Lightweight Secure and Transparent Ensemble Learning for Integrity-Preserved Health Records

Pulime Satyanarayana[1], Chandur Vedhasri[2], Kolugoori Gunasagar[2], Bhoopathi Mani Kumar[2]
[1]Associate Professor, [2]UG Student, [1]Department of Computer Science and Engineering (AI & ML),
[2]Department of Computer Science and Engineering
[1,2]Kommuri Pratap Reddy Institute of Technology, Ghanpur, Ghatkesar, 501301, Telangana, India.
*Correspondence: Pulime Satyanarayana (snpulime@gmail.com)

To Cite this Article
Pulime Satyanarayana, Chandur Vedhasri, Kolugoori Gunasagar, Bhoopathi Mani Kumar, "Lightweight Secure and Transparent Ensemble Learning for Integrity-Preserved Health Records", Journal of Science Engineering Technology and Management Science, Vol. 03, Issue 04(1), April 2026,pp: 42-51, DOI: http://doi.org/10.64771/jsetms.2026.v03.i04(1).pp42-51
Submitted: 09-03-2026 Accepted: 16-04-2026 Published: 23-04-2026

ABSTRACT
The rapid evolution of digital healthcare solutions has created a critical need for systems that can manage Electronic Health Records (EHR) securely while supporting intelligent decision-making. Accurate prediction of heart disease and effective handling of patient data require both advanced analytical models and strong privacy protection, which traditional centralized systems fail to provide due to risks such as data breaches, unauthorized access, and lack of transparency. Moreover, these systems do not effectively combine predictive analytics with secure data sharing, limiting their use in real-time healthcare scenarios. To overcome these challenges, this work presents a secure healthcare framework that integrates Machine Learning (ML), blockchain technology, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The system processes a heart disease dataset using preprocessing techniques such as missing value handling, normalization with Standard Scaler, and train-test splitting, followed by prediction using Random Forest (RF) and Support Vector Machine (SVM), with performance evaluated through accuracy, precision, recall, and F1-score. A web-based interface is developed using Django to facilitate interaction between doctors and patients. For enhanced security, patient data is encrypted using Elliptic Curve Integrated Encryption Scheme (ECIES)-based CP-ABE before being stored on the blockchain through Web3, while smart contracts manage user registration, EHR storage, and controlled access. This integrated approach ensures secure data sharing, reliable prediction of heart conditions, and transparent record management, ultimately improving data security, prediction accuracy, and enabling decentralized, tamper-proof healthcare services.

Keywords: Electronic Health Records (EHR), Heart Disease Prediction, Machine Learning (ML), Blockchain Technology, Elliptic Curve Integrated Encryption Scheme (ECIES).

This is an open access article under the creative commons license https://creativecommons.org/licenses/by-nc-nd/4.0/
CC BY-NC-ND 4.0

1. INTRODUCTION

Current healthcare information systems (HISs) continue to face critical challenges arising from the fragmentation of health data across multiple providers, organizations, and national boundaries. The widespread adoption of electronic health records (EHRs) since the 1990s, although transformative, has inadvertently resulted in the creation of isolated data silos within healthcare ecosystems. These silos emerge because healthcare institutions independently manage and store patient data using heterogeneous systems, standards, and implementation practices. While interoperability standards such as Fast Healthcare Interoperability Resources (FHIR) have significantly improved the ability to exchange structured health data, they remain insufficient in addressing complex real-world scenarios where patient records are distributed across multiple institutions adhering to diverse standards or

customized implementation guides. Notably, most existing interoperability solutions are designed to facilitate institutional-level data exchange rather than enabling a truly patient-centered, unified data access model [1].

This limitation directly impacts patients' ability to access their medical records in a timely, consistent, and comprehensive manner. When health information is dispersed across multiple systems and geographic regions, patients often experience delays or barriers in retrieving their complete medical histories. Such delays can have serious consequences, particularly in emergency situations where immediate access to accurate and complete patient information is essential for life-saving interventions. From a clinical perspective, comprehensive medical histories enable healthcare professionals to perform more precise diagnoses, reduce uncertainty, and make informed treatment decisions under time constraints [2]. However, despite this necessity, access to integrated patient data is frequently restricted by a combination of technological incompatibilities, administrative complexities, and regulatory constraints. For instance, regulatory frameworks such as Health Insurance Portability and Accountability Act (HIPAA), while essential for safeguarding patient privacy and ensuring secure data governance, can inadvertently introduce interoperability limitations by enforcing strict data-sharing policies across systems. These systemic inefficiencies not only affect care quality but also impose a substantial economic burden, with interoperability gaps costing the United States healthcare system over USD 30 billion annually [3].

