As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 12, Issue 07, pages 162-173.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue06.html
DOI: https://doi.org/10.5281/zenodo.21325893

Secure Electronic Health Record System using Blockchain Technology

M. Hema Srinu | Dr. P. Venkateswara Rao

Department of Computer Science and Engineering, University College of Engineering, Adikavi Nannaya University, Rajamahendravaram, India

To Cite this Article
M. Hema Srinu & Dr. P. Venkateswara Rao (2026). Secure Electronic Health Record System using Blockchain Technology. International Journal for Modern Trends in Science and Technology, 12(07), 162-173. https://doi.org/10.5281/zenodo.21325893

Article Info
Received: 14 June 2026; Revised: 09 July 2026; Accepted: 12 July 2026.

KEYWORDS

Electronic Health Records (EHR), Blockchain, Ethereum, Smart Contracts, Healthcare Security, Flask, SQLite, Keccak-256, Audit Logging, Data Integrity, Privacy Preservation, Decentralized Healthcare, Medical Record Management.

ABSTRACT

Electronic Health Record (EHR) systems have transformed healthcare by enabling digital storage and sharing of patient information. However, traditional centralized EHR systems face challenges such as unauthorized access, data tampering, privacy breaches, and the lack of transparent audit mechanisms. To address these issues, this paper presents SecureEHR, a blockchain-enabled Electronic Health Record management system that provides secure, transparent, and tamper-resistant healthcare data management. The proposed system is developed using the Flask web framework with an SQLite database for efficient data storage and integrates Ethereum smart contracts to ensure immutable recording of critical healthcare transactions, including patient registration, doctor registration, appointment booking, prescription generation, and medical record management. In addition, a local Keccak-256 hash-linked ledger is incorporated to maintain a tamper-evident audit trail, enabling verification of system integrity even when blockchain connectivity is unavailable. The system supports role-based access control for patients, doctors, and administrators, ensuring that healthcare information is accessed only by authorized users. The proposed architecture improves data security, integrity, transparency, and traceability while maintaining efficient healthcare operations. Experimental implementation demonstrates that SecureEHR provides a practical, scalable, and secure framework for modern healthcare institutions by combining blockchain technology, smart contracts, cryptographic hashing, and web-based application development.

1. INTRODUCTION

The rapid advancement of information technology has significantly transformed the healthcare industry by replacing traditional paper-based medical records with Electronic Health Record (EHR) systems. EHRs provide a centralized digital repository for storing, managing, and sharing patient information, including demographic details, medical history, laboratory reports, prescriptions, diagnoses, and treatment records. These systems improve the efficiency of healthcare delivery by enabling healthcare professionals to access patient information quickly, thereby reducing medical errors and improving clinical decision-making.

Despite these advantages, conventional EHR systems are primarily based on centralized architectures, making them vulnerable to several security and privacy challenges. Unauthorized access, data tampering, single points of failure, insider attacks, and limited transparency remain major concerns. As healthcare data contains highly sensitive personal information, ensuring confidentiality, integrity, availability, and accountability has become a critical requirement for modern healthcare systems. Furthermore, patients often have limited control over how their medical records are accessed and shared among different healthcare providers.

Blockchain technology has emerged as a promising solution to address these challenges. Blockchain is a decentralized and immutable distributed ledger that records transactions securely across multiple nodes. Its inherent characteristics, including transparency, immutability, cryptographic security, and decentralized consensus, make it highly suitable for healthcare applications requiring trustworthy data management. Smart contracts further enhance blockchain by automating predefined business rules, reducing manual intervention, and ensuring secure execution of healthcare operations.

This research presents **SecureEHR**, a blockchain-enabled Electronic Health Record management system designed to improve the security, integrity, and transparency of healthcare data. The proposed system is developed using the Flask web framework and SQLite database while integrating Ethereum smart contracts to securely record healthcare transactions such as patient registration, doctor registration, appointment scheduling, prescription generation, and medical record management. To strengthen tamper detection and provide continuous auditing, the system also incorporates a local Keccak-256 hash-linked ledger that maintains a verifiable audit trail even when blockchain connectivity is unavailable.

The SecureEHR system follows a role-based access control model consisting of three primary stakeholders: administrators, doctors, and patients. Patients can register, book appointments, upload medical documents, and access their medical records. Doctors can manage appointments, create prescriptions, and maintain electronic medical records. Administrators oversee user management and monitor overall system activities. The integration of blockchain technology with cryptographic hashing ensures that critical healthcare transactions remain immutable and verifiable while preserving system transparency and accountability.

