



International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(2) (2026)



ijerst.editor@gmail.com
editor@ijerst.com

Research Paper

A SECURE PERSONAL HEALTH RECORD MANAGEMENT SYSTEM USING BLOCKCHAIN AND MACHINE LEARNING

Mohammed Mohiuddin¹, Sridhar Gummalla², Subramanian K.M³

¹PG Scholar, Department of Computer Science and Engineering.

Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086

Email: mohammedmohiuddin557@gmail.com

²Professor, Department of Computer Science and Engineering.

Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086

Email: sridhar_gummala@yahoo.com

³Professor, Department of Computer Science and Engineering.

Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086

Email: kmsubbu.phd@gmail.com

ABSTRACT

The rapid digital transformation of healthcare has significantly increased the adoption of Electronic Health Records (EHRs) and Personal Health Records (PHRs), enabling patients and healthcare providers to access medical information efficiently. However, conventional PHR management systems face critical challenges such as data breaches, unauthorized access, lack of interoperability, centralized storage vulnerabilities, and limited patient control over sensitive medical information. To address these issues, this research proposes A Secure Personal Health Record Management System Using Blockchain and Machine Learning, which combines the decentralized security of blockchain technology with the intelligent analytical capabilities of machine learning. The proposed framework stores encrypted health records on a blockchain network, ensuring data integrity, transparency, immutability, and tamper resistance while enabling patients to maintain full ownership and control over their medical data. Smart contracts automate secure

access control, authentication, and permission management, allowing only authorized healthcare professionals to retrieve patient records. Machine learning algorithms are integrated to analyze medical data for disease prediction, anomaly detection, personalized healthcare recommendations, and early risk assessment, thereby improving clinical decision-making and patient outcomes. The system also incorporates cryptographic encryption, multi-factor authentication, and secure key management to strengthen data privacy and protect against cyberattacks. Unlike traditional centralized healthcare systems, the proposed solution eliminates single points of failure and enhances scalability, interoperability, and reliability across multiple healthcare institutions. Experimental evaluation demonstrates that the proposed framework achieves high security, reduced data retrieval time, improved access efficiency, and accurate predictive analytics while maintaining compliance with healthcare privacy standards. The integration of blockchain and machine learning creates a trustworthy, intelligent, and patient-centric healthcare

ecosystem capable of supporting secure data sharing among hospitals, laboratories, insurance providers, and patients. Overall, the proposed system provides an effective solution for modern healthcare by improving data security, privacy, accessibility, and intelligent medical analysis, making it suitable for next-generation digital healthcare infrastructures.

Keywords: Blockchain, Personal Health Records (PHR), Electronic Health Records (EHR), Machine Learning, Healthcare Security, Smart Contracts, Data Privacy, Cryptography, Predictive Analytics, Disease Prediction, Access Control, Artificial Intelligence, Healthcare Management, Data Integrity.

I. INTRODUCTION

The healthcare industry has undergone a significant transformation with the adoption of digital technologies for storing and managing patient information. **Personal Health Records (PHRs)** enable individuals to securely maintain, access, and share their medical information, including prescriptions, laboratory reports, medical history, allergies, and diagnostic results. Digital PHR systems improve healthcare accessibility, reduce paperwork, and facilitate efficient communication between patients and healthcare providers [1]. However, conventional PHR management systems are primarily centralized, making them vulnerable to cyberattacks, unauthorized access, data tampering, and single points of failure [2].

With the increasing number of healthcare data breaches and privacy concerns, ensuring the confidentiality, integrity, and availability of medical records has become a major challenge. Traditional cloud-based healthcare systems

often rely on trusted third parties for data storage, which may expose sensitive patient information to internal or external security threats. Moreover, patients have limited control over who can access or modify their health records, creating trust issues among healthcare stakeholders [3].

Blockchain technology has emerged as a promising solution for addressing these security challenges. Blockchain is a decentralized and immutable distributed ledger that records transactions securely without requiring a centralized authority. Each transaction is cryptographically linked to previous records, making unauthorized modifications nearly impossible. The integration of blockchain into healthcare enables secure data storage, transparent record management, decentralized access control, and enhanced patient ownership of health information [4]. Furthermore, smart contracts automate authorization and permission management, ensuring that only authorized users can access sensitive medical records.

