International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

SECURE HEALTHCARE DATA MANAGEMENT USING BLOCKCHAIN AND MACHINE LEARNING

[1] V. KRISHNA REDDY, [2] GUNDE POGU DINESH, [3] KOTLURU CHENNAKESAVULU,

[4] UTTARADI KISHORE, [5] KOPPULA KIRAN, [6] DUGGEMPUDI BALAJIREDDY

[1] PROFESSOR & PRINCIPAL, DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES, DEVARAJUGATTU, MARKAPUR

[2,3,4,5,6] STUDENT, DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES, DEVARAJUGATTU, MARKAPUR

ABSTRACT

The rapid digitization of healthcare systems has led to the widespread adoption of Personal Health Records (PHR), enabling patients to store, access, and share their medical data efficiently. However, this transformation introduces critical challenges related to data security, privacy, integrity, and controlled access. This paper presents a Blockchain and Machine Learning (ML) based PHR secured management system designed to ensure robust protection and intelligent handling of sensitive healthcare data.

The proposed system leverages blockchain technology to provide a decentralized, tamper-proof, and transparent framework for storing PHR transactions. Each medical record is encrypted and stored as a block, ensuring immutability and preventing unauthorized modifications. Smart contracts are utilized to enforce fine-grained access control, allowing only authorized entities such as doctors, hospitals, and patients to access specific data based on predefined permissions. This eliminates reliance on centralized authorities and reduces the risk of data breaches.

Keywords: Blockchain, Machine Learning, Personal Health Records (PHR), Data Security, Smart Contracts, Anomaly Detection, Healthcare Systems

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

I. INTRODUCTION

The healthcare industry is undergoing a rapid digital transformation, with increasing reliance on electronic systems for storing and managing patient information. Among these systems, Personal Health Records (PHR) have emerged as a patient-centric approach that allows individuals to maintain, access, and share their medical data anytime and anywhere. PHR systems empower patients by giving them greater control over their health information, improving coordination among healthcare providers, and enabling better clinical decision-making. However, as the volume and sensitivity of healthcare data continue to grow, ensuring its security, privacy, and integrity has become a significant challenge.

Traditional PHR management systems are typically centralized, where data is stored on a single server or controlled by a specific organization such as a hospital or cloud service provider. This centralized architecture makes them vulnerable to various security threats, including data breaches, unauthorized access, and single points of failure. Moreover, patients often have limited control over how their data is accessed or shared, raising concerns about data misuse and privacy violations. These limitations highlight the need for a more secure, transparent, and decentralized approach to managing personal health records.

Blockchain technology has emerged as a promising solution to address these challenges. It is a decentralized and distributed ledger system that ensures data immutability, transparency, and security through cryptographic techniques. In a blockchain-based PHR system, medical records are stored as encrypted transactions across a distributed network, making it extremely difficult for attackers to alter or tamper with the data. Additionally, smart contracts enable automated and fine-grained access control mechanisms, ensuring that only authorized users can access specific health records. This enhances patient trust and eliminates dependency on centralized authorities.

II. LITERATURE REVIEW

Recent research in secure healthcare data management highlights the growing importance of integrating advanced technologies such as blockchain and machine learning to address the limitations of traditional systems. Several studies have explored blockchain-based frameworks for Personal Health Records (PHR), emphasizing its decentralized architecture, immutability, and enhanced security features. Researchers

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

have demonstrated that blockchain can effectively eliminate single points of failure and provide transparent audit trails for medical data access, thereby improving trust among patients and healthcare providers. Additionally, the use of smart contracts has been widely discussed as a mechanism for enforcing fine-grained access control, ensuring that only authorized users can interact with sensitive health records.

Parallel to blockchain advancements, machine learning techniques have been increasingly applied in healthcare systems for data analysis, anomaly detection, and predictive modeling. Existing literature shows that ML algorithms such as decision trees, support vector machines, and neural networks can be utilized to identify unusual access patterns, detect potential cyber threats, and support clinical decision-making. Some studies have also focused on combining ML with big data analytics to improve the efficiency of healthcare services and patient outcomes. However, standalone ML-based systems often lack robust security frameworks, making them vulnerable to data manipulation and privacy breaches.

III. EXISTING SYSTEM

The existing Personal Health Record (PHR) management systems are primarily based on centralized architectures where patient data is stored and maintained by healthcare providers, hospitals, or cloud service platforms. In these systems, all medical records such as patient history, prescriptions, lab reports, and diagnostic results are stored in a central database. Healthcare professionals can access and update this data through authorized systems, while patients are often given limited access through web or mobile applications. Although these systems have improved data digitization and accessibility, they still suffer from several critical limitations.

