department of Computer Science & Engineering, PVKK Institution of Technology, Anantapur*

[4]*Professor & HOD of CSG Department of Computer Science & Engineering, PVKK Institution of Technology, Anantapur*

Abstract - The Internet has developed into a platform which allows healthcare workers to access medical documents and files. Files need secure transmission and management because organizations must share them while safeguarding private patient details. This research evaluates different approaches which enable safe medical data sharing by showing their specific strengths and weaknesses. The two categories include centralized techniques involving encryption and watermarking, and distributed methods including blockchain and federated learning. The study investigates medical file watermarking techniques which have advanced from basic methods to modern AI-based systems. Traditional white box techniques provide easy system understanding but deep learning models function as black box systems delivering superior performance and operational flexibility. The research results show that current technological systems must deal with complex security threats which threaten the precise diagnosis of medical documents.

Key Words: Centralized Approaches, Decentralized Approaches, Medical Image Sharing, Blockchain, AI Watermarking, Federated Learning, Role-Based Access Control.

I. INTRODUCTION

The demand for secure medical file management systems has increased because healthcare facilities are adopting digital technologies. All medical files contain essential patient information which healthcare providers use to make accurate clinical assessments and create treatment strategies and deliver continuous patient care. The handling of sensitive files must be done properly because any unauthorized access will result in breaching patient privacy and disrupting clinical decision-making.

The team developed a Secure Medical File Management System which enables secure access control for Administrators, Doctors and Patients based on their specific roles. The system allows administrators to control user account creation and monitor all file access activities while safeguarding the data from unauthorized usage. Doctors use the system to access and control patient files during their diagnostic process. Patients receive the ability to upload their medical files which they can organize and access at their convenience.

The system uses advanced technologies including AI-based watermarking and encryption for safe data storage and transfer, and blockchain technology for secure data verification and access control. The system includes an automatic auditing function which records all file operations to create a complete audit trail. The solution enables healthcare professionals to work together securely while medical files remain confidential with their integrity and diagnostic value protected.

A. Objective

The project aims to develop a secure Medical File Management System which allows different user roles — admins, doctors, and patients — to access the system according to their designated permissions. The system establishes protected pathways for users to upload, view, and share files while ensuring that patient information remains confidential and all data remains secure. The system implements AI watermarking together with advanced encryption methods and blockchain technology to prevent unauthorized system entry and safeguard against data leaks and tampering incidents.

B. Scope

The project creates a secure medical file management system which uses role-based access control to protect healthcare environments. The system provides three user roles — Admin, Doctor and Patient — with capabilities to upload files, view files, share files and manage access rights. The system uses advanced encryption methods together with AI watermarking solutions and blockchain technology to protect data security and user privacy while maintaining data traceability.

II. LITERATURE SURVEY

Various research studies have developed medical image archiving and sharing systems which provide different security and operational capabilities but leave certain deficiencies unaddressed. Patel et al. (2019) created a medical image archiving and retrieval system using a centralized database with secure login to enable image upload, viewing, and storage [1]. The system lacked advanced encryption features together with role-based access control and traceability functions which created security vulnerabilities unsuitable for large healthcare settings [2].

Kumar and Singh (2021) developed a medical data sharing system which used basic watermarking technology to authenticate image content [3]. The system required artificial intelligence models to operate with blockchain technology and multiple user categories which included doctors, administrators, and patients [4]. Gupta et al. (2020) created a cloud-based medical image sharing system which used AES encryption to protect image transmission [5]. The system failed to offer methods for confirming image integrity while tracking user activities [6].

Rao and Mehta (2018) developed a patient–doctor portal which enables users to upload medical reports and images but its communication system falls short because it does not have proper authentication measures, audit logging and role-based access controls [7]. Sharma et al. (2022) created a secure medical image transmission system which enables unchangeable medical image transfers through blockchain technology while providing advanced tracking capabilities. The system gained better transparency through blockchain integration yet required more processing power [8].

III. PROPOSED SYSTEM

The secure Medical File Management System operates with role-based access control to serve three user groups: Admins, Doctors, and Patients. The system protects data through advanced encryption technology, AI-based watermarking, and complete access restriction. The system enables secure medical file handling through role-based access control which enables users to upload and share files while protecting specific information from unauthorized users.