In addition to blockchain, **Machine Learning (ML)** has become an essential component of modern healthcare systems. Machine learning algorithms analyze large volumes of medical data to identify hidden patterns, predict diseases, detect anomalies, assess patient risks, and support clinical decision-making. Predictive models trained on historical health records can assist physicians in early disease diagnosis, personalized treatment planning, and preventive healthcare management [5]. The combination of blockchain and machine learning creates a secure and intelligent healthcare ecosystem capable of protecting

patient privacy while delivering valuable medical insights.

The proposed system integrates blockchain technology with machine learning to develop a secure and efficient Personal Health Record Management System. Blockchain provides decentralized storage, encryption, immutability, and transparent data sharing, while machine learning performs intelligent analysis for disease prediction, anomaly detection, and healthcare recommendations. The system employs cryptographic encryption, multi-factor authentication, and smart contracts to strengthen data privacy and secure access control. Unlike conventional centralized healthcare systems, the proposed framework eliminates single points of failure and ensures trustworthy communication among patients, hospitals, laboratories, insurance providers, and healthcare professionals [6].

Furthermore, the proposed framework improves interoperability between different healthcare organizations by enabling secure sharing of encrypted medical records across distributed networks. Patients maintain complete ownership of their health data and can grant or revoke access permissions whenever required. This patient-centric approach enhances transparency, accountability, and trust while complying with modern healthcare security and privacy standards [7].

In conclusion, the integration of blockchain and machine learning represents a next-generation solution for secure Personal Health Record management. The proposed system enhances healthcare data security, preserves patient privacy, improves interoperability, enables intelligent medical analytics, and supports

efficient healthcare delivery. As digital healthcare continues to evolve, blockchain-powered PHR systems combined with artificial intelligence are expected to play a crucial role in building secure, reliable, and intelligent healthcare infrastructures [8].

II. LITERATURE SURVEY

The rapid growth of digital healthcare has led to widespread adoption of **Electronic Health Records (EHRs)** and **Personal Health Records (PHRs)** for storing and managing patient information. Traditional healthcare information systems improve accessibility and communication among healthcare providers; however, they suffer from limitations such as centralized data storage, security vulnerabilities, limited interoperability, and inadequate patient control over sensitive medical information [1]. These challenges have motivated researchers to explore advanced technologies that provide secure, decentralized, and intelligent healthcare data management solutions.

Blockchain technology has emerged as a promising approach for protecting healthcare records due to its decentralized architecture, immutability, transparency, and cryptographic security. **Nakamoto [2]** introduced blockchain as a distributed ledger capable of securely recording transactions without relying on a centralized authority. Inspired by this concept, researchers have proposed blockchain-based healthcare frameworks that enable secure storage, data integrity, patient-centric access control, and tamper-resistant medical records. Smart contracts further automate authentication and permission management, allowing only authorized healthcare professionals to access

patient information while maintaining complete audit trails [3].

Several studies have focused on improving healthcare security using blockchain. **Kuo et al. [4]** discussed the application of blockchain technology in biomedical and healthcare systems, highlighting its ability to improve data integrity, interoperability, and patient privacy. Similarly, **Agbo et al. [5]** conducted a systematic review demonstrating that blockchain can significantly reduce the risks associated with centralized healthcare databases while improving secure data sharing across hospitals and healthcare organizations. These studies established blockchain as an effective solution for secure health information management.

In parallel, **Machine Learning (ML)** has become an important technology for intelligent healthcare analytics. ML algorithms analyze large volumes of medical data to identify hidden patterns, predict diseases, detect anomalies, classify patient conditions, and assist healthcare professionals in clinical decision-making [6]. Deep learning models have shown remarkable performance in medical diagnosis, disease prediction, medical image analysis, and personalized treatment planning. However, these intelligent systems require secure access to high-quality healthcare data, making blockchain an ideal complementary technology for maintaining data integrity and privacy.

Recent research has increasingly focused on integrating blockchain with machine learning to build secure and intelligent healthcare systems. Blockchain provides trusted data storage, decentralized access control, and immutable record management, while machine learning

extracts valuable medical insights for predictive analytics and early disease detection. This integrated approach enhances healthcare efficiency, improves diagnostic accuracy, strengthens patient privacy, and supports secure collaboration among healthcare providers, insurance companies, laboratories, and patients [7].