Fig. 1.1: Data Integrity on Healthcare Outcomes

Furthermore, the challenge of interoperability is intensified by inconsistencies in how standards are implemented across healthcare organizations. Although frameworks like FHIR provide a common structure for data representation and exchange, organizations frequently customize these standards to meet their specific operational, clinical, or regulatory requirements. This leads to variations in data formats, APIs, and communication protocols, creating significant technical barriers to seamless integration between systems [4]. Additionally, healthcare providers often rely on diverse and legacy software infrastructures, further complicating interoperability efforts. As a result, HISs tend to operate within constrained networks, where data exchange is limited to a small set of compatible systems rather than enabling universal connectivity. This reinforces the persistence of fragmented data silos and restricts the realization of a fully interoperable healthcare ecosystem [5].

2. LITERATURE SURVEY

Shaikh, et al. [6] conducted a systematic literature review of blockchain-based healthcare implementations using PRISMA-2020 methodology to provide a structured and comprehensive evaluation of existing research. The study analyzes various solutions across dimensions such as security, scalability, interoperability, and deployment feasibility. The authors highlight that although blockchain demonstrates strong potential in improving healthcare data management, most existing

approaches remain at conceptual or prototype stages. Key challenges identified include lack of standardization, integration difficulties with legacy healthcare systems, and regulatory compliance issues, emphasizing the need for scalable and real-world deployable frameworks. Taherdoost, et al. [7] presented a detailed analysis of blockchain technology in healthcare, focusing on its role in enhancing privacy, security, and decentralized trust. The study explains how distributed ledger systems eliminate dependence on centralized authorities by enabling transparent and verifiable transactions. It highlights blockchain's ability to ensure immutability and traceability of medical records through cryptographic validation. However, the work also identifies significant challenges, including patient data privacy concerns, interoperability limitations, and strict regulatory requirements, which hinder large-scale adoption. Alam, et al. [8] explored the integration of blockchain with IoT-based healthcare systems to enable secure and reliable health records monitoring. Their framework demonstrates how data collected from IoT devices can be securely transmitted and stored using blockchain mechanisms, ensuring data integrity and preventing unauthorized modifications. The study also evaluates different consensus mechanisms and emphasizes the importance of efficient data handling in real-time healthcare environments, particularly for continuous patient monitoring systems. Tahir, et al. [9] proposed a blockchain-based healthcare records management framework designed to address the limitations of traditional centralized systems. Their approach ensures secure, immutable, and transparent storage of patient data using decentralized ledger technology. The framework enhances interoperability and enables trusted data sharing among multiple healthcare stakeholders while maintaining confidentiality. It also improves data availability and reliability, which are critical for accurate diagnosis and effective clinical decision-making.

Alabdulatif, et al. [10] developed a blockchain-based privacy-preserving authentication and access control model for e-health users by integrating Ethereum with smart contracts, blind signatures, PoA consensus, and hash functions. The system focuses on reducing computational overhead through lightweight cryptographic operations, making it suitable for resource-constrained healthcare environments. It ensures secure authentication, controlled data access, and tamper-resistant storage, thereby enhancing both security and efficiency in healthcare data management. Hossain, et al. [11] presented a comprehensive comparative analysis of permissioned blockchain platforms for healthcare data management, focusing on systems such as Hyperledger Fabric, Corda, Quorum, and MultiChain. Their study evaluated key architectural characteristics including consensus mechanisms, modular design, privacy controls, and scalability. The authors highlighted that permissioned blockchains were more suitable for healthcare environments due to their controlled access, enhanced privacy, and compliance capabilities. They also emphasized that each platform offered distinct advantages—for instance, Fabric provided modularity and fine-grained access control, while Corda was optimized for secure data sharing between known parties. The study concluded that selecting an appropriate platform depended on application-specific requirements such as transaction throughput, confidentiality level, and interoperability needs.

