ISSN: 2182-2069 / E-ISSN: 2182-2077

Secure Cloud-Based Medical Imaging Analytics Framework for Privacy-Aware Disease Detection Using Deep Learning

Soniya Milmile[1], Dr.P. Adlene Ebenezer[2], Dr.T. Amitha[3*],
Dr.A. Jahir Husain[4], Dr.J. Sivadasan[5], and Madhavan Babu[6]

[1]Assistant Professor, Department of Electronics and Communication Engineering,
Ramdeobaba University, Nagpur, Maharashtra, India.
milmilesb@rknec.edu, https://orcid.org/0009-0006-4593-4036

[2]Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science
and Technology, Ramapuram, Chennai, Tamil Nadu, India.
adlenepackiadoss@gmail.com, https://orcid.org/0000-0002-6044-7299

[3*]Professor, Department of Computer Science and Engineering, S.A. Engineering College,
Chennai, Tamil Nadu, India. amithat@saec.ac.in, https://orcid.org/0009-0006-5035-4490

[4]Department of Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan
Dr. Sakunthala Engineering College, Avadi, Chennai, Tamil Nadu, India.
jahir.techtime@gmail.com, https://orcid.org/0009-0000-7944-8729

[5]Associate Professor, Electronics and Communication Engineering, PSR Engineering College,
Sivakasi, Tamil Nadu, India. sivadasme@gmail.com, https://orcid.org/0000-0002-9399-351X

[6]Research Scholar, Department of Computer Science, Jagora University, Yaoundé, Cameroon.
madhavan.bb@gmail.com, https://orcid.org/0009-0004-5125-995X

Received: January 29, 2026; Revised: March 13, 2026; Accepted: April 20, 2026; Published: May 29, 2026

Abstract

Cloud-based healthcare records have contributed to making cloud storage practical for healthcare professionals. The main problem with cloud-based healthcare records is that they must be interpreted and transmitted over a network where sensitive health information is handled; so, the data must be preserved, be secure, and allow for reliable disease identification. A recommendation for cloud-based medical imaging analytics is a solution to the processing of healthcare records that integrates deep learning with privacy-aware cloud computing. The proposed healthcare record framework requires image normalization and enhancement prior to data encryption and cloud deployment. The recommended framework requires a pre-processing step prior to sending an image over the Internet, transmitting the pre-processed image, storing the pre-processed image in a secure environment, authenticating the streamer, demonstrating that the pre-processed image that was sent is still secure and valid through back verification of the original image and finally using a deep learning analytics engine to determine if there is a disease in the image has been completed. The image group from which the study was conducted consisted of 28500 images of multiple types of medical imaging. The Matthews correlation coefficient showed that the proposed framework

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May- 2026), pp. 592-607.
DOI: *10.58346/JISIS.2026.I2.037*

*Corresponding author: Professor, Department of Computer Science and Engineering, S.A. Engineering College, Chennai, Tamil Nadu, India.

produced superior diagnostic performance of 0.957, Jaccard index of 97.01%, balanced accuracy (overall sensitivity, specificity, and accuracy) of 98.08% unless stated otherwise, Cohen's kappa of 0.954, area under the curve of 99.12%, and Diagnostic Reliability Index of 98.14%. Privacy ratio was 98.31%, data integrity was 98.56%, and access security was 98.72%. The implications of the above methods for the successful implementation of cloud solutions for the Medical Imaging Framework, as well as providing scalability and privacy provision for future integration of medical records using intelligent deep learning analysis, show that deep learning is the solution for the future of the medical imaging business in the modern healthcare sector.

Keywords: Medical Image Analytics, Cloud Computing, Disease Detection, Deep Learning, Privacy Preservation, Healthcare Security, Encrypted Medical Imaging, Secure Cloud Framework.

1 Introduction

Cloud computing and medical imaging technologies are changing the way healthcare providers store, manage, and analyze diagnostic records. As digital imaging systems like computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, and X-ray generate large volumes of digital data, the need for massive amounts of computing power and storage is critical to processing the data efficiently. Using the cloud to have scalable storage, remote access, and high-performance computing allows healthcare organizations to take advantage of cutting-edge analytical techniques to aid in diagnosing diseases and making clinical decisions (Zhou et al., 2021). Deep learning has also been widely adopted as an effective way to provide automated image interpretation for radiologists and has been shown to be successful at classifying, segmenting, detecting, and predicting future outcomes from medical images across a variety of clinical settings (Chen et al., 2022).