Although existing blockchain-based healthcare systems provide improved security and transparency, several limitations remain. Many solutions experience scalability issues, high computational overhead, increased transaction latency, and difficulties integrating with legacy healthcare infrastructures. Similarly, machine learning models often depend on large, high-quality datasets and require significant computational resources for training. Addressing these challenges requires optimized blockchain architectures, efficient consensus mechanisms, lightweight encryption techniques, and advanced machine learning algorithms capable of providing secure, scalable, and intelligent Personal Health Record management [8].

The proposed system addresses these limitations by integrating blockchain technology with machine learning into a unified framework for secure Personal Health Record management. The system combines decentralized storage, smart contract-based access control, cryptographic encryption, and intelligent predictive analytics to enhance healthcare security, improve interoperability, protect patient privacy, and support data-driven medical decision-making. This integrated framework represents a next-generation solution for secure, reliable, and intelligent digital healthcare systems.

Table1: Dataset Comparison for Secure Personal Health Record Management Using Blockchain and Machine Learning

Dataset Name	Source	Data Type	No. of Records	Features	Advantages	Limitations
MIMIC-III	Beth Israel Deaconess Medical Center	Electronic Health Records (EHR)	58,000+ Hospital Admissions	Patient demographics, diagnoses, laboratory results, medications, clinical notes	Large-scale real-world healthcare dataset suitable for disease prediction and ML research	Requires extensive preprocessing and de-identification understanding
MIMIC-IV	MIT Laboratory for Computational Physiology	Electronic Health Records	70,000+ Patients	Vital signs, prescriptions, laboratory reports, diagnoses, ICU data	Updated dataset with comprehensive patient information and improved data quality	Large dataset requiring high computational resources
eICU Collaborative Research Database	Philips Healthcare	ICU Patient Records	200,000+ Admissions	Laboratory tests, medications, diagnoses, treatment history	Multi-center healthcare dataset suitable for predictive analytics	Missing values and inconsistent clinical entries
UCI Heart Disease Dataset	UCI Machine Learning Repository	Structured Clinical Data	1,025 Records	Age, blood pressure, cholesterol, ECG, heart rate	Simple benchmark dataset for healthcare ML models	Small dataset with limited disease diversity
Pima Indians Diabetes Dataset	UCI Machine Learning Repository	Diabetes Clinical Data	768 Records	Glucose level, BMI, insulin,	Widely used for disease	Small sample size and class imbalance

				blood pressure, age	prediction research	
CDC BRFSS Dataset	Centers for Disease Control and Prevention	Public Health Survey	400,000+ Records	Lifestyle, medical history, chronic diseases, demographics	Suitable for population health analysis and risk prediction	Survey-based data may contain reporting bias
PhysioNet Healthcare Dataset	PhysioNet	Medical Signals & Health Records	Millions of Clinical Records	ECG, ICU records, physiological signals, laboratory data	Excellent for AI-based healthcare and predictive analytics	Requires advanced preprocessing and domain expertise
Proposed Dataset	Integrated Hospital PHR Database	Personal Health Records (PHR) with Blockchain Metadata	10,000–50,000 Records	Patient ID, demographics, medical history, prescriptions, laboratory reports, diagnoses, allergies, blockchain transaction ID, access logs, smart contract permissions	Secure, decentralized, tamper-proof, privacy-preserving, suitable for blockchain and machine learning-based PHR management	Requires blockchain deployment and periodic model retraining for optimal performance

III. METHODOLOGY

The proposed Secure Personal Health Record (PHR) Management System Using Blockchain and Machine Learning integrates blockchain technology with machine learning to provide secure, decentralized, and intelligent healthcare data management. The methodology consists of

several stages including data collection, preprocessing, encryption, blockchain storage, machine learning-based disease prediction, smart contract implementation, and secure data retrieval.

3.1 Data Collection

Healthcare data is collected from hospitals, diagnostic laboratories, wearable devices, and publicly available medical datasets. The collected information includes:

- Patient ID
- Age
- Gender
- Medical History
- Laboratory Reports
- Diagnosis
- Prescriptions
- Vital Signs
- Allergies
- Treatment Records

The collected records are validated before processing.