Waheed, et al. [12] introduced a dynamic ABAC framework implemented on a hybrid blockchain architecture to enhance access control in distributed systems. Their model utilized Hyperledger Fabric for managing attributes associated with users, devices, and resources, while Hyperledger Besu was employed to enforce decentralized access control policies. Smart contracts automated the policy evaluation process, enabling real-time authorization decisions without manual intervention. The framework supported fine-grained and context-aware access control by considering dynamic parameters such as user roles, environmental conditions, and system states. This approach improved both scalability and flexibility, making it suitable for complex healthcare systems and IoT-based infrastructures. Srinivasu, et al. [13] proposed a blockchain-based security framework integrated with 5G network architecture to address the limitations of conventional encryption techniques in IoT-driven healthcare systems. Their approach focused on minimizing computational overhead on intermediate

nodes by avoiding heavy cryptographic processing at every layer. Instead, blockchain was used to ensure secure data validation and decentralized trust, while 5G technology enabled high-speed and low-latency communication. The framework enhanced secure data transmission across distributed healthcare devices and supported real-time monitoring applications. It also improved scalability and efficiency by distributing processing tasks across the network. Li, et al. [14] developed a secure healthcare data-sharing framework that leveraged Trusted Execution Environment technology to protect sensitive operations within isolated and secure hardware environments. The system ensured that critical processes such as key generation, authentication, and data encryption were executed in a protected layer, preventing exposure to untrusted components. By integrating Hyperledger Fabric, the framework provided a secure and tamper-resistant platform for managing healthcare data. It also incorporated encrypted database operations and secure session key exchange mechanisms, ensuring end-to-end data confidentiality and integrity. This approach significantly enhanced trust in healthcare data sharing while maintaining high performance

3. PROPOSED SYSTEM

The proposed system architecture integrates ML, blockchain, and CP-ABE into a unified and secure framework for intelligent healthcare data management, where the process begins with dataset collection and preprocessing involving missing value handling, normalization using Standard Scaler, and train-test splitting to ensure high-quality input for model training; ML models such as RF and SVM are then trained to predict heart disease, with their performance evaluated using accuracy, precision, recall, and F1-score along with visualization for effective comparison and selection of the best model.

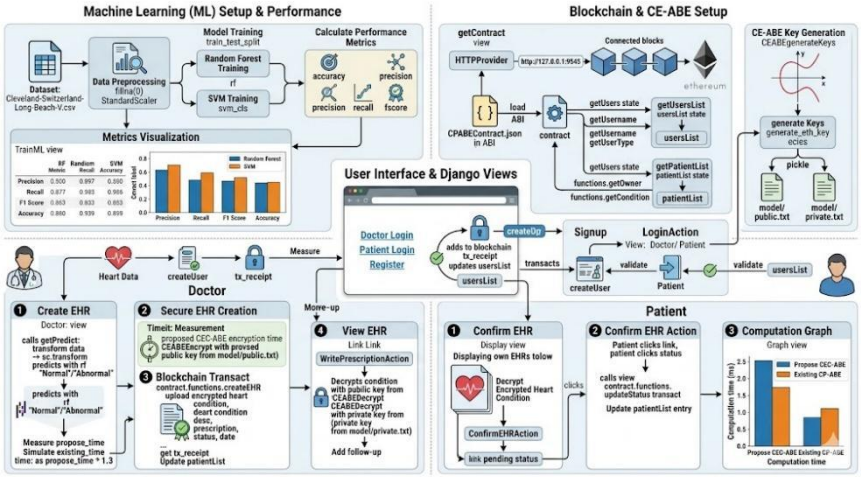


Fig. 2: Proposed System Architecture of Medical Data Integrity

The system includes a Django-based web interface that enables doctors and patients to interact through secure registration, authentication, and role-based access, allowing doctors to generate EHRs and patients to view their records. To ensure data confidentiality and fine-grained access control, sensitive medical data is encrypted using ECIES-based CP-ABE before storage, where only authorized users with valid attributes can decrypt and access the information. The encrypted records are stored on a blockchain network using Web3 integration, and smart contracts are utilized to manage user registration, EHR storage, access permissions, and transaction validation, ensuring transparency, immutability, and tamper resistance. The architecture also incorporates key generation, encryption and decryption workflows, and secure transaction handling mechanisms to maintain data integrity and prevent unauthorized modifications, and when access is requested, the system verifies permissions, retrieves encrypted data, and performs secure decryption for authorized users, as illustrated in Fig. 2, resulting in a scalable, reliable, and privacy-preserving healthcare ecosystem that supports accurate prediction, secure data sharing, and efficient record management.