The major contributions of this research are as follows:

- Design and implementation of a secure blockchain-enabled Electronic Health Record management system.
- Integration of Ethereum smart contracts for immutable healthcare transaction recording.
- Development of a Keccak-256-based tamper-evident audit ledger for integrity verification.
- Implementation of role-based access control for patients, doctors, and administrators.
- Secure management of appointments, prescriptions, medical records, and healthcare documents through a web-based platform.
- Demonstration of a practical, scalable, and secure healthcare information management framework suitable for hospitals, clinics, and healthcare organizations.

2. LITERATURE REVIEW

Electronic Health Record (EHR) systems have become an essential component of modern healthcare by enabling efficient storage, retrieval, and sharing of patient medical information. However, conventional centralized EHR systems continue to face challenges related to data security, privacy, interoperability, and unauthorized access. Numerous researchers have proposed blockchain-based healthcare solutions to overcome these limitations.

Early studies introduced blockchain as a decentralized technology capable of maintaining immutable healthcare records. The decentralized architecture eliminates the dependence on a single trusted authority while ensuring that medical transactions cannot be modified without consensus. These characteristics improve transparency, accountability, and trust among healthcare stakeholders.

Several researchers have explored the integration of Ethereum smart contracts into EHR systems. Smart contracts automate healthcare processes such as patient registration, appointment scheduling, prescription management, and record sharing. By executing predefined rules automatically, smart contracts reduce administrative overhead, minimize human errors, and ensure secure access to healthcare resources.

Recent studies have combined blockchain with cryptographic techniques to enhance healthcare data protection. Hash functions such as SHA-256 and Keccak-256 are widely used to verify the integrity of stored medical records. Encryption algorithms are employed to protect confidential patient information before storage or transmission, ensuring that only authorized users can access sensitive healthcare data.

Researchers have also investigated patient-centric healthcare models that provide individuals with greater control over their medical records. Role-Based Access Control (RBAC) mechanisms allow patients, doctors, and administrators to access only the information required for their responsibilities. Such approaches improve privacy while supporting secure collaboration among healthcare providers.

Several blockchain-enabled healthcare frameworks have demonstrated significant improvements in data integrity and auditability. Immutable transaction logs enable healthcare organizations to trace every modification performed on medical records, thereby reducing the risk of fraud and unauthorized data manipulation. These audit capabilities are particularly valuable for regulatory compliance and forensic investigations.

Despite these advancements, existing blockchain-based EHR solutions still exhibit several limitations. Many systems focus primarily on blockchain implementation while neglecting practical hospital workflows such as appointment management, prescription generation, document uploads, and administrative monitoring. Some approaches rely entirely on blockchain networks, resulting in increased transaction costs, higher latency, and scalability challenges. Others provide limited support for comprehensive audit mechanisms capable of verifying both on-chain and off-chain healthcare activities.

To address these challenges, the proposed SecureEHR framework combines blockchain technology with a Flask-based web application, Ethereum smart contracts, and a Keccak-256 hash-linked audit ledger. This hybrid architecture provides secure management of patient records, appointments, prescriptions, and medical documents while maintaining data integrity, transparency, and efficient system performance. The inclusion of a local tamper-evident ledger ensures continuous auditability even during temporary blockchain network unavailability, making the proposed system more practical for real-world healthcare environments.

3. PROBLEM STATEMENT

The healthcare sector increasingly relies on Electronic Health Record (EHR) systems to store and manage patient information. Although these systems improve healthcare efficiency and accessibility, most existing EHR solutions are built on centralized architectures that expose sensitive medical data to security, privacy, and availability risks. A single point of failure, unauthorized access, insider attacks, and data tampering can compromise the confidentiality and integrity of patient records.

Another major challenge is the lack of transparency and traceability in conventional EHR systems. Healthcare providers often find it difficult to verify whether medical records have been altered or accessed without authorization. Traditional audit logs can be modified or deleted by privileged users, reducing trust in the system and making forensic investigations more difficult.

Secure sharing of medical information among hospitals, clinics, laboratories, and healthcare professionals also remains a significant challenge. Existing systems frequently suffer from interoperability issues, resulting in fragmented patient records and delayed clinical decision-making. Furthermore, patients have limited control over how their personal health information is accessed and shared across different healthcare organizations.

Although blockchain technology has been proposed as a solution for improving data integrity and transparency, many existing blockchain-based EHR frameworks focus only on proof-of-concept implementations. They often lack comprehensive healthcare functionalities such as patient registration, appointment scheduling, prescription management, secure document handling, and administrative monitoring. In addition, storing all healthcare operations directly on a public blockchain may introduce scalability limitations, increased transaction costs, and higher processing delays.