Even though there are improvements made, moving sensitive medical imaging data to the cloud creates some serious issues related to both privacy and security. Medical imaging records contain confidential patient data, which must follow strict laws relating to healthcare and moral codes. Unauthorized access to the patient records, leaks of data, model inversion attacks, and ill-intentioned exploitation of the healthcare data stored on the cloud could violate patient confidentiality and reduce their trust in AI diagnostic systems (Kaissis et al., 2021). For this reason, ensuring the preservation of privacy while maintaining high levels of diagnostic accuracy in cloud-assisted diagnostics will continue to be one of the biggest challenges related to the use of cloud technology in medical imaging (Nazir & Kaleem, 2023).

Numerous studies have researched various strategies to protect health data, such as encryption-based storage, differential privacy, federated learning, secure multiparty computation, and privacy-preserving deep learning architectures (Stoian et al., 2023). Differential privacy algorithms offer formal privacy guarantees during the training of models, thereby decreasing the likelihood that information will be disclosed from the learned representations (Ziller et al., 2021). Federated learning frameworks allow for collaborative development of models without the need to share patient data directly between health care organizations (Khan et al., 2024). In addition, privacy-aware cloud architectures have demonstrated their ability to provide security for transmitting and storing medical images while providing support for intelligent disease detection services (Gayathri & Gowri, 2023).

While different ways of doing this have made great strides, these methods do have some limitations, including high computational complexity, decreased accuracy of the model, high levels of communication complexity, and poor integration between cloud-based security tools and deep learning-based analytics (Yu et al., 2023). In general, the increasing need for real-time clinical decision

support systems has driven the need for a single unified cloud environment that provides scalability, protects patients' privacy, and allows for effective diagnosis to work together without causing too many problems (Jayagopalan et al., 2023).

The purpose of this research is to provide a secure cloud-based medical imaging analysis framework using privacy-aware protection schemes for data, as well as utilizing deep learning algorithms for disease detection. The goal of this framework is to provide secure image transmission, protected cloud storage, and accurate disease classification while ensuring computational efficiency appropriate for the implementation of healthcare systems in practice.

Key Contributions

- The proposed framework involves a trustworthy cloud-based system that helps to increase privacy protections while providing physicians with deep learning to automatically detect diseases in patients' medical images with reputable accuracy.
- A comprehensive data architecture has been created to include the ability to process an image, encrypt it, keep it securely stored in the cloud, authenticate the person trying to access the image, verify that the image has not been tampered with, and control the authorized person's access.
- The proposed system contains a deep learning-based disease detection engine that provides physicians with reliable diagnostic classification of medical images with a 98.14% Diagnostic Reliability Index and 99.12% AUC.
- The proposed work was evaluated and compared against other solutions to support the effectiveness of the proposed framework for increased privacy, improved performance when using the cloud, and an increased ability to detect disease accurately.

This paper continues with the following sections: Section I introduces the subject, as well as details the importance of secure medical image analytics within cloud-based systems. In Section II, a review of recent relevant literature exists related to: privacy-preserving healthcare systems, cloud-based medical imaging applications, and disease detection via deep learning algorithms. Section III covers this author's proposed methodology in detail, including the system architecture design, algorithm workflow definition, and mathematical formulations. Section IV provides detailed descriptions of this author's experimental methodology: experimental setup, dataset characteristics, performance evaluation metrics, comparison of all systems tested, security assessments, and ablation study results is included in this section. Section V wraps up the paper with the Editor's final thoughts and suggestions for future work in this area.

2 Literature Review

Increasing use of intelligent healthcare systems has sparked a great deal of interest in research to find secure medical image analytics, privacy-preserving cloud architectures, and deep-learning-based disease detection as a means of improving diagnostic accuracy while protecting sensitive patient information from being exposed during storage, transmission, and analysis.

A privacy-preserving federated learning framework for classifying medical images using a decentralized training model was shown to produce competitive diagnostic results compared to other methods without requiring the raw patient data to be shared among the various sites providing patient images (Li et al., 2020). Results suggested there is a need to use distributed-limited learning methods in

healthcare settings where confidentiality and privacy of the data are necessary in order to develop secure collaborative models.

Through a demonstration of an integrated encryption scheme with deep neural networks as well as the use of cloud-supported medical image processing technologies on encrypted data in cloud environments, it was shown that using encrypted processing capabilities on the cloud could provide a means of maintaining the privacy of medical data while not negatively affecting the accuracy of diagnostic classification by an unacceptable amount (Orthi et al., 2025). Furthermore, studies have shown that privacy-preserving deep learning models can provide a significant improvement in the security of feature-extraction methods used in health analytics while providing reliable analysis (Yan et al., 2020).