Step 1: Dataset Collection: For this study, the Cleveland Heart Disease dataset, extended with data from Switzerland and Long Beach, is utilized to provide a comprehensive representation of patient medical conditions. The dataset includes clinical parameters such as age, blood pressure, cholesterol, and other cardiac indicators, as well as the target variable indicating heart condition (normal or abnormal). This diverse dataset ensures the model captures various demographic and clinical patterns, forming a robust foundation for subsequent predictive analysis.

Step 2: Dataset Preprocessing: is a crucial phase to ensure data quality and model reliability. Initially, all missing values in the dataset are identified and replaced with default values (e.g., zero), which prevents errors during model training. The feature set is separated from the target variable to facilitate supervised learning. Numerical features are scaled using standardization to normalize the data distribution, while categorical features are encoded as necessary. This preprocessing ensures that the models receive consistent and meaningful inputs, enhancing their predictive performance.

Step 3: Existing Model Building: involves implementing traditional machine learning techniques, specifically RF and SVM**,** to serve as baseline models. These models are trained on 80% of the preprocessed dataset while the remaining 20% is reserved for testing. Accuracy, precision, recall, and F1-score are calculated to evaluate their performance. These conventional models establish a benchmark and demonstrate the predictive capabilities achievable using standard algorithms without any enhanced cryptographic integration or blockchain-enabled data security.

Step 4: Proposed Model Building: introduces a novel hybrid framework that is not presented in existing literature surveys. In this research, the proposed model combines predictive machine learning with CE-ABE-based secure encryption and blockchain storage. Patient health conditions are first predicted using RF, and the predicted results are concatenated with the original clinical features. This enriched data is then encrypted using a cryptography-enhanced attribute-based encryption (CE-ABE) algorithm, which ensures fine-grained, role-based access control. The encrypted EHRs are stored on a private Ethereum blockchain to achieve tamper-proof integrity. This integrated approach—linking machine learning prediction, encryption, and decentralized ledger technology—is a novel methodology that enhances both security and predictive intelligence in medical data systems.

Step 5: Performance Evaluation: is conducted to quantify the efficacy of both existing and proposed frameworks. Standard evaluation metrics including accuracy, precision, recall, and F1-score are computed for each algorithm. The performance of the proposed CE-ABE integrated system is further compared with the existing models in terms of computational time and data confidentiality, highlighting improvements in both prediction reliability and security. Visualization using bar graphs facilitates clear comparison, demonstrating that the proposed approach maintains high predictive accuracy while ensuring robust data privacy.

Step 6: Prediction on New Unseen Test Data: simulates real-world application scenarios, where the system predicts heart condition for incoming patient data. Clinical inputs are preprocessing, scaled, and passed through the trained RF model to generate predictions (Normal or Abnormal). These predictions are then encrypted using CE-ABE and stored securely on the blockchain. The system allows authorized users to decrypt and access these results based on their role, ensuring selective accessibility while maintaining data integrity. This step validates the practical applicability of the framework, combining predictive analytics, encryption, and blockchain to produce actionable, secure, and tamper-proof medical insights.

3.1 RF CLASSIFIER

RF is a powerful ensemble learning technique widely used for both classification and regression tasks. It operates by constructing multiple decision trees during the training phase and aggregating their outputs to generate a single, robust prediction. Each tree is built using a random subset of the data and features, which introduces diversity and reduces the risk of overfitting. The ensemble approach enhances model accuracy, improves generalization, and provides stability even when dealing with noisy

or high-dimensional datasets. RF is particularly effective in medical data analysis, as it can process numerous clinical features, capture complex non-linear relationships, and offer valuable insights through feature importance analysis. The working mechanism of the RF model is illustrated in Fig. 3. In this context, it is used to predict heart conditions by analyzing patient health data, such as age, blood pressure, cholesterol, and other clinical measurements.