The system uses modern technologies including blockchain and federated learning to improve its ability to track data and protect user information and maintain data accuracy. Blockchain encrypts and securely stores files because it creates tamper-proof records which maintain all access and sharing activities visible to authorized users. The system enables healthcare professionals to work together securely while maintaining medical file confidentiality and diagnostic integrity.

Fig -1: Block Diagram for Proposed System

IV. METHODOLOGY

The project creates a protected Medical File Management System which uses role-based access control to safeguard sensitive medical data through limited access and traceable sharing methods. The system secures medical documents using encryption, AI-based watermarking, blockchain-based audit systems and controlled access methods which protect files throughout their complete lifecycle from upload to approved distribution.

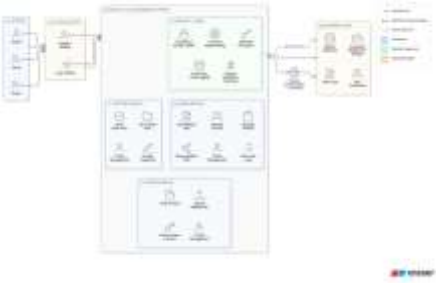

Fig -2: System Architecture

A. Working Principle

The system uses a secure access system that assigns different access rights to users based on their roles. Users including Admins, Doctors and Patients must complete a secure login process for identity verification. The RBAC framework controls access rights after authentication. Patients upload medical files which are immediately encrypted before database storage to block unauthorized access. AI creates invisible watermarks which protect file ownership and alert users to file tampering while maintaining diagnostic quality.

The system tracks all activities through a blockchain-based ledger together with a secure audit log which records every file upload, access and sharing activity to maintain complete visibility and unchangeable records. When a doctor accesses patient files, the system checks authorization before decrypting the file for display while recording the entire process. This workflow enables secure teamwork which safeguards patient data and ensures proper medical record handling.

B. Technical Tools and Frameworks

The system is built using contemporary secure technological infrastructure. ReactJS develops the frontend enabling an interactive and accessible interface. The backend uses Java for user authentication, encryption processes, watermark creation, blockchain development and API operations. MySQL database securely stores user credentials, role details, metadata and encrypted file references. Advanced Encryption Standards and RSA encryption create strong data protection during storage and transmission. The AI-enabled watermarking system embeds invisible marks into medical documents. Blockchain establishes permanent audit trails which record file access and sharing activities. HTTPS secure communication protocols stop data interception attacks.

C. Security Methods

The system implements multiple security techniques together with management protocols to achieve complete safeguard of medical records. Advanced encryption techniques render data inaccessible to unauthorized users who breach the database. AI-driven watermarking embeds invisible identification marks into medical files to detect tampering and unauthorized distribution while preserving diagnostic integrity. Blockchain-based logging creates permanent records of file transactions. Role-Based Access Control restricts system functionalities according to user roles which reduces internal security risks. Hashing techniques confirm file integrity while detecting unauthorized changes.

V. MODULES AND IMPLEMENTATION

A. User Module

The User Module permits patients to manage their personal medical information throughout the entire medical file lifecycle from registration to secure file sharing and review. The system protects patient activities through encryption, AI-driven watermarking and blockchain-based audit logs while upholding complete privacy and access security.

- Registration and Login: Patients create user accounts and access the system through secure login with authentication methods that verify user identities.
- Medical File Upload: Patients submit medical reports, prescriptions and diagnostic images. All uploaded files are automatically encrypted for secure storage.
- View My Files: Patients access their uploaded medical files. Files are decrypted only when users with permission access them during authorized times.
- Authorize Doctor Access: Patients provide specific permission to particular doctors requiring access to their medical records.
- Activity Monitoring: Access history logs enable patients to see who entered or viewed their files, maintaining transparency and accountability.

B. Doctor Module

Healthcare professionals use Doctor Module to access protected tools enabling them to review patient medical records for diagnostic and treatment needs. The system ensures that doctors can only access files authorized by patients or administrators. All file interactions use encryption methods which establish watermark protections while creating records to protect confidential information.

- Secure login and authentication to access the dashboard with professional verification.
- Access to medical records shared by authorized patients with full encryption protection.
- AI-based watermark verification to authenticate documents and identify unauthorized changes.
- Secure file access and sharing of diagnostic evaluation files according to assigned access permissions.

• Secure audit log files recording all document access and user activities for full transparency.