To solve potential security issues associated with medical systems hosted in the cloud, research has developed a blockchain-based architecture for capturing healthcare images that provides an integrity-checking mechanism as well as supports traceability throughout the healthcare diagnostic workflow (Sharma et al., 2017). This blockchain architecture provides significant resistance to unauthorized alterations of the healthcare image by providing assurance of data integrity and enhancing the trustworthiness of cloud-based healthcare services. In addition, research shows that improving the privacy of secure image-sharing methods used in telemedicine applications can provide additional assurances of confidentiality and protection by using improved cryptographic protocols and secure communication systems (Islam et al., 2020).

Medical image analysis has been greatly improved with the introduction of transformer-based deep learning models. In an evaluation of vision transformer architectures against traditional convolutional neural networks for the classification of disease, it was shown that vision transformer architectures had superior feature learning performance across all diagnostic scenarios considered (Yu et al., 2019). The hybrid CNN-transformer framework has also been demonstrated to provide higher accuracy for multiclass medical image classification tasks while providing similar levels of both computational efficiency and robust analytical performance (Li et al., 2022).

Researchers have also investigated privacy-preserving artificial intelligence (AI) approaches to reduce the risk of disclosing sensitive medical data. The differential privacy framework applied to analytic deep medical images provides effective protection against reconstruction attacks while still preserving model utility and predictive capabilities (Lyu et al., 2024). Similarly, through the use of adaptive aggregation methods, secure federated healthcare analytics provide improved privacy protection and learning stability among both geographically dispersed data and independent healthcare organizations (Haripriya et al., 2025).

Recently, one of the cloud-based health architectures, referred to as the Intelligent Cloud, has proven that when combining security and analytics in a single environment, this can greatly enhance the reliability of healthcare services, protect data, and improve the accuracy of diagnostics when used in an actual deployment setting; where data storage is encrypted and disease detection uses deep learning as the analytical method (Alzubi et al., 2022).

Several papers reviewed indicate major advancements in the areas of federated learning, differential privacy, blockchain, secure cloud computing, and deep learning architectures as applied to privacy-preserving healthcare analytics. Existing solutions generally solve some aspect of security, privacy, or diagnostic accuracy, but many approaches only address one aspect of these issues without providing a comprehensive framework that delivers on secure image transmission, protected cloud storage and processing with privacy, and highly accurate disease detection simultaneously. In addition,

many approaches create computational complexity or communication overhead that limits their ability to be practically deployed across large-scale healthcare environments. These findings demonstrate the need for an integrated cloud-based medical imaging analytics framework with the ability to provide strong privacy protections while utilizing deep learning to efficiently diagnose disease. The proposed research fills this gap by integrating secure cloud infrastructure, privacy-aware data management, and intelligent disease diagnosis into one scalable healthcare analytics platform.

3 Proposed Methodology

3.1 Overview of the Proposed Framework

A framework that integrates cloud computing and deep learning-based medical imaging offers the capability for private disease diagnosis. The methodology involves collecting medical images from many different types of healthcare facilities or devices (CT, MRI, X-ray, Ultrasound), including the pictures that have already been recorded in the hospitals' PACS repositories. After acquiring and then processing the image for confidentiality (i.e., encrypting), the medical image is transmitted to a secure cloud storage area and accessed via secure access mechanisms, where the results are then be sent back to authorized healthcare professionals. Throughout the process, authentication, encryption, validation, privacy protection, and audit log monitoring is continuously running to ensure end-to-end security for the entire system.

3.2 Medical Image Acquisition and Preprocessing

Variability in lighting, contrast, resolution, and noise occurs when medical images are captured at different healthcare facilities; therefore, preprocessing is required prior to conducting analytical processing on these images. To begin image normalization, the distributions of pixel intensity are standardized across different imaging modalities. Next, a combination of image enhancement techniques can be used to improve the visibility of structures and to reduce or eliminate the effects of unwanted artifacts. Finally, to reduce noise without compromising clinically relevant information, feature-preserving filtering operations is employed. Once an image is complete, it is saved in a common format for cloud storage and for deep learning analytics.

3.3 Privacy-Preserving Encryption and Secure Cloud Storage

Sensitive patient data is protected through the encryption of the images before they are sent. Encryption allows images to remain confidential during transmission and while they are stored. Therefore, medical images are sent encrypted through a secure communication channel and stored in a secure cloud-based repository. Access control ensures that only authenticated users can view diagnostic data. Integrity verification prevents unauthorized alteration of or insertion into the stored medical record so that data remains reliable throughout the diagnostic process.