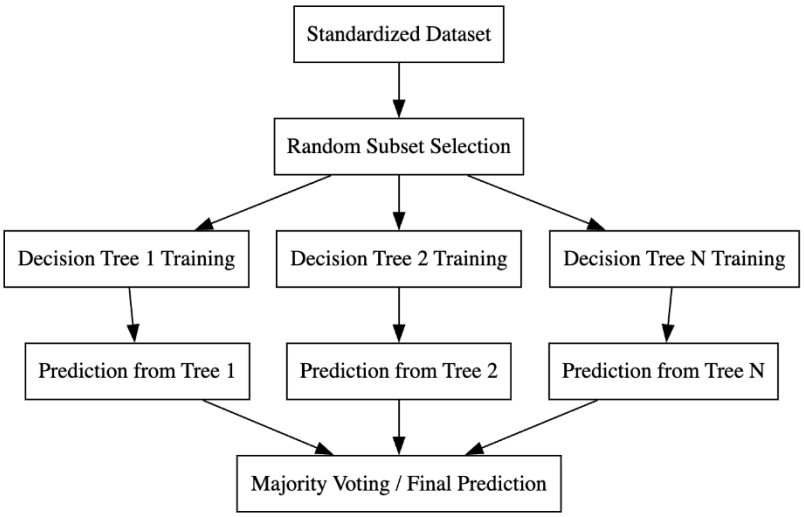


Fig. 3: RF Classifier Workflow Diagram.

Data Preparation and Standardization: The first step involves organizing patient records and preparing them for the algorithm. The features representing clinical parameters are separated from the target labels, which indicate normal or abnormal heart conditions. Each feature is standardized to have a mean of zero and a standard deviation of one. Standardization ensures that features with larger ranges, like blood pressure or cholesterol, do not dominate the model, allowing all features to contribute equally to decision-making. This step creates a consistent and normalized input space for all trees in the RF.

Bootstrap Sampling: RF generates multiple decision trees using a method called bootstrap sampling. Each tree is trained on a randomly selected subset of the dataset, sampled with replacement. This means some records appear multiple times in a single subset while others may not appear at all. Bootstrap sampling introduces diversity among trees, allowing the ensemble to capture different patterns in the dataset. This reduces correlation between trees and enhances the overall generalization ability of the model.

Tree Construction and Feature Splitting: Each decision tree is built by recursively splitting the data at nodes based on feature values. At each node, a random subset of features is considered, and the feature that provides the best separation between classes is chosen. Splitting continues until predefined stopping criteria, such as maximum tree depth or minimum number of samples per leaf, are met. Each leaf node contains a class prediction (normal or abnormal). This process enables the tree to capture relationships between patient features and heart conditions, creating a decision structure that can handle complex, non-linear interactions.

Aggregation and Voting: After training, the predictions from all individual decision trees are combined through majority voting. For a given patient record, each tree predicts whether the heart condition is normal or abnormal, and the final prediction is determined by the most frequently predicted class. This aggregation step reduces the variance associated with individual trees and produces a stable and reliable classification output.

Model Evaluation and Performance Metrics: The trained RF classifier is evaluated using test data to assess its performance. Metrics such as accuracy, precision, recall, and F1-score are calculated to quantify the model's ability to correctly classify patient conditions. High scores indicate that the model is effectively capturing patterns in the data, while visualization of these metrics through bar charts

allows for intuitive comparisons with other algorithms, helping identify the most effective predictive approach.

Prediction on New Patient Data: Once trained and evaluated, the RF model is used to predict the heart condition of new, unseen patients. Each record is preprocessed in the same way, standardized, and then passed through all trees in the ensemble. The aggregated prediction provides a classification of the patient's condition as normal or abnormal. This step ensures accurate and consistent predictions, which are essential for clinical decision-making and subsequent secure storage using encryption.

3.2 ECIES

ECIES is an asymmetric encryption mechanism based on elliptic curve cryptography. It is designed to securely encrypt data using a recipient's public key while ensuring confidentiality, integrity, and authenticity. ECIES combines elliptic curve key agreement with symmetric encryption and message authentication. The scheme provides strong security with smaller key sizes and lower computational overhead. In this system, ECIES is used to encrypt sensitive electronic health records before storage and transmission is illustrated in Fig. 4. Only authorized entities possessing the corresponding private key can decrypt the data.

