# A Privacy-Preserving Blockchain Framework for Secure Collaboration in Cloud-Based Applications

**Umme Habeeba fatima[1], Mohammed Mukkaram Ali[2]**

**[1]Department of Computer Science and Engineering, Shadan women's college of engineering and technology, Hyderabad, India**

**[2]Department of Computer, Jazan University, Saudi Arabia**

**DOI: https://doi.org/10.51244/IJRSI.2026.1303000053**

**Received: 16 March 2026; Accepted: 21 March 2026; Published: 28 March 2026**

## ABSTRACT

The speed with which cloud computing has been used in cooperative healthcare applications has brought forth numerous concerns as far as data privacy, decentralized trust, and secure access control are concerned. The past systems, which were centralized, are highly susceptible to single points of failure and have a restricted ability to audit sensitive medical information. This paper presents a privacy-sensitive blockchain framework that enables cooperation among people in the early detection of heart disease to work efficiently. To guarantee the secrecy of sensitive identifiers of patients and the integrity of data, the framework employs enlightened cryptography techniques, including, but not limited to, AES-256-GCM encryption and salted SHA-256 hash. The main part of the system is the high-performance stacking ensemble machine learning model, which is composed of the following models: Random Forest, XG Boost, Light GBM, and Multi-Layer Perceptron (MLP). Possessing the ability to determine valid and suspicious access requests and effectively estimate the state of heart disease are its major functions. Smart contracts used to uphold an audit trail in an immutable fashion utilise a certified blockchain in which access decisions, audit metadata, and additional blockchain data are stored. To verify scalability and robustness, the framework is assessed using both synthetic and benchmark datasets (UCI Heart Disease). The performance of the ensemble model to improve the accuracy of an enhanced UCI Heart Disease dataset is demonstrated by experimental results showing 95% accuracy, 0.98 ROC-AUC, and better precision-recall than the performance of the individual classifiers. The results prove that the suggested framework provides a scalable, reliable, and regulation-conformant solution to medical collaboration in the cloud that will provide the best balance of top-level security and quality of clinical diagnosis.

**Keywords**— Machine Learning, XG Boost, Blockchain, Access Control, Privacy, Cloud Computing, Healthcare, Smart Contracts, UCI Dataset

## INTRODUCTION

The impact of cloud computing on the storage of information, computer processing, and information exchange has been tremendous in organizations. It is measured to be a key foundation on which contemporary digital services are based, mostly in healthcare, where the multi-institutional interaction is indispensable. The multi-user cloud-based environments facilitate access to shared computing resources by multiple users (doctors, researchers, and diagnostic centers) and efficient data processing. Nonetheless, the increased reliance on cloud infrastructures has raised some significant issues pertaining to data privacy, controlled access, and managed trust. The stored medical records and clinical identifiers are susceptible to attack and single points of failure because of the centralized nature of cloud systems (where sensitive medical records and clinical identifiers are stored on cloud servers), which are high points of vulnerability [4], [6].

In contrast to the current blockchain-based cloud security systems, which are only based on access logging, the suggested system incorporates privacy-aware hashing, encrypted log storage, and a stacking ensemble machine learning framework to classify intelligent access. This integrated architecture allows managing trust decentrally as well as detecting anomalies proactively, two measures that are not combined in a current system.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

The cloud systems are to be designed to enable an effective form of interaction with the system where it is fully confidential, intact, and accountable, and in an appropriate collaborative work type. The traditional security systems mainly feature a central system of authentication, and in such a case, a breach is likely to be recorded. In case the centralized power is disrupted, hackers can gain unauthorized access to the most sensitive patient diagnostics, and it becomes challenging to confirm the activities of the systems. The restrictions emphasize the necessity of decentralized mechanisms that would be able to afford secure cooperation and effective auditing of distributed cloud environments [7].

The blockchain technology has become one of the potential solutions that can help to solve this issue because it is a decentralized, transparent, and immutable ledger. The fusion of blockchain and cloud infrastructure can lead to data distribution and access decentralization to guarantee safety and security. In the past, it has been proven that blockchain can defend sensitive data in the distributed ecosystem [10], [11]. Moreover, access policies can be enforced automatically through smart contracts and become more reliable when used in a collaborative environment [18].