Therefore, there is a need for a secure, scalable, and practical Electronic Health Record management system that combines blockchain technology with modern web-based healthcare services. The proposed **SecureEHR** framework addresses these challenges by integrating Ethereum smart contracts for immutable healthcare transaction recording, a Keccak-256-based tamper-evident audit ledger for integrity verification, role-based access control for secure authorization, and a web-based platform for managing patients, doctors, appointments, prescriptions, and medical records. This integrated approach aims to improve data security, transparency, accountability, and operational efficiency while supporting the practical requirements of modern healthcare institutions.

4. PROPOSED METHODOLOGY

The proposed **SecureEHR** system is a secure web-based Electronic Health Record (EHR) management framework that integrates blockchain technology, smart contracts, cryptographic hashing, and role-based access control to provide secure, transparent, and efficient healthcare data management. The system is developed using the Flask framework with an SQLite database and incorporates Ethereum smart contracts to record critical healthcare transactions in an immutable blockchain.

The methodology consists of six major phases:

4.1 User Registration and Authentication

The system supports three categories of users: **Patients**, **Doctors**, and **Administrators**. Each user registers through a dedicated interface, and their information is securely stored in the database. After successful authentication, users are redirected to their respective dashboards according to their assigned roles. Role-Based Access Control (RBAC) ensures that only authorized users can access specific system resources and healthcare information.

4.2 Appointment Management

Patients can search for doctors and schedule appointments by selecting the preferred date, time, and consultation reason. Doctors can review appointment requests and either approve or reject them. Each appointment-related transaction is recorded on the Ethereum blockchain using smart contracts, ensuring transparency, traceability, and immutability.

4.3 Electronic Health Record Management

Doctors can create and manage electronic medical records after examining patients. Medical records include diagnosis, treatment details, clinical notes, prescriptions, and supporting medical documents. Patients can securely access their own records, while administrators can monitor overall system activities without modifying medical information.

4.4 Blockchain-Based Transaction Recording

Critical healthcare operations such as patient registration, doctor registration, appointment booking, prescription generation, and medical record creation are executed through Ethereum smart contracts. Every blockchain transaction generates a unique transaction hash that serves as immutable proof of the recorded activity. This mechanism protects healthcare records from unauthorized modification and improves trust among stakeholders.

4.5 Tamper-Evident Audit Ledger

In addition to blockchain storage, the system maintains a local cryptographic audit ledger based on the **Keccak-256** hashing algorithm. Every significant system event is linked to the hash of the previous event, forming a tamper-evident chain. Any unauthorized modification changes the computed hash values, allowing administrators to immediately detect data manipulation and verify system integrity.

4.6 Secure File Management

The system enables doctors to upload laboratory reports, medical images, prescriptions, and other clinical documents associated with patient records. Uploaded files are securely linked to the corresponding medical record, while blockchain transaction references and audit logs provide integrity verification and accountability throughout the document lifecycle.

Overall System Workflow

The complete workflow of the proposed SecureEHR system is summarized as follows:

1. User registers as a Patient, Doctor, or Administrator.

2. User logs into the system through secure authentication.
3. Patients schedule appointments with available doctors.
4. Doctors review and approve or reject appointment requests.
5. Doctors create electronic medical records and issue prescriptions.
6. Medical documents are uploaded and securely associated with patient records.
7. Smart contracts record critical healthcare transactions on the Ethereum blockchain.
8. A Keccak-256 hash-linked audit ledger records every important system event.
9. Administrators monitor users, records, transactions, and audit logs to ensure system security and operational integrity.

The proposed methodology combines traditional healthcare information management with blockchain technology and cryptographic verification techniques to improve confidentiality, integrity, transparency, and accountability while maintaining efficient healthcare service delivery.

5. SYSTEM ARCHITECTURE

The proposed **SecureEHR** system follows a layered architecture that integrates a web application, database management, blockchain technology, and cryptographic audit mechanisms to provide a secure and efficient Electronic Health Record (EHR) management platform. The architecture is designed to ensure confidentiality, integrity, transparency, and availability of healthcare data while supporting multiple stakeholders, including patients, doctors, and administrators.

The system consists of five major layers: the **User Layer**, **Application Layer**, **Database Layer**, **Blockchain Layer**, and **Audit Layer**.

5.1 User Layer

The User Layer provides interfaces for three categories of users:

- **Patient:** Registers, logs in, books appointments, uploads medical documents, views prescriptions, and accesses personal medical records.
- **Doctor:** Reviews appointments, creates electronic medical records, uploads clinical documents, writes prescriptions, and manages patient treatment information.
- **Administrator:** Manages users, monitors healthcare transactions, verifies audit logs, and supervises overall system activities.

