International Journal of Innovative Trends in Engineering Science and Technology
ijitest.org | E-ISSN: 3139-6887

A Secure and Intelligent Framework for Electronic Health Records Using Attribute-Based Encryption, Blockchain, and Machine Learning

[1]Srikanth Durgam [2]CH. Swapna Priya, [3]K. Suseela
[1,2]Associate Professor, [1,2]Department of Computer Science Engineering, [3]Department of School education
[1]Scient Institute of Technology, Hyderabad, [2]Vignan's Institute of Information Technology, Visakhapatnam,
[1]durgam.srikanth69@gmail.com [2]swapnachsp@gmail.com, [3]jackbenison12@gmail.com

Abstract -- Electronic Health Records (EHRs) hosted on centralized cloud platforms face significant security and privacy challenges, including unauthorized access and data manipulation. This paper proposes a robust, decentralized protection scheme for EHRs by amalgamating Attribute-Based Encryption (ABE) with Blockchain technology. Specifically, an advanced encryption algorithm—CEC-ABE (a refined version of Ciphertext-Policy ABE)—is introduced to decentralize the decryption phase, drastically minimizing computational overhead while enforcing strict, patient-centric access control. The immutable nature of blockchain, facilitated by Ethereum smart contracts written in Solidity, guarantees data provenance, traceability, and protection against tampering. Furthermore, the framework integrates machine learning models, specifically Random Forest and Support Vector Machines (SVM), to perform predictive analysis on patient cardiac data to aid clinical diagnosis. Experimental evaluations indicate that the proposed CEC-ABE algorithm significantly outperforms standard CP-ABE in computational efficiency, while the integrated machine learning classifiers achieve high predictive accuracy. The combined approach establishes a secure, traceable, and intelligent ecosystem for modern healthcare data management.

Keywords: Electronic Health Records (EHRs), Attribute-Based Encryption (ABE), Blockchain Technology, Machine Learning, Decentralized Security, Smart Contracts, Privacy Protection, Predictive Diagnostics.

I. INTRODUCTION

The digitization of healthcare through Electronic Health Records (EHRs) has streamlined medical data management and greatly enhanced patient care delivery. However, relying on traditional, centralized cloud computing architectures for storing sensitive health information introduces critical vulnerabilities. Centralized data centers often act as single points of failure, making them lucrative targets for malicious attacks and unauthorized data modifications. When patients outsource their medical history to third-party cloud providers, they effectively lose direct ownership and control over their personal data. This paradigm raises profound ethical and privacy concerns, as unauthorized entities, or even unscrupulous healthcare agents, could easily tamper with, leak, or exploit sensitive medical records without the patient's explicit consent.

To mitigate these inherent vulnerabilities, decentralized architectures and advanced cryptographic techniques have emerged as highly promising solutions. Blockchain technology, characterized by its distributed ledger and immutable cryptographic chaining, provides a tamper-proof environment highly suitable for maintaining the integrity of medical records. Concurrently, Attribute-Based Encryption (ABE)—particularly Ciphertext-Policy ABE (CP-ABE)—offers a granular, one-to-many encryption mechanism where data owners can dictate access policies based on user attributes. Despite its advantages, conventional CP-ABE schemes often impose heavy computational burdens during the decryption phase, rendering them inefficient for real-time, large-scale healthcare applications operating in edge cloud environments.

Addressing these computational and security bottlenecks, this research proposes a comprehensive, decentralized framework that synergizes a refined CEC-ABE algorithm with blockchain infrastructure and machine learning diagnostics. The proposed CEC-ABE mechanism optimizes the decryption process by offloading heavy computations, ensuring rapid and secure access exclusively for authorized medical personnel. Blockchain smart contracts govern the transparent and immutable logging of all EHR interactions. Moreover, the framework embeds predictive machine learning algorithms—Support Vector Machines (SVM) and Random Forest—to autonomously analyze encrypted patient data for heart condition diagnostics. By fusing advanced encryption,

DOI: 10.5281/zenodo.24444434
IJITEST-2026-032 | Volume 1, Issue 4, June 2026 | ISSN: 3139-6887
Creative Commons Attribution 4.0 International (CC BY 4.0)
Article Received: November 8, 2026 | Accepted: November 22, 2026

decentralized ledgers, and artificial intelligence, this system delivers an end-to-end secure, patient-controlled, and highly efficient healthcare management platform.

II. Related Work

Recent advancements in cryptography and decentralized networks have driven significant research into secure healthcare data outsourcing. Wang et al. proposed an identity-based data outsourcing (IBDO) framework designed to address origin auditing and secure delegation in cloud environments. Their scheme allowed users to authorize proxies to upload data securely without complex certificate management.