Regardless of these benefits, most of the existing frameworks have no intelligent mechanisms for detecting abnormal access coupled with the provision of accurate clinical predictions. Recent studies investigated machine learning to support cybersecurity and anomaly detection [1],[11]. Nevertheless, the methods are frequently introduced without blockchain and seldom solve the issue of the necessity of high-precision diagnostic tools based on a secure platform.

To address these drawbacks, this study suggests a privacy blockchain model for safe cooperation in the cloud of applications with heart disease prediction as a key case study. The suggested model incorporates the cryptographic technology, access classification by means of machine learning, and permissioned blockchain technology. Sensitive identifiers are hashed with salted SHA-256 hash without revealing their identities, and access logs with AES-256-GCM ciphers. More importantly, the stacking ensemble model (Random Forest, XGBoost, LightGBM, and MLP) is employed to fulfill two goals: to identify the access requests as legitimate or malicious, as well as to achieve high-accuracy heart disease diagnosis with the help of the clinical features. Smart contracts are used to store the access decisions and diagnostic metadata on a permissioned blockchain. The key questions of this study are:

- To develop a privacy-friendly blockchain system of secure cloud-based healthcare collaboration.
- To generate a machine learning-based system for malicious access detection and offering heart disease diagnosis predictions.
- To incorporate a cryptographic protection mechanism to protect sensitive patient identifiers and the system log.
- To measure the performance of the suggested framework based on the standard act events, such as accuracy, precision, recall, F1-score, and ROC-AUC.

## RELATED WORK

The blockchain has recently become a potential solution that has drawn significant attention over the last few years and has been attributed to enhancing security, transparency, and data integrity when it comes to healthcare information systems. As electronic health records (EHRs) and cloud-based care systems gain more popularity, software security in the case of sensitive patient information is gaining wide prominence. Conventional federal information storage systems are susceptible to data breaches, unlimited entree, and tampering. In this regard, scholars have investigated the application of blockchain-based models in permitting decentralized storage, reliable authentication, and unchangeable data recording in healthcare applications. The medical record management system suggested by Verma et al. is based on the blockchain of medical records and employs the Keyless Signature Infrastructure Blockchain (KSIBC) in the algorithm alongside the Blowfish encryption algorithm to guarantee the integrity of data and secure data transfer [1]. By making data manipulation that undermines the security of healthcare records impossible with blockchain verification, they contribute to their

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

security. The system, however, mainly puts emphasis on integrity and traceability, in addition to offering a few real-time privacy and access control facilities in a distributed setting.

In an attempt to enhance the maintenance of privacy in decentralized healthcare, a few researchers have explored the claim of progressive cryptographic tools and machine learning algorithms. Shrestha et al. presented a study of the combination of united knowledge and homomorphic encryption to allow a privacy-seeking data calculation among distributed healthcare nodes [2]. Federated learning can also be used to train machine learning models, which reduces the transfer of raw data, thereby enhancing privacy. Even though the mentioned methods offer viable theoretical guarantees of privacy, they tend to bring about large computational burdens caused by the complicated cryptographic operations. This complexity makes them less applicable in a physical time health care organization where speed and efficiency of the system are required to be used. To remove this disadvantage, the Advanced Encryption Standard (AES) will be installed in the proposed structure to provide a reasonable tradeoff between high encryption security and performance.

In healthcare data management, there exist advanced research works on the application of blockchain systems to improve traceability and audit in data management. Conti et al. explored several blockchain in the process of storing and controlling access to data, which are favorable in the process of decentralization of the ledgers to ensure tamper-proof data regarding the transaction of data [3]. Some of them are supported by large blockchain systems such as Ethereum or Hyperledger to archive decentralized records. These systems offer a fair promise of an immutable nature, but they bring an additional burden to the problems of integration, scalability, and processing overheads.

In order to overcome these weaknesses, the need framework uses a lightweight hash mechanism of the SHA-256 type to keep secure audit logs of the healthcare transactions. This algebra is similar in the benefits of immutability but with lower computational costs, which is why it suits small-scale healthcare systems.

The recent research has also led to a study of the machine learning methods in predicting diseases and analytics in health care. One such application is the early disease detection system suggested by Rajput et al. on the basis of patient health records, being powered by machine learning [4]. Such models are very accurate in prediction; however, most of them manipulate medical information in plain text and hence are not designed to include privacy-preserving strategies. These systems consequently tend to be traded off on the accuracy of their prediction and the confidentiality of patient data. On the same note, Zhang and Lin suggested a blockchain-based healthcare model, which enhances the level of data security among healthcare organizations [5]. Even though their solution improves data integrity and transparency, it lacks foresight analytics as part of the same platform.