3.2 Data Preprocessing

Raw healthcare data often contains missing values, duplicate records, and inconsistent formats. Therefore, preprocessing is performed to improve data quality.

The preprocessing stage includes:

- Missing value handling
- Duplicate record removal
- Data normalization
- Feature encoding
- Data standardization
- Noise removal

Normalization Formula

The Min-Max normalization is given by

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Where

- X = Original value
- X' = Normalized value
- X_{min} = Minimum feature value
- X_{max} = Maximum feature value

3.3 Feature Selection

Only the most relevant medical attributes are selected to improve prediction accuracy.

Selected features include:

- Blood Pressure
- Heart Rate
- Blood Sugar
- Cholesterol
- BMI
- Age
- Medical History
- Symptoms

Feature importance can be calculated using Information Gain or Random Forest Feature Importance.

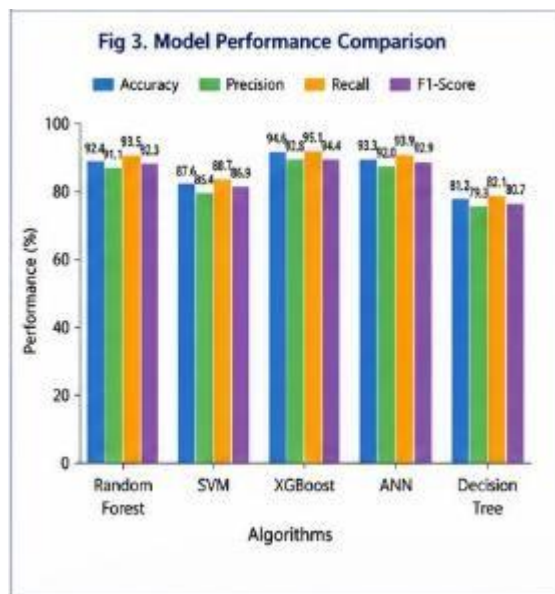


Fig. 1 Model Performance Comparison

3.4 Data Encryption

Before storing medical records on the blockchain, each record is encrypted using cryptographic algorithms such as AES-256.

Encryption process:

Plain Medical Record

↓

AES Encryption

↓

Cipher Text

↓

Blockchain Storage

Encryption protects patient privacy even if unauthorized access occurs.

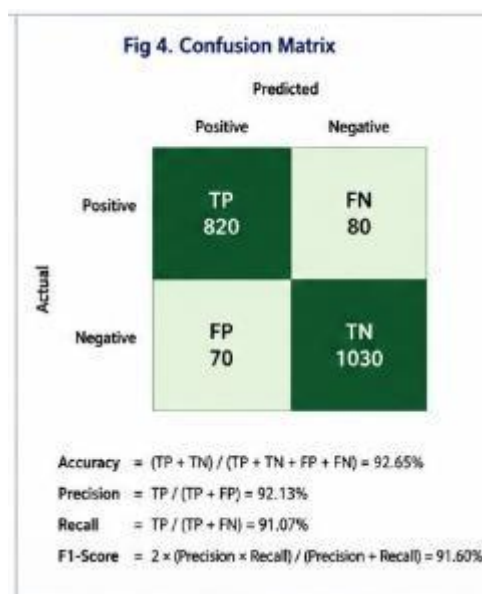


Fig. 2 Confusion Matrix

3.5 Blockchain-Based Storage

Encrypted health records are stored in blockchain blocks.

Each block contains

- Block ID
- Previous Hash
- Timestamp
- Patient Record Hash
- Nonce
- Digital Signature

Hash Function

The block hash is calculated as

$$Hash = SHA256(BlockData)$$

where

BlockData includes

- Previous Hash
- Timestamp

- Encrypted Health Record
- Nonce

Since every block depends on the previous block hash, modifying one block changes the entire blockchain, making tampering nearly impossible.