Addressing storage efficiency, Zhang and Xu introduced 'HealthDep', an encrypted EMR deduplication scheme for cloud-assisted health systems. Their approach allowed cloud servers to reduce storage costs by over 65% while preserving data confidentiality against unauthorized entities.

The foundational mechanics of access control in distributed systems were advanced by Bethencourt and Sahai, who developed the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme. They demonstrated how encrypted data could remain secure against untrusted storage servers by embedding complex access structures directly into the ciphertext. Building upon this, Wang et al. explored a fast CP-ABE system tailored for cyber-physical security in mobile healthcare networks. By offloading complex computational tasks to semi-trusted third parties, their model effectively accommodated the low computational power of mobile terminal devices.

Finally, Xu et al. presented 'Healthchain', a privacy-preserving scheme for large-scale medical data. By utilizing blockchain technology, their system prevented the tampering of IoT-generated health records and doctor diagnoses, thereby minimizing medical disputes through fine-grained, encryption-backed access control.

III. Proposed Methodology

The proposed system architecture provides a holistic solution encompassing decentralized data storage, cryptographic access control, and diagnostic predictive modeling.

A. Cryptographic Framework (CEC-ABE). To guarantee data confidentiality, the system employs a Custom Elliptic Curve Attribute-Based Encryption (CEC-ABE) algorithm. Doctors generate the EHR, which is then encrypted using CEC-ABE public keys before being stored. The algorithm enforces an access policy tree where only users (e.g., follow-up doctors) possessing the correct attributes can successfully compute the decryption keys. By decentralizing decryption processes and pushing partial computation to edge servers, the CEC-ABE algorithm significantly reduces the local computational time required by end-users.

B. Blockchain Integration and Smart Contracts. To ensure the integrity and traceability of the encrypted EHRs, the system leverages the Ethereum blockchain environment. Data storage and retrieval operations are governed by smart contracts written in the Solidity programming language. When a doctor uploads a prescription or a diagnostic report, a transaction is initiated via the Web3 interface. The blockchain records the cryptographic hash of the encrypted EHR, the timestamp, and the transaction details immutably. Patients act as the primary authority, verifying the records and granting attribute-based access to subsequent healthcare providers.

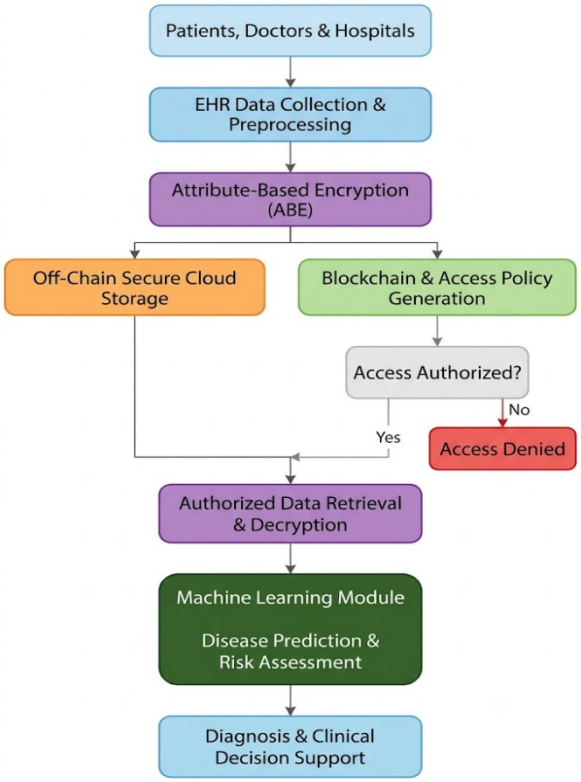


Figure 1: System Model of the Decentralized EHR Protection and Diagnostic Scheme.

C. Machine Learning Integration. The diagnostic component of the framework evaluates patient symptoms to predict heart conditions. A historical cardiovascular dataset (Cleveland) is loaded and preprocessed, utilizing standard scaling techniques (StandardScaler) to normalize the features. The system employs two prominent machine learning classifiers: Random Forest and Support Vector Machine (SVM). The data is split into an 80/20 ratio for training and testing. When a doctor inputs new patient parameters into the Django-based web interface, the integrated machine learning model processes the data in real-time, generating a prediction (Normal or Abnormal) that is subsequently encrypted and appended to the patient's blockchain record.

IV. Results and Discussions

The system was implemented using Python, the Django web framework, and a local Ethereum blockchain network. The evaluation focused on two primary metrics: the computational efficiency of the cryptographic algorithm and the diagnostic accuracy of the integrated machine learning models.