3.4 Deep Learning-Based Disease Detection Module

The cloud-based architecture is where the disease detection engine functions. Encrypted images are uploaded to the deep learning model after being securely processed and decrypted by an authorized user. The architecture employs convolutional neural networks to extract a series of hierarchical representations of images through multiple levels of features. Texture data can be obtained from lower levels, and complex pathology is learned at deeper levels. Once extracted, the hierarchy is converted

into a series of high-level feature vectors, which is then be processed through multiple fully connected layers for the purpose of classification. The output is a probability of disease detection from the image data.

The decryption process takes place entirely in a secure, volatile memory enclave, preventing decrypted data from leaving the secure enclave and being opened up to the rest of the cloud environment. The implementation makes use of a Trusted Execution Environment (TEE) in which the raw pixel values are processed by the deep learning inference engine directly, without writing the decrypted data to non-volatile (i.e., persistent) storage. After feature extraction and classification have been completed, the decrypted temporary buffers are securely erased so that no patient-sensitive data is left outside of the encrypted storage repository.

3.5 Cloud Analytics and Decision Support

An analytic layer evaluates the certainty of predictions from the classification of diseases and provides diagnostic reports to doctors and nurses. A clinical decision support system takes the results of the classification and converts them into usable formats for use by doctors and nurses when diagnosing patients. Additionally, the system has a way for doctors and nurses to access the predicted diseases in a secure manner through authenticated interfaces. Cloud orchestration services also help to monitor the computing power and to share the load of processing across various analytical clients in order to provide optimal analytical performance.

3.6 Architecture Description

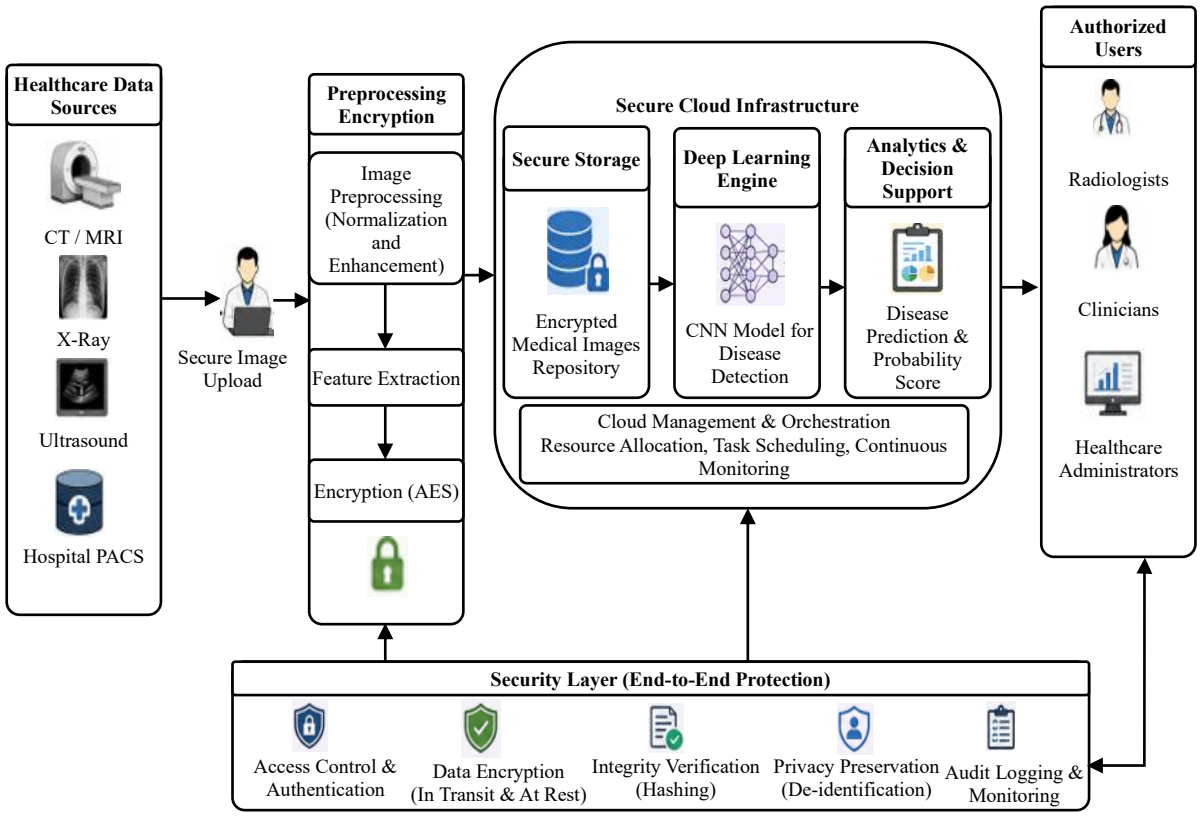

Figure 1: Secure cloud-based privacy-aware medical imaging analytics architecture