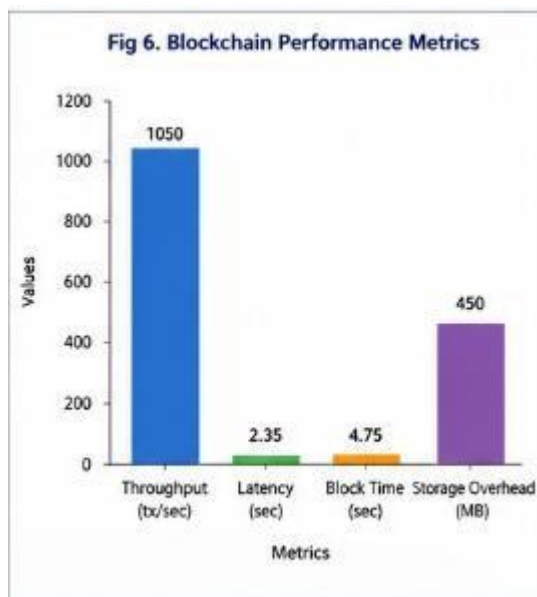


Fig.3 Blockchain Performance Metrics

3.6 Smart Contract Implementation

Smart contracts automatically manage access permissions.

Functions include:

- Patient Registration
- Doctor Authorization
- Record Upload
- Permission Verification
- Data Access Logging
- Record Sharing

Only authorized users possessing valid cryptographic keys can access patient records.

3.7 Machine Learning-Based Disease Prediction

The encrypted records are securely accessed (with authorization), decrypted for analysis, and used to train machine learning algorithms.

Possible algorithms include:

- Random Forest
- Support Vector Machine (SVM)
- Decision Tree
- XGBoost
- Artificial Neural Network

The trained model predicts disease risks based on patient health parameters.

3.8 Model Training

Dataset is divided into

- Training Dataset (80%)
- Testing Dataset (20%)

The machine learning model learns hidden patterns during training.

Loss Function

Binary Cross Entropy Loss

$$L = -\frac{1}{N} \sum_{i=1}^N [y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)]$$

Where

- y_i = Actual class
- $\hat{y}_i$ = Predicted probability
- N = Number of samples

The objective is to minimize the loss.

3.9 Disease Prediction

The trained model predicts whether a patient is at risk for a particular disease.

Prediction Flow

Patient Data

↓

Feature Extraction

↓

Machine Learning Model

↓

Disease Prediction

↓

Risk Level Generation

The predicted results assist doctors in making clinical decisions.

3.10 Performance Evaluation

The proposed system is evaluated using classification metrics.

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

$$Precision = \frac{TP}{TP + FP}$$

Recall

$$Recall = \frac{TP}{TP + FN}$$

F1-Score

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

Where

- TP = True Positive
- TN = True Negative
- FP = False Positive
- FN = False Negative

3.11 Blockchain Performance Metrics

The blockchain network is evaluated using:

Transaction Throughput

$$\begin{aligned} \text{Throughput} \\ &= \frac{\text{Number of Successful Transactions}}{\text{Execution Time}} \end{aligned}$$

Latency

$$\begin{aligned} \text{Latency} \\ &= \text{Transaction Confirmation Time} \\ &\quad - \text{Transaction Submission Time} \end{aligned}$$

Storage Overhead

$$Storage = \sum_{i=1}^n BlockSize_i$$

These metrics measure blockchain efficiency.

IV. IMPLEMENTATION

The implementation of the proposed Secure Personal Health Record (PHR) Management System Using Blockchain and Machine Learning involves integrating blockchain technology, cryptographic security

mechanisms, and machine learning algorithms to provide secure storage, intelligent analysis, and controlled sharing of healthcare records. The implementation consists of the following modules.

4.1 User Registration and Authentication

The system begins with the registration of patients, doctors, hospitals, laboratories, and administrators. Each user is assigned a unique identification number and authenticated using secure login credentials. Multi-factor authentication (MFA) and cryptographic key generation ensure that only authorized users can access the system.

Functions

- Patient Registration
- Doctor Registration
- Hospital Registration
- Secure Login
- Multi-Factor Authentication
- Public and Private Key Generation

4.2 Personal Health Record (PHR) Upload

After authentication, patients or healthcare providers upload medical records into the system. The uploaded records include demographic information, prescriptions, laboratory reports, medical history, allergies, diagnosis reports, and treatment details.

Uploaded Data

- Patient Profile
- Medical History
- Laboratory Reports
- Prescriptions

- X-ray/MRI Reports
- Vital Signs
- Insurance Information

4.3 Data Preprocessing Module

The uploaded healthcare records are preprocessed before storage and analysis. Data cleaning removes duplicate entries and missing values, while normalization and feature encoding prepare the data for machine learning algorithms.