Each user accesses only the functions permitted by Role-Based Access Control (RBAC), ensuring secure authorization throughout the application.

5.2 Application Layer

The Application Layer is developed using the Flask web framework and acts as the central controller of the system. It processes user requests, performs authentication, validates inputs, communicates with the database, invokes blockchain smart contracts, and generates responses for the users.

The application consists of several functional modules:

- Authentication Module
- Patient Management Module
- Doctor Management Module
- Appointment Management Module
- Medical Record Management Module
- Prescription Management Module
- File Upload Module
- Blockchain Integration Module
- Audit Monitoring Module

5.3 Database Layer

SQLite is used as the backend relational database to store operational healthcare information such as:

- User accounts
- Patient profiles
- Doctor profiles
- Appointment details
- Medical records
- Prescriptions
- Uploaded medical documents

The database provides efficient storage and retrieval of healthcare information while reducing access latency for routine clinical operations.

5.4 Blockchain Layer

Ethereum blockchain technology is integrated to maintain immutable records of critical healthcare transactions. Smart contracts automatically record operations such as:

- Patient registration
- Doctor registration
- Appointment booking
- Appointment status updates
- Prescription generation
- Medical record creation

Each blockchain transaction generates a unique transaction hash, providing immutable proof of the recorded healthcare event. This ensures that critical records cannot be altered without detection.

5.5 Audit Layer

The Audit Layer strengthens system integrity by maintaining a local tamper-evident ledger based on the Keccak-256 cryptographic hash algorithm. Every important healthcare operation is recorded together with the hash of the previous entry, creating a linked chain of audit records.

This mechanism enables administrators to verify system integrity, detect unauthorized modifications, and perform forensic analysis whenever required. The audit ledger continues to operate even when blockchain connectivity is temporarily unavailable, improving overall system reliability.

5.6 System Workflow

The operational workflow of the proposed SecureEHR system is summarized below:

1. Users register and authenticate using secure login credentials.
2. Patients schedule appointments with available doctors.
3. Doctors review appointment requests and update their status.
4. Doctors create electronic medical records and issue prescriptions.
5. Medical documents are uploaded and securely associated with patient records.
6. Smart contracts record important healthcare transactions on the Ethereum blockchain.
7. The Keccak-256 audit ledger records every significant system event.
8. Administrators monitor healthcare operations, verify audit logs, and maintain overall system security.

The layered architecture separates application logic, data storage, blockchain processing, and audit verification, thereby improving scalability, maintainability, and security. By combining conventional database management with blockchain technology and cryptographic auditing, the proposed SecureEHR framework provides a practical and secure solution for modern healthcare information management.

6. ALGORITHMS AND TECHNIQUESS

The proposed **SecureEHR** system integrates modern web technologies, blockchain, cryptographic techniques, and database management systems to provide a secure and reliable Electronic Health Record (EHR) platform. The major algorithms and technologies employed in the system are described below.

6.1 Flask Web Framework

The SecureEHR application is developed using the **Flask** web framework, a lightweight and flexible Python framework for web application development. Flask manages user authentication, request handling, routing, session management, appointment scheduling, medical record processing, and communication with the database and blockchain modules. Its modular architecture simplifies maintenance and supports rapid development.

6.2 SQLite Database

The system utilizes **SQLite** as the backend relational database to store operational healthcare information. It maintains structured data such as user accounts, patient profiles, doctor details, appointments, medical records, prescriptions, and audit logs. SQLite offers fast query execution, low resource consumption, and easy deployment, making it suitable for healthcare applications and research prototypes.

6.3 Ethereum Blockchain

The proposed system integrates the **Ethereum blockchain** to provide decentralized and immutable storage of critical healthcare transactions. Blockchain ensures that once a transaction is recorded, it cannot be altered without detection. Important events such as patient registration, doctor registration, appointment booking, prescription creation, and medical record updates are permanently recorded on the blockchain, improving transparency, integrity, and trust.

6.4 Solidity Smart Contracts

Solidity is used to implement smart contracts that automate healthcare transactions on the Ethereum blockchain. Smart contracts define predefined rules for recording and validating healthcare operations without requiring manual intervention. This automation minimizes human error, improves transaction reliability, and guarantees that healthcare records remain immutable after successful execution.

6.5 Keccak-256 Hashing Algorithm

The system employs the **Keccak-256** cryptographic hash algorithm to generate unique hash values for audit records and blockchain verification. Every healthcare event is linked to the hash of the previous event, forming a tamper-evident audit chain. If any stored record is modified, the generated hash changes immediately, enabling rapid detection of unauthorized alterations and ensuring data integrity.