C. Admin Module

The Admin Module provides administrators with essential tools to manage user accounts, monitor system activities and implement security protocols. The admin supervises all aspects of medical file management ensuring encryption standards, watermarking mechanisms and audit logging procedures are maintained.

• Protected Admin Login: Authorized administrators access a secure dashboard to monitor and manage all system operations.

• User Management: The admin creates new doctor and patient accounts while making updates and deleting accounts as necessary.

• File Monitoring: The admin monitors all uploaded documents with their corresponding records and blockchain-based audit trails.

• Role-Based Access Control (RBAC): The admin restricts user access rights to authorized system functions.

• Activity Tracking: The admin tracks all file-related activities including uploading, downloading and sharing files to detect security threats.

VI. DISCUSSION AND RESULTS

A. Homepage

The landing page provides all users — admin, doctor, patient — full access to login or registration functionality, serving as the primary entry point to the system.

Fig -1: Homepage

B. Register Page

The interface enables users to establish new Doctor or Patient accounts through required personal information and authentication login details for system access.

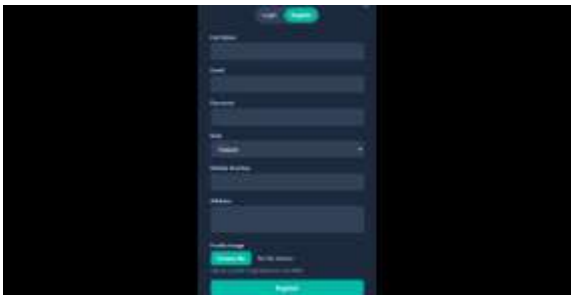

Fig -2: Register Page

C. Login Page

A secure system requiring users to provide email and password credentials for authentication to access their respective dashboards according to their Admin, Doctor or Patient roles.

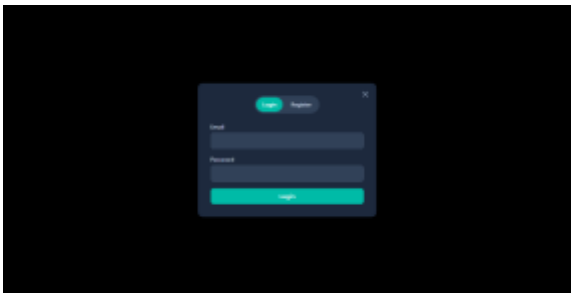

Fig -3: Login Page

D. Admin Dashboard

After successful admin login, the admin dashboard is displayed providing full system management capabilities including user and file management controls.

Fig -4: Admin Dashboard

E. Manage Users

An admin-exclusive capability allows access to view or delete the doctor and patient profiles in the medical portal with complete user management controls.

Fig -5: Manage Users

F. Manage Files

A feature enabling authorized users such as Admins or Doctors to view, verify, share, or delete uploaded medical files stored in the system.

Fig -6: Manage Files

G. Manage Secrets

Administrative module used for holding keys, access tokens, or confidential parameters in relation to medical file protection, sharing, and user authentication.

Fig -7: Manage Secrets

H. Doctor Dashboard

After successful doctor login, the doctor dashboard is displayed providing tools to access and manage authorized patient files for diagnostic purposes.

Fig -8: Doctor Dashboard

I. View Patient Files

The system provides doctors with a secure method to access and examine medical files uploaded by their designated patients for the purposes of diagnosis and monitoring.

Fig -9: View Patient Files

J. Doctor View Profile

A user-specific page displaying personal information and role details for the doctor user with complete profile management capabilities.

Fig -10: Doctor View Profile

K. Patient Dashboard

After successful patient login this dashboard is displayed providing access to upload, view and manage their medical files.

Fig -11: Patient Dashboard

L. Upload File

A secure feature enabling patients to submit their medical files including X-rays and MRIs for storage, diagnosis or sharing with authorized doctors.

Fig -12: Upload File

M. View All Files

A functionality enabling patients to access all their uploaded medical files with full decryption support for authorized file viewing.

Fig -13: View All Files

N. Patient View Profile

A user-specific page displaying personal information and role details for the patient user with complete profile management capabilities.