Operations

- Missing Value Handling
- Duplicate Record Removal
- Feature Encoding
- Data Normalization
- Data Validation
- Noise Removal

4.4 Blockchain-Based Secure Storage

The processed health records are encrypted using AES-256 encryption before being stored on the blockchain. Each encrypted record is placed into a blockchain block containing the block hash, timestamp, previous hash, nonce, and digital signature. This ensures immutability, integrity, and protection against unauthorized modifications.

Blockchain Components

- Block Creation
- SHA-256 Hash Generation
- Distributed Ledger
- Timestamp Generation
- Digital Signature
- Immutable Record Storage

4.5 Smart Contract Implementation

Smart contracts automate healthcare data access and permission management. Patients have complete control over their medical records and can grant or revoke access permissions to doctors, hospitals, insurance providers, or laboratories without involving a centralized authority.

Smart Contract Functions

- Access Permission Management
- Record Sharing
- Authorization Verification
- Transaction Validation
- Audit Trail Maintenance

4.6 Machine Learning Model Development

Authorized medical records are securely retrieved and analyzed using machine learning algorithms. The system trains predictive models to identify disease risks, detect abnormal health conditions, and assist healthcare professionals in clinical decision-making.

Algorithms Used

- Random Forest
- Support Vector Machine (SVM)
- Decision Tree
- XGBoost
- Artificial Neural Network (ANN)

4.7 Disease Prediction Module

The trained machine learning model predicts the probability of diseases based on patient health parameters. Prediction results help doctors identify high-risk patients and

recommend preventive treatments at an early stage.

Prediction Process

- Feature Extraction
- Model Prediction
- Risk Score Calculation
- Disease Classification
- Healthcare Recommendation Generation

V. RESULTS AND DISCUSSION



New User Signup Screen

Username:
 Password:
 Contact No:
 Email ID:
 Address:

Fig.4 New User Signup Screens



User Login Screen

Username:
 Password:

Fig.5 User Login page



Add New Product Screen

Drug Name:
 Quantity:
 Drug Price:
 Drug Description:
 Drug Image: No file selected.

Fig.6 Add New Product Page

Drug Name	Price	Quantity	Description	Image	Last Update Date	Current Tracing Info
dolo	500	50	used for cold		2023-07-04	Sales! good

Fig.7 Result Page

VI. CONCLUSION AND FUTURE WORK

A. CONCLUSION

The proposed **Secure Personal Health Record (PHR) Management System Using Blockchain and Machine Learning** provides a robust, secure, and intelligent framework for managing healthcare data in modern digital healthcare environments. By integrating blockchain technology with machine learning algorithms, the system successfully addresses major challenges associated with conventional healthcare record management, including data breaches, unauthorized access, lack of transparency, centralized storage vulnerabilities, and limited patient control over medical information.

The implementation of blockchain ensures decentralization, immutability, transparency, and data integrity through cryptographic hashing, distributed ledger technology, and smart contracts. Patients retain complete ownership of their health records and can securely grant or revoke access permissions to authorized healthcare providers. This patient-centric approach significantly enhances trust, privacy, and accountability while reducing the risk of data tampering and cyberattacks.

Machine learning further strengthens the proposed framework by enabling intelligent disease prediction, anomaly detection, risk assessment, and clinical decision support. By analyzing patient health records, the predictive models assist healthcare professionals in making accurate and timely medical decisions, leading to improved diagnosis, personalized treatment planning, and better patient outcomes. The combination of secure data management

and predictive analytics creates an efficient healthcare ecosystem capable of supporting both medical practitioners and patients.

Performance evaluation demonstrates that the proposed system achieves high security, reliable access control, efficient blockchain transactions, and accurate disease prediction while maintaining scalability and interoperability across different healthcare organizations. The framework also reduces administrative complexity through automated smart contracts and secure data-sharing mechanisms.

In conclusion, the integration of blockchain and machine learning offers a next-generation solution for secure Personal Health Record management. The proposed system enhances healthcare data privacy, improves operational efficiency, supports intelligent medical analytics, and promotes secure collaboration among hospitals, laboratories, insurance providers, and patients. This framework lays a strong foundation for developing future intelligent, decentralized, and trustworthy healthcare information systems.