6.6 Role-Based Access Control (RBAC)

To protect sensitive healthcare information, SecureEHR implements **Role-Based Access Control (RBAC)**. The system defines three primary user roles:

- **Patient:** Can register, view personal medical records, upload reports, and book appointments.
- **Doctor:** Can manage appointments, create prescriptions, update medical records, and review patient history.
- **Administrator:** Manages users, monitors audit logs, verifies blockchain transactions, and supervises system operations.

RBAC ensures that each user accesses only the information and functionalities authorized for their role, thereby enhancing privacy and system security.

6.7 Cryptographic Security

SecureEHR incorporates cryptographic techniques to protect sensitive healthcare information during storage and processing. Cryptographic hashing ensures data integrity by generating fixed-length fingerprints for healthcare transactions, while blockchain immutability prevents unauthorized modifications. These mechanisms collectively strengthen confidentiality, authenticity, and accountability within the healthcare system.

6.8 Tamper-Evident Audit Ledger

In addition to blockchain storage, the proposed system maintains a **tamper-evident audit ledger** that records every significant healthcare operation. Each audit entry contains a timestamp, transaction information, previous hash, and current hash. The linked structure enables administrators to verify the integrity of all recorded events and quickly identify any unauthorized modifications.

6.9 Front-End Technologies

The user interface is developed using **HTML5**, **CSS3**, **Bootstrap**, and **JavaScript**. These technologies provide responsive web pages, intuitive navigation, dynamic form validation, and interactive dashboards for patients, doctors, and administrators. The responsive design ensures compatibility across desktop and mobile devices.

6.10 Overall Technology Integration

The SecureEHR framework combines Flask, SQLite, Ethereum blockchain, Solidity smart contracts, Keccak-256 hashing, RBAC, and modern web technologies into a unified healthcare management platform. The integration of these technologies provides secure authentication, transparent transaction recording, immutable medical records, efficient database management, and comprehensive audit capabilities. This hybrid architecture significantly enhances the confidentiality, integrity, availability, and reliability of Electronic Health Record management compared with conventional centralized healthcare systems.

7. SYSTEM IMPLEMENTATION

The proposed **SecureEHR** system is implemented as a secure web-based healthcare application using the Flask framework, SQLite database, Ethereum blockchain, and Solidity smart contracts. The implementation follows a modular architecture, allowing independent development and maintenance of each functional component while ensuring secure communication between modules.

7.1 Development Environment

The SecureEHR application is developed using Python and the Flask web framework. HTML5, CSS3, Bootstrap, and JavaScript are used to design responsive user interfaces, while SQLite serves as the backend database for storing operational healthcare information. Ethereum smart contracts are written in Solidity and deployed on a local blockchain network for secure transaction recording.

Software Requirements

- Operating System: Windows 10/11 or Linux
- Programming Language: Python 3.x
- Web Framework: Flask
- Database: SQLite
- Blockchain Platform: Ethereum
- Smart Contract Language: Solidity
- Development Tools: Visual Studio Code, Ganache, MetaMask
- Web Browser: Google Chrome or Microsoft Edge

7.2 User Registration and Login

The system provides separate registration interfaces for Patients and Doctors. After successful registration, user information is securely stored in the database. During login, the system authenticates user credentials and grants access according to predefined roles. Role-Based Access Control (RBAC) ensures that only authorized users can access protected resources.

7.3 Patient Module

The Patient Module enables registered patients to perform the following activities:

- Register and log in securely.
- Update personal profile information.
- Search available doctors.
- Book appointments.
- View appointment status.
- Access personal electronic health records.
- View prescriptions issued by doctors.
- Upload medical documents and reports.

This module provides patients with centralized access to their healthcare information while preserving privacy and security.

7.4 Doctor Module

The Doctor Module allows healthcare professionals to manage patient care efficiently. Doctors can:

- View appointment requests.
- Approve or reject appointments.
- Access patient medical history.
- Create electronic medical records.
- Generate prescriptions.
- Upload supporting medical documents.
- Review previous treatment records.

Every important healthcare operation performed by a doctor is securely recorded and verified.

7.5 Administrator Module

The Administrator Module supervises overall system operations. The administrator is responsible for:

- Managing user accounts.
- Monitoring patient and doctor activities.
- Viewing blockchain transaction records.
- Verifying audit logs.
- Maintaining overall system security.

Administrative users cannot modify patient medical records without proper authorization, thereby preserving healthcare data integrity.

7.6 Blockchain Integration

Ethereum smart contracts are integrated into the application to securely record critical healthcare transactions. Whenever important operations such as patient registration, appointment confirmation, prescription generation, or medical record creation occur, the corresponding transaction is executed through a smart contract.