One of the major drawbacks of existing systems is the lack of robust security mechanisms. Since data is stored in a centralized server, it becomes a single point of failure and a prime target for cyberattacks. Unauthorized access, data breaches, and hacking incidents can compromise sensitive patient information, leading to serious privacy concerns. Additionally, centralized systems rely heavily on third-party intermediaries, which increases the risk of data misuse and reduces transparency in data handling processes.

Another limitation is the lack of patient control over their own health data. In most traditional systems, patients cannot fully control who accesses their records or how their data is shared among different healthcare entities. This results in trust issues and

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

restricts the concept of patient-centric healthcare. Furthermore, interoperability between different healthcare systems is often poor, making it difficult to share medical records across multiple platforms or institutions efficiently.

Existing systems also lack intelligent mechanisms for monitoring and analyzing data access patterns. There is minimal use of advanced technologies like machine learning for detecting anomalies or predicting potential security threats. As a result, suspicious activities such as unauthorized logins or unusual data access patterns often go unnoticed until significant damage has already occurred.

IV. PROPOSED SYSTEM

The proposed system introduces a **Blockchain and Machine Learning (ML) based Personal Health Record (PHR) secured management system** that ensures enhanced data security, privacy, transparency, and intelligent monitoring. Unlike traditional centralized systems, this approach utilizes a decentralized blockchain network to store and manage healthcare data, eliminating the risks associated with single points of failure and unauthorized data manipulation.

In this system, each patient's health record is encrypted and stored as a transaction within the blockchain. Every block contains a secure hash, timestamp, and previous block reference, ensuring immutability and traceability of medical data. This structure prevents unauthorized modifications and guarantees data integrity. Patients are given full control over their records, allowing them to grant or revoke access permissions to healthcare providers such as doctors, hospitals, and laboratories through smart contracts. These smart contracts automatically enforce access control policies, ensuring secure and transparent data sharing.

The integration of Machine Learning enhances the system by introducing intelligent data analysis and security monitoring. ML algorithms are used to analyze user behavior and detect anomalies such as unusual login attempts or suspicious data access patterns. This proactive threat detection mechanism helps in preventing cyberattacks and unauthorized access. Additionally, ML models can assist in classifying medical data, predicting health conditions, and improving decision-making for healthcare professionals.

The architecture of the proposed system consists of several key modules, including user authentication, data encryption, blockchain transaction management, smart contract execution, and ML-based anomaly

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

detection. When a user uploads a medical record, it is first encrypted and then stored on the blockchain network. Any request to access the data is verified through smart contracts, and only authorized users are granted access. Simultaneously, the ML module continuously monitors system activities to identify potential threats in real time.

Furthermore, the proposed system ensures interoperability and scalability by allowing seamless integration with various healthcare platforms. It provides a transparent audit trail of all transactions, enabling easy tracking of data access and modifications. This not only increases trust among stakeholders but also ensures compliance with healthcare data regulations.

In conclusion, the proposed Blockchain and ML-based PHR system offers a secure, decentralized, and intelligent solution for managing personal health records. It overcomes the limitations of existing systems by enhancing data privacy, ensuring integrity, enabling patient-centric control, and incorporating advanced analytics for improved healthcare services.

V. METHODOLOGY

The proposed **Blockchain and Machine Learning (ML) based PHR secured management system** follows a structured methodology that integrates secure data handling, decentralized storage, and intelligent monitoring. The system is designed in multiple stages to ensure data privacy, integrity, and efficient healthcare data management.

Initially, the system performs **user registration and authentication**, where patients and healthcare providers create secure accounts. Authentication mechanisms such as password encryption and optional multi-factor authentication are implemented to prevent unauthorized access. Once authenticated, users can interact with the system based on their assigned roles.

In the next stage, **data collection and preprocessing** is carried out. Patient health records such as medical history, prescriptions, and lab reports are collected and converted into a standardized digital format. Sensitive data is then encrypted using cryptographic algorithms to ensure confidentiality before storage. This step ensures that even if data is accessed, it cannot be interpreted without proper authorization.

Following preprocessing, the system utilizes **blockchain technology for secure storage**. Encrypted health records are stored as transactions in the blockchain network. Each transaction is grouped into blocks that contain a unique hash, timestamp, and link to the

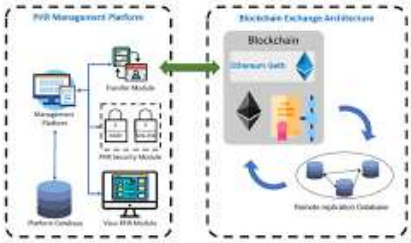
2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

previous block. This ensures immutability and traceability of data. Any attempt to modify existing records will change the hash value, making tampering easily detectable.