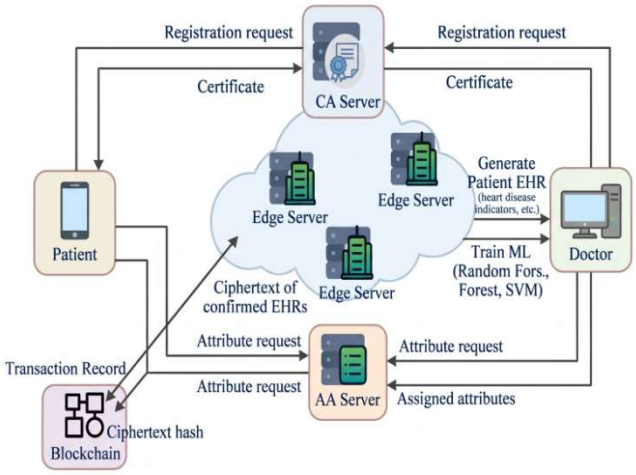


Figure 2: System Architecture of the Proposed Blockchain-Based EHR Framework.

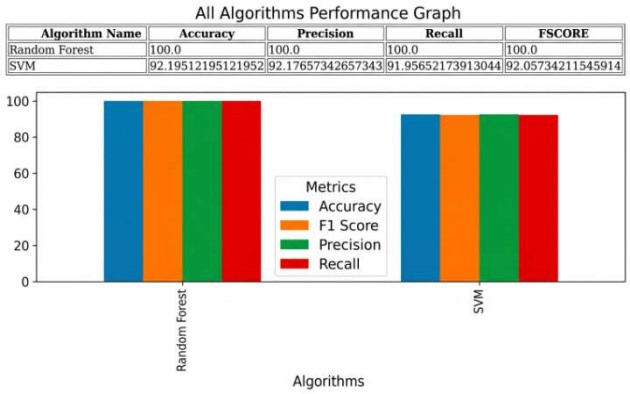


Figure 3: Performance Evaluation of Machine Learning Classifiers for Disease Prediction.

A. Computational Efficiency. A comparative time analysis was conducted between the standard CP-ABE algorithm and the proposed CEC-ABE algorithm. Simulation graphs demonstrated a substantial reduction in computational latency for the CEC-ABE approach. While the existing CP-ABE required extended processing times, the CEC-ABE algorithm completed the encryption and decryption cycles notably faster. This confirms that the proposed scheme is highly suitable for time-sensitive, real-time edge cloud healthcare scenarios.

B. Machine Learning Performance. The predictive models were evaluated using Accuracy, Precision, Recall, and F1-Score metrics.

Table 1: Performance Comparison of Random Forest and Support Vector Machine Classifiers on the Testing Dataset.

Classification Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest Classifier	100	100	100	100
Support Vector Machine (SVM)	92.19	92.17	91.95	92.05

The integration of these algorithms proves highly effective in serving as a reliable secondary diagnostic tool for healthcare professionals.

V. Conclusion and Future Scope

This research successfully establishes a secure, decentralized, and intelligent framework for managing Electronic Health Records (EHRs) by synergizing Attribute-Based Encryption (ABE) with blockchain technology. The implementation of the proposed CEC-ABE algorithm significantly alleviates the computational overhead traditionally associated with CP-ABE by decentralizing the decryption process, thereby ensuring swift and secure data access exclusively for authorized medical personnel. By anchoring the data storage and retrieval processes on an immutable blockchain ledger via smart contracts, the system guarantees comprehensive data provenance, traceability, and protection against unauthorized tampering.

Furthermore, the integration of machine learning classifiers—specifically Random Forest and Support Vector Machines (SVM)—adds a robust predictive diagnostic layer to the architecture. These models demonstrated high efficacy in analyzing patient symptoms to predict cardiovascular conditions accurately, serving as a reliable secondary diagnostic tool for healthcare providers. Ultimately, this integrated approach resolves the privacy vulnerabilities of centralized cloud servers, restores data ownership to the patients, and creates a trustworthy, efficient ecosystem for modern medical data management.

Future work will focus on integrating Layer-2 blockchain solutions, Federated Learning, IoMT devices, and automated anomaly detection to improve scalability, privacy, real-time patient monitoring, and proactive healthcare management.

References

[1] Wang, Y., Wu, Q., & Qin, B. "Identity based data outsourcing with comprehensive auditing in clouds." (Reference details adapted from literature survey).

[2] Zhang, Y., & Xu, C. "HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems." (Reference details adapted from literature survey).

[3] Bethencourt, J., Sahai, A., & Waters, B. "Ciphertext-policy attribute-based encryption." (Reference details adapted from literature survey).

[4] Wang, S., et al. "A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare network." (Reference details adapted from literature survey).

[5] Xu, J., et al. "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data." (Reference details adapted from literature survey).

Funding Declaration

The authors declare that no funds, grants, or other forms of financial support were received from any organization or institution for the conduct of this research.