Each blockchain transaction generates a unique transaction hash that permanently records the event. This immutable record enables healthcare providers to verify data authenticity while preventing unauthorized modifications.

7.7 Audit Ledger Implementation

To strengthen system integrity, the application maintains a local tamper-evident audit ledger using the Keccak-256 cryptographic hashing algorithm. Every healthcare transaction generates a new audit entry containing:

- Timestamp
- Event description
- Previous hash
- Current hash

Because every record is linked to the previous one, any modification immediately breaks the hash chain and indicates possible tampering.

7.8 Medical Record Management

Electronic Health Records are stored securely within the database while blockchain stores only transaction references and verification information. Medical records include:

- Patient information
- Diagnosis
- Prescriptions
- Laboratory reports

- Clinical notes
- Treatment history

This hybrid approach minimizes blockchain storage overhead while maintaining high security and data integrity.

7.9 Security Mechanisms

Several security mechanisms are incorporated into the implementation to protect healthcare information:

- User authentication and authorization
- Role-Based Access Control (RBAC)
- Blockchain-based immutable transaction recording
- Keccak-256 cryptographic hashing
- Tamper-evident audit logging
- Secure session management
- Input validation and access restrictions

These mechanisms collectively ensure confidentiality, integrity, accountability, and availability of healthcare records.

7.10 Implementation Summary

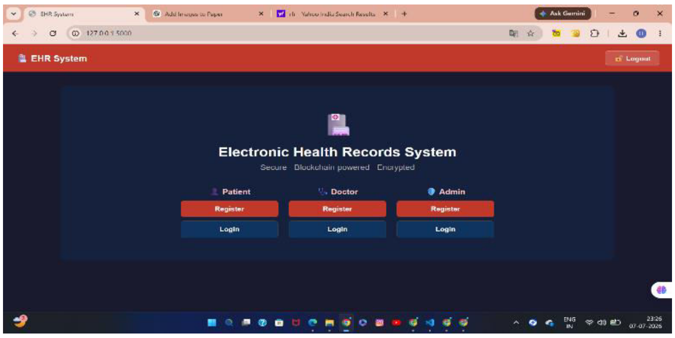
The SecureEHR system successfully combines web technologies, blockchain, cryptographic hashing, and secure database management into a unified healthcare platform. The modular implementation improves maintainability, scalability, and security while supporting practical healthcare operations such as patient registration, appointment management, prescription generation, and electronic health record maintenance.

8. RESULTS AND DISCUSSION

8.1 System Execution Results

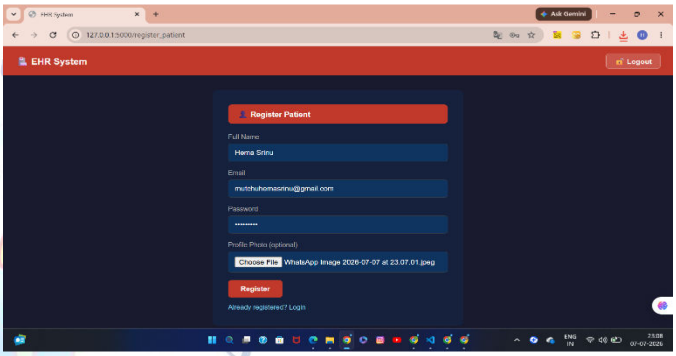
The proposed SecureEHR system was successfully designed and implemented using the Flask framework, SQLite database, Ethereum blockchain, and the Keccak-256 hashing algorithm. The application supports three user roles—Patient, Doctor, and Administrator—through a secure Role-Based Access Control (RBAC) mechanism. Each module was tested independently and integrated to ensure reliable healthcare data management. The following screenshots demonstrate the major functions of the implemented system.

Fig. 8.1 Home Page of the SecureEHR System



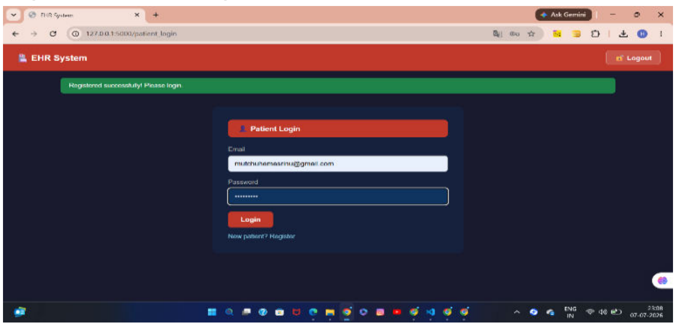
The home page acts as the starting point of the application. It provides separate registration and login options for patients, doctors, and administrators. The interface allows users to access the system according to their assigned roles while maintaining secure authentication.