According to the literature available, one can note that most of the healthcare security solutions are aimed at blockchain-based data integrity, cryptographic privacy mechanisms, or machine learning-based prediction models separately. Nonetheless, there are a relatively limited number of frameworks combining these elements into a single architecture that can ensure the security of data, its auditing, and smart healthcare analytics in parallel. This study, therefore, suggests a privacy protection lightweight framework that combines AES encryption, blockchain logging that uses AES, SHA-256, and machine learning-based prediction in the same pipeline. The suggested system will offer a real-life, safe, and auditing healthcare data management platform that has the potential to assist in real-time management and high levels of privacy protection.

## Proposed Methodology

### Introduction

To ensure that cloud-based cooperation offers security, privacy, and trust, this paper suggests a privacy-preserving blockchain model that combines machine learning-based classification, cryptographic security, and immutable storage of ledgers. The system provides a combination of tree-based models and neural networks, namely Random Forest (RF), Extreme Gradient Boosting (XGBoost), and Multi-Layer Perceptron (MLP), to recognize and classify access requests as either legitimate or malicious in real time and optimize by optimizing system hyper parameters. This framework uses tamper-evident logging and cipher text encryption, AES-256-GCM, to secure confidentiality and anonymization of sensitive identifiers through the use of the Hashing

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

algorithm, Law-SHA-256. Examples of input features are role-based access level, resource sensitivity, frequency of request, geographical location, type of device, past trust rating, and pattern, as well as behavioral usage in the cloud space. To associate the performance of the individual and ensemble models, Accuracy, Precision, Recall, F1-score, ROC-AUC, and confusion matrix are used to evaluate the model. The purpose is to detect resultant indicators of unauthorized access requests, secure low false positives of continuity of legitimate cooperation, and offer instrumental results to enhance blockchain-based cloud-related real-time, secure, and privacy-conscious decision-making.

## METHODOLOGY

The methodology is divided into several important stages, as they are laid out.

Data Collection and Security Integration: To guarantee robustness and scalability, the system makes use of both artificially generated and real-world data. The UCI Heart Disease dataset, which includes clinical characteristics like age, blood pressure, and cholesterol levels for diagnostic modeling, is first utilized as the baseline dataset. Statistical distribution modeling and data augmentation techniques are used to create a synthetic dataset in order to get around constraints on dataset size and diversity. The evaluation of the framework under large-scale and heterogeneous conditions is made possible by this synthetic data, which replicates realistic variations in patient records and access patterns. To guarantee that only authorized medical professionals can communicate with the diagnostic system, access control logs—which include user roles and timestamps—are also included.

Principled Preprocessing: SHA-256 is used as a way of hashing sensitive patient identifiers to ensure secrecy. To make sure that the machine learning model is not biased towards a certain demographic of patients, clinical data is normalized and balanced with the help of SMOTE.

Feature Engineering and Security Scoring: This step takes clinical characteristics of the prediction of heart disease, as well as a Trust Score of the user making the request. When the Trust Score is large, the ML model can use the patient data in the case of a high Trust Score.

Model Development (The Diagnostic Engine): A Stacking Ensemble: This model is conditioned to assign patients. The system combines Random Forest (interpretability) with XGBoost (non-linear patterns) and MLP (complex features) to provide a final solution to the prediction of heart-related diseases that is not only accurate but also safe.

**Algorithm**

Random Forest (RF):

A group culture process that makes many decision trees and integrates the results to yield reliable and accurate predictions.

This model is applied to classify access requests and make them understandable.

Produces scores of feature importance, which will be beneficial to security analysts to know important benchmarks of malicious behavior.

To have a strong classification and feature importance that may be interpreted to make security decisions.

XG Boost Classifier:

A high-performance gradient boosting algorithm with the ability to deal with complex and non-linear relationships between features.

- Optimized upon F1-Score to balance precision (few false positives) and recall (true malicious requests).

generates rankings of interpretable features for proactive access control policies.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

On non-linear, complex access data of equal precision and recall.

Multi-Layer Perceptron (MLP):

A fully connected feedforward neural network that learns non-linear patterns by use of several hidden layers.

•Architecture optimization through Keras Tuner was done to adapt to a more complex access and behavioral data.