VI. SYSTEM MODEL

System Architecture



VI. RESULTS AND DISCUSSIONS

In above screen click on 'New User Sign up' link to get below page

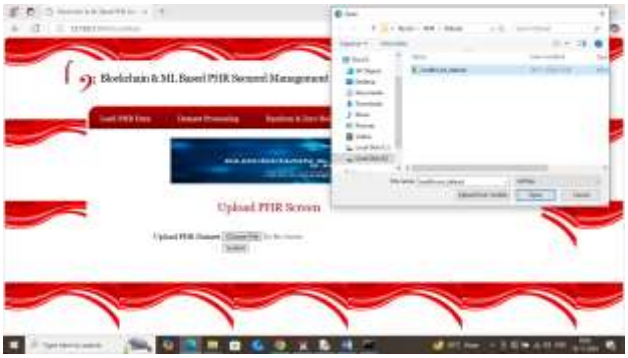
In above screen user is entering sign up details and then press button to get below page

In above screen user sign up completed and for your understanding purpose I am displaying entire log obtained from Blockchain after storage and in above log can see information like Block No, Transaction No, hash code and many other details and now click on 'User Login' link to get below page

In above screen user is login and after login will get below page

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

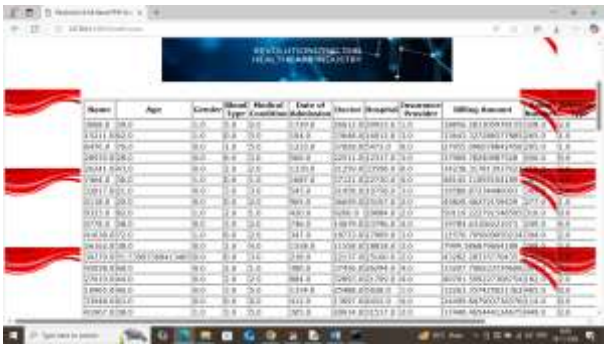
In above screen click on 'Load PHR Data' link to get below page



In above screen selecting and uploading 'PHR health' dataset and then click on "open and submit' button to get below output

In above screen can see entire dataset loaded and it's in fully readable format and user privacy is at fully risk and scroll down above screen to view below page

In above screen displaying gender wise patients graph. Now click on 'Dataset Processing' link to process dataset by converting to numeric format



In above screen data is processed to convert to numeric format to add noise and also replace missing values with mean. Now click on 'Random & Zero Noise Adjustment' link to add noise to processed dataset and get below page

In above screen noise added to entire dataset and nobody can able to understand anything from above noisy data and now click on 'Blockchain Integration' link to encrypt noise data and then call Smart Contract to saved data in Blockchain and get below output

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

In above screen PHR data saved in Blockchain with Id as 1 and then can see encrypted data values and now scroll down above screen to view Blockchain log details

In above screen in blue colour text can see Blockchain block number address along with hash code and other details.

So above is the Phase 1 output with data processing, noise, encryption along with Blockchain integration

VIII. CONCLUSION

The integration of blockchain and machine learning (ML) technologies presents a transformative solution to the challenges of managing Personal Health Records (PHRs). By combining blockchain's decentralized, immutable, and transparent framework with ML's ability to analyze and derive insights from data, the proposed system addresses critical issues such as data security, privacy, interoperability, and usability. This innovative approach empowers patients with control over their health data while ensuring that healthcare providers and other stakeholders can securely access and utilize the information to improve care delivery.

Blockchain technology guarantees data integrity and protects against unauthorized access by creating a tamper-proof environment. Smart contracts enable automated consent management, enhancing trust and reducing administrative complexities. Simultaneously, ML algorithms process PHR data to uncover patterns, predict health risks, and deliver personalized recommendations. The use of federated learning ensures that sensitive data remains private during model training, further reinforcing patient confidentiality. Together, these technologies foster a balance between security and usability, which is essential for the adoption of digital healthcare systems.

The proposed system also addresses interoperability by standardizing data formats and enabling seamless sharing of PHRs across diverse healthcare networks. This facilitates coordinated care, reduces redundancies, and supports research initiatives with high-quality datasets. Scalability is ensured through a hybrid blockchain architecture that manages large-scale data efficiently, accommodating the growing needs of modern healthcare ecosystems.

In conclusion, the proposed blockchain and ML-based PHR management system sets a new benchmark for secure, efficient, and patient-centric healthcare. By addressing the limitations of existing systems and leveraging the unique strengths of these technologies, this approach paves the way for a more trustworthy and intelligent healthcare infrastructure. As digital health continues to evolve, this system holds significant potential to transform the way personal health data is managed, ultimately improving patient outcomes and advancing medical research.