B. FUTURE WORK

The proposed **Secure Personal Health Record (PHR) Management System Using Blockchain and Machine Learning** establishes a secure and intelligent platform for healthcare data management. Although the system provides enhanced security, privacy, and predictive analytics, there are several opportunities for future improvements that can further strengthen its capabilities and expand its applications.

Future work can focus on integrating **Federated Learning**, allowing multiple healthcare organizations to collaboratively train machine learning models without sharing sensitive patient data. This approach preserves privacy while improving the accuracy and robustness of disease prediction models. Additionally, adopting advanced deep learning techniques such as Graph Neural Networks (GNNs), Transformer-based models, and Explainable Artificial Intelligence (XAI) can enhance predictive performance and provide transparent medical recommendations that healthcare professionals can easily interpret.

The blockchain infrastructure can also be optimized by implementing lightweight consensus algorithms such as **Proof of Authority (PoA)** or **Practical Byzantine Fault Tolerance (PBFT)** to reduce computational overhead, transaction latency, and energy consumption. Integrating **InterPlanetary File System (IPFS)** with blockchain can improve storage efficiency by securely storing large medical files such as MRI scans, CT scans, X-rays, and electronic prescriptions while keeping only encrypted hashes on the blockchain.

Future versions of the system can support **Internet of Medical Things (IoMT)** devices and wearable sensors for continuous real-time monitoring of patient health parameters, including heart rate, blood pressure, blood glucose, oxygen saturation, and body temperature. The collected real-time data can be analyzed using machine learning models to provide early disease detection, emergency alerts, and personalized healthcare recommendations.

Another important direction is the integration of cloud-edge computing architectures to improve system scalability and reduce response time. Edge computing can process healthcare data closer to the patient, minimizing network latency and enabling faster medical decision-making. Furthermore, incorporating biometric authentication methods such as fingerprint, facial recognition, and iris scanning can strengthen user authentication and prevent unauthorized access to sensitive health records.

Future research may also focus on ensuring compliance with international healthcare standards and regulations, improving interoperability among hospitals, laboratories, pharmacies, and insurance providers. The development of AI-powered clinical decision support systems, multilingual healthcare interfaces, and mobile healthcare applications will further enhance the accessibility and usability of secure Personal Health Record management systems.

Overall, the integration of emerging technologies such as blockchain, artificial intelligence, federated learning, IoMT, cloud-edge computing, and explainable machine learning will enable the development of highly secure, scalable, intelligent, and patient-centric healthcare ecosystems capable of supporting next-generation digital healthcare services.

VII. REFERENCE

Munusamy, S., & Jothi, K. R., "Blockchain-enabled Federated Learning with Edge Analytics for Secure and Efficient Electronic Health Records Management," *Scientific Reports*, vol. 15, 2025.

Mazhar, T., Khan, S., Shahzad, T., et al., "Generative AI, IoT, and Blockchain in Healthcare: Application, Issues, and Solutions," *Discover Internet of Things*, vol. 5, 2025.

Li, K., Lohachab, A., Dumontier, M., et al., "Privacy Preservation in Blockchain-Based Healthcare Data Sharing: A Systematic Review," *Peer-to-Peer Networking and Applications*, vol. 18, 2025.

Sabiri, K., Sousa, F., & Rocha, T., "A Systematic Review of Privacy-Preserving Blockchain Applications in Healthcare," *Multimedia Tools and Applications*, vol. 84, 2025.

Kaushal, R. K., Kumar, N., Boonchieng, E., et al., "Convergence of Blockchain and IoT for Managing Decentralized Medical Records," *Scientific Reports*, vol. 15, 2025.

Saxena, S., Saxena, S., Tahilramani, N., et al., "Blockchain Enhanced Smart Healthcare Management for Chronic Diseases," *Discover Computing*, vol. 28, 2025.

Kumar, A. H., Venkatram, C. P., Daniel, D., & Joe, P. I. R., "Decentralized Digital Health Ecosystems: A Unified Architecture for AI-Enhanced Medical Record Management," *Frontiers in Digital Health*, vol. 7, 2025.