Fig -14: Patient View Profile

VII. CONCLUSIONS

The Medical File System we propose establishes a protected medical record management system which enables Doctors, Patients and Admins to exchange confidential medical documents through monitored access. The system employs state-of-the-art encryption methods together with AI-based watermarking technology to protect data security while enabling tracking of information and precise medical assessment. The system uses role-based access control to enhance security because this feature prevents unwanted users from entering the system. The system supports future technology advancements through its modular design which allows for blockchain and federated learning system integrations. The system provides improved functions that help medical staff treat patients better while improving data management through collaboration with various stakeholders. The system provides a trustworthy solution for managing medical images which ensures protection throughout its operation in contemporary healthcare settings.

VIII. FUTURE ENHANCEMENTS

The Medical File System requires upcoming enhancements because its existing capabilities fail to meet future healthcare delivery requirements. Blockchain technology will create permanent access records that guarantee secure document sharing while establishing transparent operations. Hospitals will use federated learning to develop AI systems while protecting patient data confidentiality. AI diagnostic tools will help doctors identify medical file irregularities with increased speed and improved accuracy. A mobile application will enable users to securely upload and access images throughout the day. Biometric authentication methods including fingerprint scanning and facial recognition will enhance security protecting user login processes. Multi-language support will allow users from different regions to access the system without facing challenges.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the faculty members and all individuals who supported and guided this research. Their valuable insights and constructive feedback significantly contributed to the development and completion of this work.

REFERENCES

[1] Al-Busaidi, A., Mani, J., Yoosuf, M. S., & P, V. (2026). A hybrid blockchain migration framework for converting traditional databases into blockchain-based EMR systems. Scientific Reports 2026.

[2] Ali, A., Ejaz, A., Jabbar, M., Hameed, K., Mushtaq, Z., Akhter, T., & Haider, A. (2017). Performance analysis of AF, DF and DtF relaying techniques for enhanced cooperative communication. INTECH 2016, 594–599.

[3] Atariata, O., Asangansi, I., Adoghe, A., Alle, O., & Abdulsalam, U. (2026). Consolidation of health data to improve health data governance using the Multi-Source Data Analytics and Triangulation platform. BMJ Health & Care Informatics, 33(1), e101837.

[4] Dhinakaran, D., Ramani, R., Edwin Raja, S., & Selvaraj, D. (2026). Enhancing clinical data security with the contextual polynomial-based data protection model (CPDPM). Biomedical Signal Processing and Control, 111, 108329.

[5] Huber, T. A. (2026). Secure Software Testing and Validation Frameworks for SAP-Centric Cloud-Native Healthcare Machine Learning Systems. IJRPETM, 9(1), 74–85.
[6] Jain, D. A. (2026). Blockchain-Based Secure Information Management Systems for Enterprises. IJEETR, 8(1), 1–7.
[7] Kavisankar, L., Aslam, N., Vemuri, A., et al. (2026). A comprehensive bluetooth security audit framework for IoT devices. Computers & Security, 164, 104840.
[8] Liu, Z., Qin, X., Wang, L., & Tian, Y. (2026). A secure telemedicine data sharing scheme based on blockchain and crystals-dilithium. IJPEDS, 1–26.
[9] Pandey, R., Khatri, A., Panigrahi, A., et al. (2026). Blockchain for Secure and Equitable Health Data Management. Computational Intelligence in Biomedical IoMT, 417–438.
[10] Patil Nitin, S., & Alate, M. (2026). Implementing Secure Health Data Exchange with Blockchain. AI and Machine Learning in Neurology, 129–151.
[11] Raghav, A., Tripathi, A. M., Ahmad, N., et al. (2026). Secure, scalable, and interoperable healthcare data exchange using layer-2 ZK-rollups. Scientific Reports 2026, 16(1), 6132.
[12] S.K, A., & G.R, K. (2026). Computational Framework for Privacy-Regulated Healthcare Data Sharing: Iterative ZKP-Blockchain-Cloud Architecture.
[13] Thakur, A., Ranga, V., & Agarwal, R. (2026). ABHealChain: Enhancing Privacy and Security in Healthcare Data Sharing. Concurrency and Computation, 38(3), e70592.
[14] V, D. (2026). Blockchain-Enabled Secure Data Exchange for Smart AI Language Platforms. Anusandhanvallari, 279–289.
[15] Varanasi, S. R. (2026). Algorithmic Governance of Secure Health Data Pipelines. SciQuest Research Database, 6(2), 33–43.