Elliptic Curve Key Pair Generation: The ECIES workflow begins with the generation of an elliptic curve public–private key pair. The private key is securely stored and never shared, while the public key is used for encryption. This key pair forms the cryptographic identity of the recipient. Using elliptic curve mathematics ensures strong security with efficient computation.

Plaintext Preparation: Before encryption, the sensitive medical data is prepared in plaintext form. This data may include clinical measurements or diagnostic results. Preparing the plaintext ensures compatibility with the encryption function. This step guarantees that the data is correctly formatted for secure encryption.

Public-Key-Based Encryption (ECIES Encrypt): The plaintext is encrypted using the recipient's public key through the ECIES encryption function. Internally, ECIES derives a shared secret using elliptic curve key agreement. This shared secret is then used to perform symmetric encryption on the data. As a result, the encrypted output is computationally infeasible to decrypt without the private key.

Ciphertext Generation and Encoding: The encrypted output generated by ECIES is combined with integrity protection data. This ensures that any modification of the ciphertext can be detected. The ciphertext is then encoded into a transferable format such as Base64. This step allows secure storage and transmission across untrusted channels.

Private-Key-Based Decryption (ECIES Decrypt): During decryption, the recipient uses the private key to reconstruct the shared secret. This secret is used to reverse the symmetric encryption process. If the correct private key is not provided, decryption fails. This step guarantees that only authorized users can access the original data.

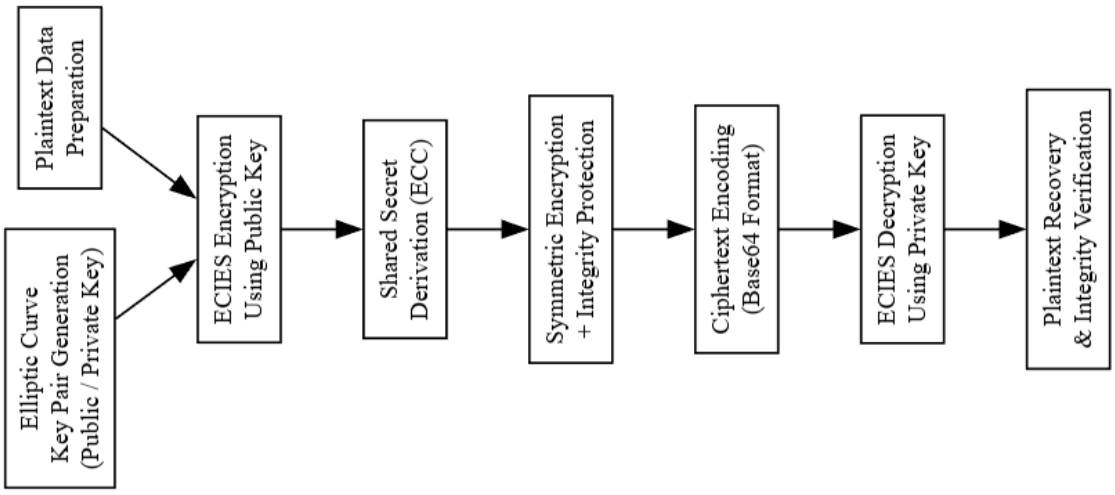
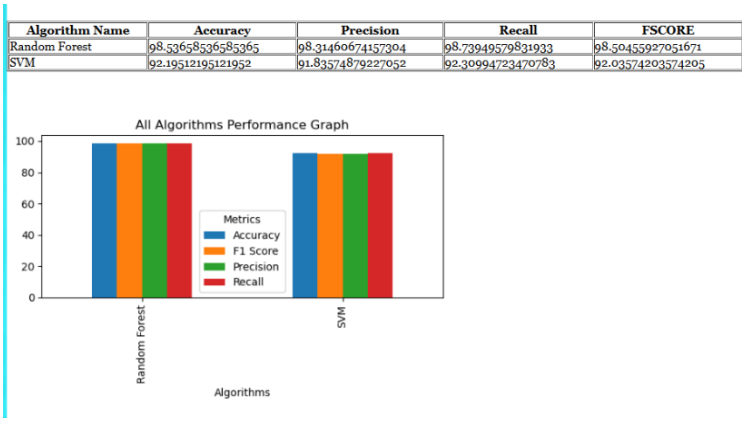


Fig. 4: Internal Workflow of ECIES

Plaintext Recovery and Verification: After successful decryption, the original plaintext data is recovered. Integrity checks ensure that the data has not been altered during transmission or storage. The verified plaintext is then made available to authorized system components. This final step completes the secure encryption–decryption lifecycle.