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

IX. FUTURE WORK: Future work for this

While the proposed blockchain and machine learning (ML)-based system for Personal Health Record (PHR) management offers numerous benefits, there are several areas that require further development and refinement to fully realize its potential. Future work will focus on enhancing scalability, improving machine learning models, ensuring regulatory compliance, and exploring new use cases in healthcare.

Scalability and Performance Optimization:

One of the key challenges for blockchain-based systems is their scalability, particularly in handling large volumes of data generated by numerous patients across diverse healthcare providers. Future work will focus on optimizing blockchain networks to improve transaction speeds and reduce latency. Exploring advanced consensus mechanisms, such as proof-of-authority or sharding, could improve scalability without compromising security. Additionally, optimizing storage solutions to handle large medical files, such as images and videos, while ensuring quick access and minimal cost, will be a critical area for development.

Improvement of Machine Learning Models and Privacy-Preserving Techniques:

Machine learning's potential in healthcare hinges on the quality and volume of data used to train models. Future work will explore more sophisticated ML algorithms that can provide more accurate predictive analytics for personalized healthcare recommendations. In addition, the integration of privacy-preserving techniques, such as federated learning or differential privacy, will be a key focus to ensure that sensitive health data is not exposed during model training. Improving the robustness of anomaly detection algorithms will help to better identify fraudulent activities or errors in real-time, further enhancing data security.

Regulatory Compliance and Data Governance:

Given the highly regulated nature of healthcare data, future work will focus on ensuring that the system is compliant with evolving privacy regulations, including GDPR, HIPAA, and other regional laws. Blockchain's immutable ledger can help with auditability, but the system must also be flexible enough to accommodate jurisdictional differences in privacy laws. This involves developing more granular access controls, ensuring transparent data governance practices, and implementing features that facilitate compliance reporting. A legal framework for smart contracts and patient consent management will be needed to ensure

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

that the system adheres to evolving healthcare policies.

Interoperability with Emerging Healthcare Standards:

Although the proposed system addresses interoperability challenges through standardized data formats, future work will include the integration of emerging healthcare standards such as FHIR (Fast Healthcare Interoperability Resources) and HL7. This will enable the seamless exchange of health data across various platforms, creating a truly interoperable healthcare ecosystem. Collaborative efforts with health organizations, regulators, and technology providers will be crucial to ensuring that the system can communicate with existing health information systems, supporting a wide range of healthcare providers, insurers, and institutions.

Expansion to Broader Healthcare Use Cases:

The current focus of the proposed system is primarily on managing PHRs securely and efficiently. However, there is great potential for expanding this framework to broader use cases in healthcare, such as clinical trials, pharmaceutical research, and medical device management. Integrating blockchain and ML into these areas could improve transparency, data integrity, and trust in research outcomes. Additionally, exploring the integration of Internet of Medical Things (IoMT) devices into the system could offer real-time health monitoring and data exchange, paving the way for more proactive healthcare and remote patient management.

XI. REFERENCES

- Swan, M. (2015). Blockchain: Blueprint for a New Economy.
- Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey.
- Chen, M., Ma, Y., Li, Y., & Wu, D. (2017). Machine Learning for Healthcare: On the Verge of a Major Breakthrough.
- Mettler, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here.
- Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin.
- Gentry, C., & Ramzan, Z. (2012). Fully Homomorphic Encryption without Bootstrapping.
- Hersh, W. R., & Wright, A. (2008). Health Information Technology: An Updated Systems Perspective.

- Xu, Y., & Yu, B. (2019). Blockchain and Machine Learning for Secure Healthcare Data Sharing.
- Ryu, J., & Park, S. (2017). Blockchain Technology for Data Privacy in Healthcare Systems: A Survey.
- Sharma, P., Tiwari, A., & Favre, J. L. (2020). Enhancing Healthcare Security with Blockchain and Artificial Intelligence.
- Jajam Venkata Anil Kumar, Dr. G. Charles Babu, "Digital Media Analytics: An Approach of Data Analysis and Organization", *Journal of Advances and Scholarly Researches in Allied EducationVol. XIV, Issue No. 1, October-2017, ISSN 2230-7540,* IIFS : 1.6 (2014), INDEX COPERNICUS : 49060 (2018), IJINDEX : 3.46 (2018), pp. 676-679, 2018.
- J.V.ANIL KUMAR , VUTUKURI LAKSHMI PRIYA, , "AN IDENTITY-ANONYMOUS AUTHENTICATION AND KEY AGREEMENT FRAMEWORK FOR PEER-TO-PEER CLOUD SYSTEMS", International Journal of Engineering Science and Advanced Technology (IJESAT) , Vol 25 Issue 12, 2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.03 9, Page 306 to 316, ISSN:2250-3676, 2025.