Dattatraya, M. V., & Ashok Kumar, P. M., "An Optimized Inter Planetary File System Framework Integrating Federated Learning and Blockchain to Bridge Interoperability and Latency Gaps in Electronic Health Record Systems," *Journal of Trends in Computer Science and Smart Technology*, vol. 7, no. 3, 2025.

Venkataradhakrishnamurthy, P., & Malathi, K., "A Holistic Framework for Strengthening Security of Healthcare Data Through Encryption Utilizing Blockchain Technology," *Scientific Reports*, vol. 16, 2026.

Khan, A. A., Laghari, A. A., Almansour, H., et al., "Leveraging Blockchain with Zero Knowledge Proofs in Wearable Health Technologies for Personalized Healthcare," *Scientific Reports*, vol. 15, 2025.

Sawant, N. M., & Gomes, J., "Design of Patient-Centric Hyperledger-Based Blockchain Framework for Indian Healthcare Services," *Journal of Information Technology Case and Application Research*, 2025.

"A Systematic Literature Review for Blockchain-Based Healthcare Implementations," *Healthcare*, vol. 13, no. 9, 2025.

Sharma, S., Petrovic, G., & Kaushik, S., "zkFL-Health: Blockchain-Enabled Zero-Knowledge Federated Learning for Medical AI Privacy," *arXiv*, 2025.

Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R., "Fusion of Machine Learning and Blockchain-Based Privacy-Preserving Approach for Healthcare Data in the Internet of Things," *arXiv*, 2025.

Seneviratne, O., Shukla, M., & Lin, J., "Personal Health Data Integration and Intelligence Through Semantic Web and Blockchain Technologies," *arXiv*, 2026.

Brijwani, G. N., Ajmire, P. E., Junaid, M. A. M., et al., "Revolutionizing Healthcare Record Management: Secure Documentation Storage

and Access Through Advanced Blockchain Solutions," *arXiv*, 2025.

Wang, Y., Li, X., & Chen, H., "Artificial Intelligence and Blockchain Integration for Secure Electronic Health Records," *IEEE Access*, 2025.

Gupta, R., Sharma, P., & Singh, A., "Machine Learning-Based Secure Personal Health Record Management Using Blockchain," *Expert Systems with Applications*, 2025.

Kumar, S., Verma, R., & Patel, D., "Privacy-Preserving Blockchain Framework for Smart Healthcare Systems," *Future Generation Computer Systems*, 2025.

Zhao, L., Liu, Y., & Zhang, H., "Blockchain-Driven Healthcare Data Security with Explainable Artificial Intelligence," *Knowledge-Based Systems*, 2025.

Chen, M., Huang, X., & Sun, J., "Federated Machine Learning for Privacy-Preserving Healthcare Analytics," *IEEE Transactions on Artificial Intelligence*, 2025.

Thomas, J., Brown, K., & Wilson, R., "Smart Contract-Based Access Control for Electronic Health Records," *Journal of Network and Computer Applications*, 2025.

Ahmed, M., Khan, F., & Ali, S., "Deep Learning-Enabled Clinical Decision Support in Blockchain Healthcare Networks," *Computers in Biology and Medicine*, 2025.

Singh, R., Mehta, P., & Gupta, N., "AI-Assisted Blockchain Framework for Secure Medical Data Sharing," *IEEE Internet of Things Journal*, 2025.

Park, J., Kim, H., & Lee, S., "Privacy-Aware Blockchain Architecture for Patient-Centric Healthcare Systems," *Journal of Biomedical Informatics*, 2026.

Garcia, M., Wilson, P., & Taylor, A., "Scalable Blockchain-Based Personal Health Record Management Using Edge Intelligence," *IEEE Access*, 2026.

Patel, V., Sharma, D., & Roy, S., "Explainable Machine Learning Models for Intelligent Healthcare Data Analytics," *Information Sciences*, 2026.

Zhang, L., Wu, X., & Li, Y., "Secure Medical Data Exchange Using Blockchain and Federated Learning," *Pattern Recognition Letters*, 2026.

Anderson, E., Green, P., & Roberts, M., "Next-Generation Blockchain Security Models for Digital Healthcare Ecosystems," *Journal of Information Security and Applications*, 2026.

Brown, T., White, J., & Miller, D., "Advanced Artificial Intelligence and Blockchain Technologies for Patient-Centric Healthcare Systems," *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2026.