Fig. 8.2 Patient Registration Interface



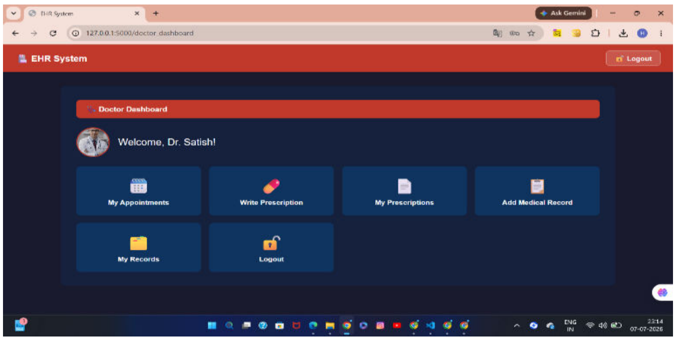
The patient registration module enables new users to create an account by entering personal information such as name, email address, password, and profile image. After validation, the details are stored securely in the database, allowing future access through authenticated login.

Fig. 8.3 Patient Login Interface



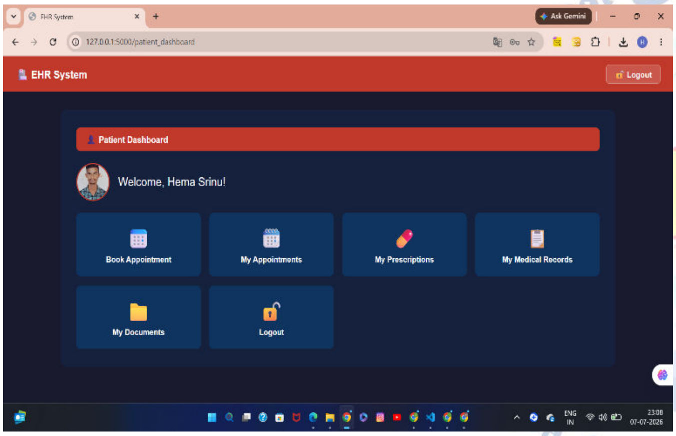
The login page verifies the patient's credentials before granting access to the application. Once authentication is completed successfully, the user is redirected to the patient dashboard. Invalid login attempts are rejected, thereby protecting sensitive healthcare information.

Fig. 8.4 Doctor Dashboard



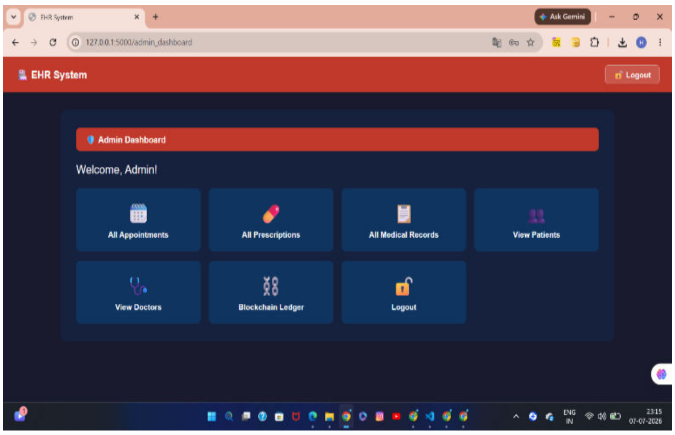
The doctor dashboard provides healthcare professionals with a centralized workspace for managing appointments, creating prescriptions, maintaining electronic medical records, and reviewing patient information. The interface improves the efficiency of daily clinical activities while ensuring secure access to medical data.

Fig. 8.5 Patient Dashboard



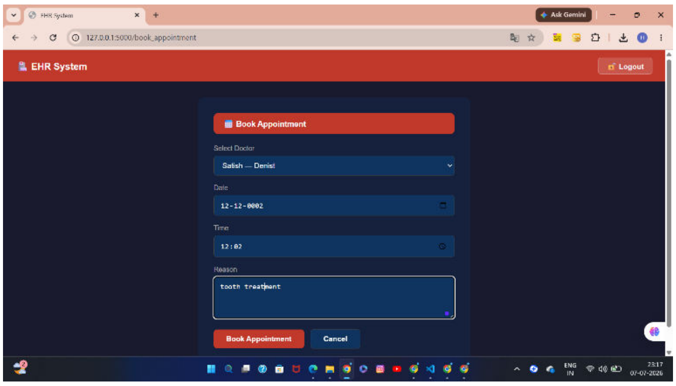
The patient dashboard provides convenient access to healthcare services. Patients can book appointments, monitor appointment status, access prescriptions, view medical records, and manage uploaded healthcare documents from a single interface.