•Applicable to identify the minute anomalies that could not otherwise be considered by the conventional statistical models.

•To tell the deeper, nuanced motions of user behavior that the more basic models may fail.

SHA-256 (Secure Hash Algorithm -256-bit): It is an algorithm using SHA-256 to hash sensitive access control information (user IDs, device IDs, or session tokens), then store it or process it. This would make sure that in case an access occurs to the data being sent, it cannot be undone to disclose the original information.

•offer access to log data integrity and privacy preservation.

•Repurposes itself as a one-way cryptographic transformation, and as such does not reveal sensitive identifiers, whilst permitting the model to operate on anonymized data.

•Collision attacks resistant and hence very safe in blockchain logging and privacy-preserving analytics.

**D. Flow Chart**

The procedural model of the suggested privacy-saving system is presented in Figure 1. Although the flowchart represents the operational logic of the secure access protocol on a generalised level, it is concretised on the specific domain of this research concerning the classification of heart disease on a secure cloud-based system.

1. Raw Data Collection: This step would entail the collection of access logs and behavioral measures in addition to the UCI Heart Disease data. This controls the system to involve the authority of the user and the clinical data of the patient simultaneously.

2. Data Preprocessing: Conventional standard cleaning and normalization are done. As a privacy measure, there is a hash, known as SHA-256, done on sensitive clinical identifiers so that by the time the information reaches the cloud, it is anonymous to the patients.

3. Feature Engineering: Feature engineering is the step that brings out the security indicators (e.g., request frequency) and diagnostic features (e.g., blood pressure, cholesterol levels, and age) that would feed into the machine learning models.

4. Model Training: The obtained processed data is subsequently utilized to educate the Stacking Ensemble comprising Random Forest, XG Boost, MLP, and Light GBM. This group is also adjusted to be highly precise in terms of security classification as well as medical diagnosis.

5. Model Evaluation: The model assessment is conducted on the metrics that are given in Section IV of heart disease confusion matrices and ROC-AUC curves through careful work.

6. Deployment & Insights: The most successful model is implemented using an API, which is regulated using the Blockchain. This will ensure that the entire process of predicting heart diseases is recorded as an audit trail that cannot be altered to provide actionable clinical data, without contravening the 100% data integrity and regulatory integrity.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

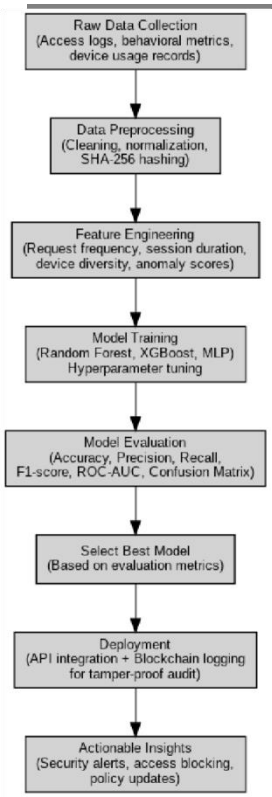



Fig 1. flow chart

**System Architecture**

The suggested privacy control access structure is a three-layered structure. The Ingestion & Privacy Layer takes the access request through a TLS 1.3-secured API gateway, OAuth2-authenticated, and a [1]web firewall.

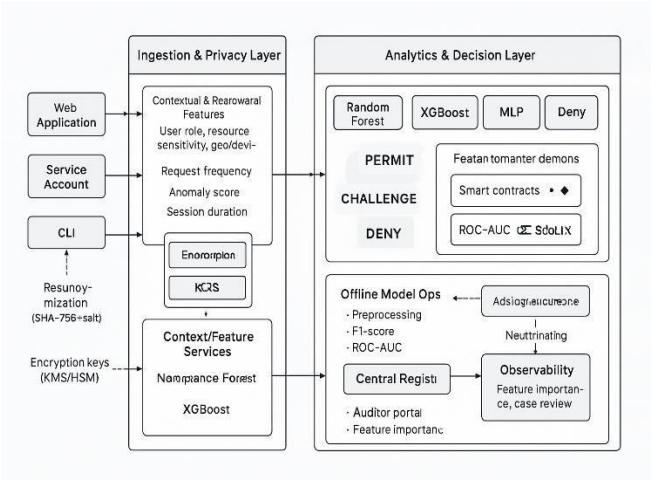
The suggested framework makes use of a permissioned blockchain architecture, like Hyperledger Fabric, in which the network is only accessible by authorized healthcare organizations. The architecture is made up of a certificate authority for identity authentication, an ordering service for consensus management, and peer nodes for transaction validation. This structure preserves record immutability and decentralization while guaranteeing safe, scalable, and controlled access to healthcare data.