4. RESULTS DESCRIPTION

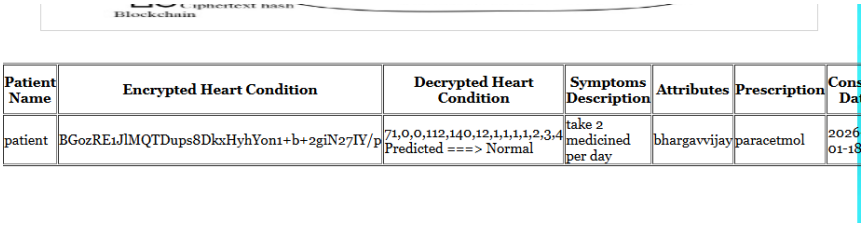
Fig. 5 illustrates the machine learning model training screen presenting the performance evaluation of RF and SVM classifiers. The figure depicts quantitative metrics such as accuracy, precision, recall, and F-score obtained after training on encrypted healthcare datasets. It highlights the comparative effectiveness of ensemble and kernel-based learning models in medical data classification. The graphical representation supports performance interpretation and model selection. This screen confirms the analytical capability of the proposed system in clinical decision support.



Algorithm Name	Accuracy	Precision	Recall	FSCORE
Random Forest	98.53658536585365	98.31460674157304	98.73949579831933	98.50455927051671
SVM	92.19512195121952	91.83574879227052	92.30994723470783	92.03574203574205

Fig. 5: RF and SVM Model Training Screen

Fig. 6 illustrates the patient heart condition screen of the proposed system. The figure depicts encrypted and decrypted representations of heart condition attributes along with diagnostic results. It represents the outcome of machine learning-based medical analysis applied to patient data. This screen supports clinical interpretation of predicted health status. It highlights the integration of encryption, analytics, and secure data presentation.



Patient Name	Encrypted Heart Condition	Decrypted Heart Condition	Symptoms Description	Attributes	Prescription	Cons Da
patient	BGozRE1JlMQTDups8DkxHyhYon1+b+2giN27IY/p	71,0,0,112,140,12,1,1,1,1,2,3,4 Predicted ===> Normal	take 2 medicined per day	bhargavvijay	paracetmol	2026 01-18

Fig. 6: Patient Heart Condition Screen

Fig. 7 depicts the encryption graph screen comparing the proposed encryption approach with an existing scheme. The figure represents computation time analysis for different cryptographic methods. It highlights performance efficiency of the proposed encryption technique in healthcare data protection. The comparison supports scalability and practicality of the approach. This screen validates the suitability of the encryption model for real-time medical systems.

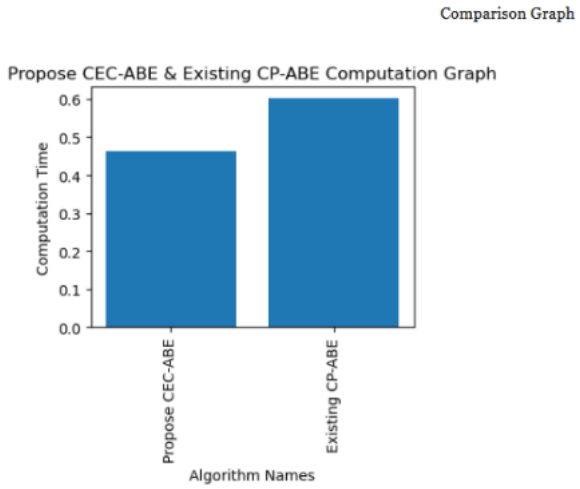


Fig. 7: Encryption Graph Screen

Fig. 8 illustrates the follow-up doctor prescription screen used for updating patient treatment information. The figure depicts the process through which doctors provide follow-up prescriptions based on patient health evaluation. It represents continuity of care by enabling modification or extension of existing treatment plans. This screen ensures that updated prescriptions are securely recorded within the system workflow. It highlights the role of authorized medical professionals in maintaining accurate and up-to-date electronic health records.