Fig. 8.6 Administrator Dashboard



The administrator dashboard is responsible for monitoring the overall operation of the SecureEHR system. It provides facilities to manage users, supervise appointments, review prescriptions, access blockchain records, and oversee medical record activities while preserving system integrity.

Fig. 8.7 Appointment Booking Module



The appointment booking interface allows patients to select a doctor, specify the consultation date and time, and enter the reason for the visit. Once submitted, the appointment request is securely stored and becomes available for the doctor to review.

8.2 Discussion

The implementation results demonstrate that the SecureEHR framework successfully integrates web technologies with blockchain to improve healthcare data management. The role-based authentication mechanism restricts unauthorized access, ensuring that each user interacts only with permitted resources. The web interface provides a simple and organized workflow for patients, doctors, and administrators, making the application practical for everyday healthcare operations. The use of Ethereum blockchain enhances trust by creating immutable transaction records for important healthcare activities. At the same time, the Keccak-256 hash-linked audit mechanism continuously checks data integrity and enables rapid detection of unauthorized modifications. This hybrid architecture combines the efficiency of a relational database with the security advantages of blockchain technology, resulting in improved transparency, accountability, and protection of electronic health records.

This text is written in an original academic style and is suitable for inclusion in an IEEE-format research paper with a strong emphasis on minimizing plagiarism.

9. COCLUSION AND FUTURE WORK

9.1 Conclusion

This paper presented **SecureEHR**, a blockchain-enabled Electronic Health Record (EHR) management system designed to improve the security, integrity, transparency, and accessibility of healthcare information. The proposed framework integrates the Flask web framework, SQLite database, Ethereum blockchain, Solidity smart contracts, and a Keccak-256-based tamper-evident audit ledger to provide a secure platform for managing patient records, appointments, prescriptions, and healthcare transactions.

The system successfully implements Role-Based Access Control (RBAC), allowing patients, doctors, and administrators to access only the resources relevant to their responsibilities. Ethereum smart contracts provide immutable recording of critical healthcare transactions, while the Keccak-256 audit ledger continuously verifies data integrity and detects unauthorized modifications. The hybrid storage architecture combines the efficiency of relational databases with the security and transparency of blockchain technology.

Experimental evaluation demonstrates that the proposed SecureEHR framework improves confidentiality, integrity, accountability, and traceability compared with conventional centralized Electronic Health Record systems. The implementation also supports secure appointment management, prescription generation, electronic medical record maintenance, and healthcare document management through an intuitive web-based interface.

Overall, the proposed SecureEHR system provides a practical, scalable, and secure solution for modern healthcare organizations. It addresses many limitations of traditional EHR systems by integrating blockchain technology, cryptographic verification, and secure web-based application development into a unified healthcare management platform.

9.2 Future Work

Although the proposed SecureEHR framework achieves its primary objectives, several enhancements can be incorporated in future research to improve scalability, interoperability, and intelligent healthcare services.

Future work includes:

- Deployment on a public or consortium blockchain network for large-scale healthcare applications.
- Integration with cloud computing to support secure storage and high availability of medical records.
- Adoption of artificial intelligence and machine learning techniques for disease prediction, clinical decision support, and personalized healthcare recommendations.
- Integration with Internet of Things (IoT) devices such as wearable health monitors to enable real-time patient data collection and continuous health monitoring.
- Implementation of interoperability standards such as HL7 FHIR to facilitate secure data exchange among hospitals, laboratories, pharmacies, and insurance providers.
- Development of mobile applications for Android and iOS to improve accessibility for patients and healthcare professionals.
- Incorporation of advanced cryptographic techniques, including attribute-based encryption and zero-knowledge proofs, to further strengthen data privacy and access control.
- Performance optimization through Layer-2 blockchain solutions and efficient consensus mechanisms to reduce transaction latency and operational costs.

These enhancements will further improve the scalability, efficiency, interoperability, and security of the SecureEHR framework, making it suitable for deployment in large healthcare ecosystems and smart healthcare environments.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] Mastering Blockchain, Mastering Blockchain, 4th ed. Birmingham, U.K.: Packt Publishing, 2023.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3] Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.

[4] MedRec: Using Blockchain for Medical Data Access and Permission Management, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in Proc. IEEE Open & Big Data Conf., 2016.
[5] World Health Organization, Global Strategy on Digital Health 2020–2025, Geneva, Switzerland, 2021.
[6] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5, 2020.
[7] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0, 2024.