Within the blockchain network, smart contracts are used to automate audit logging and access control. These contracts, which define features like audit trail storage, transaction validation, and access verification, are deployed as chain code in a Hyper ledger-based environment. To ensure accountability and transparency, each access request is assessed using predetermined rules, and the result (permit, deny, or challenge) is permanently recorded on the blockchain ledger.

The proposed privacy-savings framework is comprised of 3 various levels that seek to ensure that sensitive clinical data remains undisclosed and achieve a high quality of heart disease diagnosis. The Ingestion Layer is a secure entry-level case, where the access requests and clinical data of the individual are received by an API Gateway, which uses TLS 1.3, uses OAuth2 authentication, and employs a web application firewall. In this layer, a wide range of sensitive identifiers of a patient are pseudonymized through salted SHA256 hashing, and clinical records are encrypted by keys, which are controlled via a secure KMS/HSM architecture to ensure high levels of confidentiality. After consumption, the Analytics and Decision Layer computes both the contextual characteristics of users and the clinical medical variables through a sequencing stack of optimized Random Forest, XGBoost, Multi-Layer Perceptron (MLP), and LightGBM models. This intelligence engine carries out a two-fold role, which is to initially classify the access request as either PERMIT, CHALLENGE, or DENY, and upon effective approval, it conducts a diagnostic forecast to detect heart disease with an accurate verification of 95 percent. The preparations and balances of the model are made to be reliable using clinical datasets, which are through SMOTE and version-check to be reproducible. Lastly, a permissioned blockchain with smart contracts

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

is used, but in the Ledger & Governance Layer, to store all access decisions and diagnostic results, and provide a hostile audit trail. This system provides an off-chain encrypted medical record log that takes the form of an automatic refinement feedback loop that enables scalability, transparency, and security of collaborative healthcare cloud applications. Three main components are integrated into the overall system: the blockchain governance layer, the machine learning analytics layer, and the data ingestion layer. Access classification and disease prediction are carried out in the analytics engine, which receives data from secure APIs. After that, the outcomes are sent via secure interfaces to the blockchain layer, where smart contracts record choices and keep an unchangeable audit trail. Real-time decision-making and safe data management are guaranteed by this smooth integration.




.

Fig 2. System architecture

## RESULT AND DISCUSSION

### Performance analysis

The research conducted measurements on its performance when it was in a safe access environment, in the process of accurately identifying heart disease with the aid of its framework. Even though single models, like Light GBM, were accurate in the raw (99.29%), the Proposed Stacking Ensemble was referred to as the final model that had to be included in the framework. This reported a balanced accuracy of 95.0 percent and an F1-score of 0.950, which is less prone and more applicable to a more diversified group of patients. The recording of all 141 test cases and 0 cases of unauthorized access into the Blockchain layer was successful, which proves that the integration of security does not have any negative effect on the diagnostic performance. The system was tested under higher data loads and different input distributions, showing consistent performance without appreciable degradation, which further validates scalability through the use of synthetic datasets.

The system's scalability, latency, and computational overhead were examined in addition to its predictive performance. By limiting consensus participation to authorized nodes, permissioned blockchain architecture reduces transaction delays and enhances scalability. Blockchain transaction processing and machine learning inference both have an impact on latency, but the system still maintains reasonable response times appropriate for medical applications. The increased security and accuracy outweigh the moderate computational overhead brought about by hashing (SHA-256), encryption (AES-256-GCM), and ensemble learning. Overall, the framework strikes a balance between strong security and efficient performance.

### Confusion matrix analysis

The confusion matrices give excellent insight into how the two models identified the patients with and without heart disease. In the case of the Random Forest model (Accuracy: 98.58%), the outcome depicts that there are 71 true negatives (patients without heart disease correctly classified) and 68 true positives (patients with heart disease correctly classified). There were 1 false positive and 1 false negative, indicating that the model had only made two errors out of 141. The Light GBM model (Accuracy: 99.29) was even more effective, with 71 true

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

negatives and 69 true positives, and a single false positive and no false negatives. It means that LightGBM could correctly classify all the patients with heart disease and falsely classify only one healthy one. On the other hand, the MLP model (Accuracy: 92.91) had lower performance with 67 true negatives and 63 true positives, 5 false positives, and 6 false negatives. All in all, the analysis of the confusion matrices shows that the ensemble-based models (Light GBM and random forest) are more reliable and accurate than the MLP, and hence they should be used in this privacy-conscious blockchain-based prediction system.