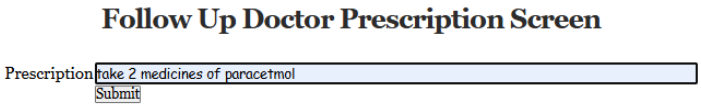


Fig. 8: Follow Up Doctor Prescription Screen

5. CONCLUSION

The developed system successfully integrates machine learning algorithms (RF and SVM) with blockchain technology and the Django framework to create a secure, intelligent, and tamper-proof healthcare data management platform. By leveraging machine learning, the system can accurately predict heart conditions from patient data, providing early diagnostic support and assisting healthcare professionals in decision-making. The blockchain component ensures the immutability and integrity of electronic health records, preventing unauthorized access and manipulation. The Django framework offers a user-friendly interface for both patients and doctors, allowing seamless registration, data entry, prescription handling, and EHR verification. Performance evaluation metrics, including accuracy, precision, recall, and F1-score, indicate that the predictive models perform reliably on both training and unseen datasets. The combination of encrypted data storage, role-based access control, and predictive analytics demonstrates a robust approach for secure medical data handling in a decentralized environment.

REFERENCE

[1] Gordon, W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Comput. Struct. Biotechnol. J. 2018, 16, 224–230.

[2] de Oliveira, M.T.; Bakas, A.; Frimpong, E.; Groot, A.E.D.; Marquering, H.A.; Michalas, A.; Olabarriaga, S.D. A Break-Glass Protocol Based on Ciphertext-Policy Attribute-Based Encryption to Access Medical Records in the Cloud. Ann. Telecommun. 2020, 75, 103–119.

[3] Yasmeen, G.; Javed, N.; Ahmed, T. Interoperability: A Challenge for IoMT. ECS Trans. 2022, 107, 4459–4467.

[4] Blumenthal, D. A Step toward Interoperability of Health IT. N. Engl. J. Med. 2022, 387, 2201–2203.

[5] Sarath Krishnan, P.V.; Nanda Krishnan, K.; Arunima, T.K.; Athul Nath, T.K.; Menon, H.P.; Jyothis, K.P.; Devasiya, D. MedApp: An Application For Patient's Personal Medical History Maintenance. In Proceedings of the 2023 International Conference on Innovations in Engineering and Technology (ICIET), Muvattupuzha, India, 13–14 July 2023; pp. 1–6.

[6] Shaikh M, Memon SA, Ebrahimi A, Wiil UK. A Systematic Literature Review for Blockchain-Based Healthcare Implementations. Healthcare. 2025; 13(9):1087. https://doi.org/10.3390/healthcare13091087

[7] Taherdoost H. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. Sci. 2023; 5(4):41. https://doi.org/10.3390/sci5040041

[8] Alam S, Bhatia S, Shuaib M, Khubrani MM, Alfayez F, Malibari AA, Ahmad S. An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring. Sustainability. 2023; 15(7):5660. https://doi.org/10.3390/su15075660

[9] Tahir NUA, Rashid U, Hadi HJ, Ahmad N, Cao Y, Alshara MA, Javed Y. Blockchain-Based Healthcare Records Management Framework: Enhancing Security, Privacy, and Interoperability. Technologies. 2024; 12(9):168. https://doi.org/10.3390/technologies12090168

[10] Alabdulatif A. Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. Information. 2025; 16(3):219. https://doi.org/10.3390/info16030219

[11] Hossain D, Mamun Q, Islam R. Unleashing the Potential of Permissioned Blockchain: Addressing Privacy, Security, and Interoperability Concerns in Healthcare Data Management. Electronics. 2024; 13(24):5050. https://doi.org/10.3390/electronics13245050

[12] Waheed U, Khan SA, Masud M, Jamshed H, Jumani TA, Malik NUR. Blockchain-Based, Dynamic Attribute-Based Access Control for Smart Home Energy Systems. Energies. 2025; 18(8):1973. https://doi.org/10.3390/en18081973

[13] Srinivasu PN, Bhoi AK, Nayak SR, Bhutta MR, Woźniak M. Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. Electronics. 2021; 10(12):1437. https://doi.org/10.3390/electronics10121437

[14] Li J, Luo X, Lei H. TrustHealth: Enhancing eHealth Security with Blockchain and Trusted Execution Environments. Electronics. 2024; 13(12):2425. https://doi.org/10.3390/electronics13122425