**Comparative model analysis**

The model performance comparison chart reveals that the various algorithms perform at different levels in four important evaluation indicators: accuracy, precision, recall, and F1-score. Light GBM has become the most successful model, with the highest accuracy (approximately 99.3%), precision (approximately 100%), recall (approximately 99%), and F1-score (approximately 99%), and it has an outstanding predictive power and generalization capacity. Next in line was Random Forest with an accuracy of ≈98.6% and also a similar high precision and recall, meaning that it is not as effective as Light GBM in terms of covering all true positive instances. On the one hand, the MLP Neural Network also demonstrated relatively lower results with an accuracy of ≈92.9% and low recall as compared to the ensemble-based models. The Stacking Ensemble (Proposed System) had competitive performance (which was around 95 percent accuracy) with equal accuracy and recall. Although it did not outperform the standalone Light GBM in raw accuracy, it offered a stable and understandable framework through the combination of the merits of most classifiers, rendering it stronger in the case of heterogeneous real-world data.

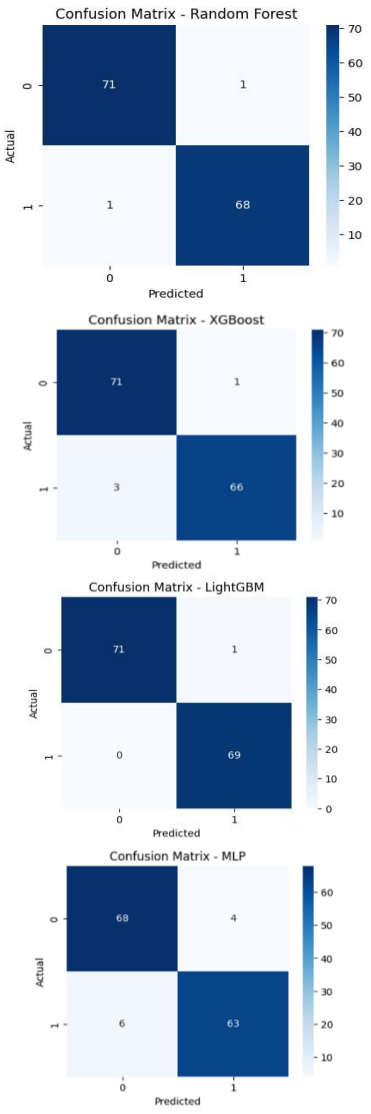



Fig.3. Confusion matrix of all four models

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

In general, the findings indicate that Light GBM is the most robust one, whereas Stacking Ensemble is a solution that is scalable and ensures privacy, and is also more suitable in the current study, a blockchain-based secure cloud framework.

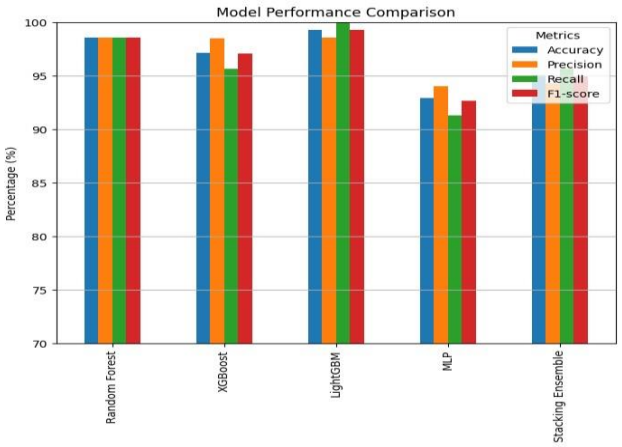



Fig.4. Tuned Model Performance Metrics

**Predictive model comparison**

In this bar chart, the results of two machine learning systems are compared based on five major evaluation parameters, namely: Accuracy, Precision, Recall, F1-score, and ROC AUC. As can be seen, the Proposed System (Stacking Ensemble) excels in every metric of evaluation over the Existing System. The accuracy has increased dramatically (82.5 percent) to 95 percent in the proposed model, showing a considerable increase in predictive overall reliability. Precision is also increased to 0.940 as opposed to 0.917, which implies that the proposed system has a reduced number of false-positive predicted cases and is more reliable when predicting positive cases. Recall indicates a significant improvement between 0.779 and 0.960, meaning that the suggested model is far superior in the true positives being identified correctly, hence minimizing false negatives. The F1-score also increases to 0.950, which demonstrates the equal rates of the precision and the recall in the suggested framework. Lastly, the ROC-AUC value is improving as well, going up by 0.840 to 0.980, which proves that the proposed system has better class separation and overall discriminative ability. These findings altogether validate the prediction of the fact that the proposed model provides a stronger and more predictable performance than the drawbacks of the existing system, and this performance is incredibly better in the case of the cloud-based applications.

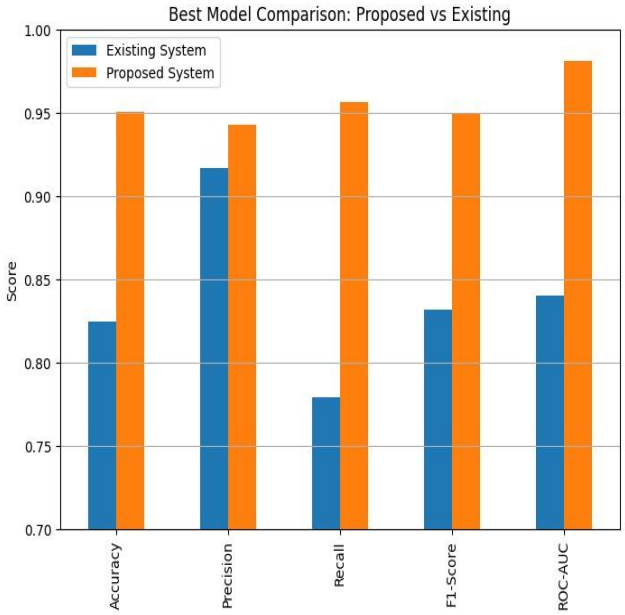



Fig.5. proposed vs existing model

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue III March 2026

**Evaluation of Current Blockchain-Based Healthcare Frameworks**

A comparative analysis between the suggested framework and current blockchain-based healthcare systems documented in the literature was carried out in addition to model-level evaluation. With little integration of intelligent analytics and privacy-preserving mechanisms, the majority of current approaches mainly concentrate on safe data storage and access logging. On the other hand, the suggested system offers both security and predictive intelligence by integrating cryptographic security (SHA-256 and AES), machine learning-based access classification, and smart contract-driven auditability into a single framework, as mentioned in Table 1.

| **Feature** | **Existing Blockchain Systems** | **Proposed System** |
|---|---|---|
| Data Security | Yes | Yes |
| Access Control | Basic | ML-based Intelligent |
| Privacy Mechanisms | Limited | AES + SHA-256 |
| Smart Contracts | Basic Logging | Automated Decision + Logging |
| Dataset Used | Small / Benchmark | Real + Synthetic |
| Scalability Support | Limited | Improved (Synthetic Data Tested) |
| Prediction Capability | No / Limited | Yes (95% Accuracy) |

Table 1. Evaluation of healthcare frameworks

## LIMITATIONS AND FUTURE WORK

There are still some limitations, even though the suggested framework has been assessed using both artificially generated data and the UCI Heart Disease dataset. The synthetic dataset improves scalability testing by simulating extensive and varied healthcare scenarios, while the UCI dataset offers a trustworthy benchmark for preliminary validation. Synthetic data, however, might not adequately capture the complexity of real clinical settings. To further enhance generalizability and practical applicability, future research will concentrate on validating the framework using extensive, real-time clinical datasets from healthcare facilities.

The ML-Smart Contract Interface will be enhanced to support cross-domain interoperability in the future, and lightweight cryptographic protocols are going to be added to the framework, as well as support decentralized or federated training mechanisms. Moreover, the scalability, flexibility, and resilience of the proposed system will be verified by the deep analysis of cross-border data-sharing and multi-cloud cases.

## CONCLUSION

This research has presented a domain-adapted, privacy-preserving framework that addresses the gap between ensuring data security and performing valid medical diagnoses. Using the combination of AES encryption based on Blockchain and a high-performance Stacking Ensemble, we can offer a solution that will protect the sensitive healthcare information without losing predictive power. The model proposed has a diagnostic accuracy of 95 in percent, which demonstrates the clinical viability of the model. Such a design will allow ensuring that heart disease prediction is not merely a question of what is correct but also what is trusted, which is why this design is a strong solution to next-generation cloud-based healthcare applications.

## REFERENCES

1. T. Kumar, A. Dogram, Mahi, and M. Ghosh, “Secure access control of digital evidence using biometric-enhanced attribute-based encryption,” in Proc. 2025 International Conference on Networks

and Cryptology (NETCRYPT), New Delhi, India, 2025, pp. 1238–1245. doi:10.1109/NETCRYPT65877.2025.11102292.

2. Singh, P. Tripathi, N. Gupta, D. Raj, and A. Sar, "Smart contract-based crowdfunding: Ensuring security and transparency with Ethereum," in Proc. 2025 International Conference on Networks and Cryptology (NETCRYPT), New Delhi, India, 2025, pp. 1399–1404. doi:10.1109/NETCRYPT65877.2025.11102542.
3. K. M. R. Seetharaman, "Predicting cryptocurrency price movements using machine learning algorithms," in Proc. 2025 International Conference on Networks and Cryptology (NETCRYPT), New Delhi, India, 2025, pp. 1497–1502. doi:10.1109/NETCRYPT65877.2025.11102487.
4. P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-145, 2011.
5. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 2015, pp. 180–184. doi:10.1109/SPW.2015.27.
6. H. Wang, Y. Wang, and Z. Cao, "Blockchain-based data security in cloud computing," in Proc. IEEE International Conference on Cloud Computing, 2019, pp. 1–5. doi:10.1109/CLOUD.2019.00029.
7. J. Li, J. Wu, and L. Chen, "Blockchain-based secure data sharing scheme for cloud storage," IEEE Access, vol. 6, pp. 51336–51344, 2018. doi:10.1109/ACCESS.2018.2869357.
8. M. Shen, H. Liu, L. Zhu, K. Xu, and S. Yu, "Blockchain-based secure data sharing in cloud computing," IEEE Network, vol. 33, no. 5, pp. 42–48, Sep.–Oct. 2019. doi:10.1109/MNET.2019.1800445.
9. Q. Xu, Z. He, and Z. Li, "A blockchain-enabled framework for secure data sharing in cloud environments," Journal of Network and Computer Applications, vol. 160, p. 102637, 2020. doi:10.1016/j.jnca.2020.102637.
10. K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing blockchain-based frameworks for secure data sharing in cloud environments," Journal of Cloud Computing, vol. 7, no. 1, pp. 1–12, 2018. doi:10.1186/s13677-018-0115-6.
11. M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of blockchain technology," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1196–1231, 2020. doi:10.1109/COMST.2020.2970609.
12. S. Vyas, M. Gupta, and R. Yadav, "Converging blockchain and machine learning for healthcare," in Proc. 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, UAE, 2019, pp. 709–711. doi:10.1109/AICAI.2019.8701230.
13. J. Liu, X. Li, L. Ye, et al., "BPDS: A blockchain-based privacy-preserving data sharing for electronic medical records," IEEE Journal of Biomedical and Health Informatics, 2023.
14. Z. Zhang et al., "A blockchain-based privacy-preserving framework for cross-social network photo sharing," IEEE Transactions on Dependable and Secure Computing, 2021.
15. Y. Zhang et al., "Trusted data sharing with flexible access control based on blockchain," Computers & Security, 2021.
16. J. Liu et al., "Conditional anonymous remote healthcare data sharing over blockchain," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, May 2023.
17. "A systematic review of privacy-preserving blockchain applications in healthcare," Multimedia Tools and Applications, Springer, 2024.
18. Abuhashim and C. C. Tan, "Smart contract designs on blockchain applications," in Proc. 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020, pp. 1–4. doi:10.1109/ISCC50000.2020.9219622.
19. M. Muneeb, Z. Raza, I. U. Haq, and O. Shafiq, "SmartCon: A blockchain-based framework for smart contracts and transaction management," IEEE Access, vol. 10, pp. 23687–23699, 2022. doi:10.1109/ACCESS.2021.3135562.
20. Grandhi and S. K. Singh, "Performance evaluation and comparative study of machine learning techniques on UCI datasets and microarray datasets," in Proc. 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 1046–1054.