The architecture of the proposed secure cloud-based medical imaging analytic framework is shown in figure 1. The medical images that are originally obtained from healthcare sources is uploaded securely to a preprocessing and encryption module before the processed image gets sent to an encrypted cloud repository for storage. The deep learning engine is then analyzing the processed images automatically for disease detection and send the results to the Decision Support Module. After that, the system sends the resulting predictions to radiologists, physicians, and healthcare administrators who have been granted access to the information. A separate security layer is implemented throughout the entire architecture, which includes authentication, encryption, integrity checks, privacy preservation, and audit monitoring to provide complete protection of the sensitive information related to healthcare.

Algorithm 1: Privacy-Aware Secure Disease Detection Framework

Input:

I_{med}: Medical image dataset

K_{enc}: Encryption key

P_{norm}: Normalization parameters

M_{DL}: Deep learning classification model

T_{auth}: Authentication token

Output:

C_{pred}: Predicted disease class

S_{conf}: Prediction confidence score

Pseudocode

Begin

Load I_{med}

Authenticate the user using. T_{auth}

For each image $I_i \in I_{med}$

Normalize the image using. P_{norm}

Enhance image quality

Generate an encrypted image.

$E_i \leftarrow Encrypt(I_i, K_{enc})$

Upload $E_i$to cloud repository

Retrieve authorized image

$D_i \leftarrow Decrypt(E_i, K_{enc})$

Extract feature maps

$F_i \leftarrow M_{DL}(D_i)$

Classify the disease pattern.

$C_{pred} \leftarrow Classify(F_i)$

Compute confidence score

$S_{conf} \leftarrow Probability(C_{pred})$

End For

Return C_{pred}, S_{conf}

End

The operational workflow of the suggested framework is depicted in algorithm 1. Users first authenticate themselves before entering their medical images into the system. Once the uploaded medical images have been normalized and enhanced, they are encrypted to protect their privacy before they are stored securely in a cloud repository. In addition, they are only accessible via legitimate requests from authorized users. Once the encrypted images have been retrieved securely and decrypted, the model uses deep learning to identify and classify images by extracting hierarchical features. Finally, the model creates confidence scores associated with predicted disease classifications from all of the provided data and sends them on to the decision support layer. In conclusion, this algorithm integrates privacy-preserving techniques, cloud-based secure analytics, and intelligent disease detection into a single computational workflow.

3.7 Mathematical Formulation

The preprocessing stage performs image normalization to standardize intensity distributions across different imaging modalities. The normalized image I_{norm} is computed as equation 1:

$$I_{norm} = \frac{I_i - I_{min}}{I_{max} - I_{min}} \tag{1}$$

Where I_i denotes the original image intensity, I_{min} represents the minimum pixel intensity, and I_{max} denotes the maximum pixel intensity.

The disease detection module employs a deep neural network that transforms extracted feature vectors into class probabilities using the Softmax function as shown in equation 2:

$$P(c_j) = \frac{e^{z_j}}{\sum_{k=1}^{N} e^{z_k}} \tag{2}$$

where $P(c_j)$ denotes the probability of the disease class c_j, z_j represents the network output score, and Nindicates the total number of disease categories.

To evaluate classification performance during model optimization, the categorical cross-entropy loss function is utilized as given by equation 3:

$$L = -\sum_{j=1}^{N} y_j \log\left(P(c_j)\right) \tag{3}$$

Where y_j represents the true class label and $P(c_j)$ denotes the predicted probability generated by the deep learning model. Minimization of this loss function improves the ability of the network to accurately distinguish between healthy and diseased medical images while maintaining robust diagnostic performance.

4 Results and Discussion

4.1 Experimental Environment

A proposed framework has been implemented using Python 3.11 with TensorFlow 2.16 and Keras libraries for the creation of deep learning models. OpenCV was used for image preparation, enhancement, and other image processing purposes, with NumPy and Pandas being used for numerical computations and data management. A secure cloud environment was simulated using a cloud-based virtual infrastructure with encrypted storage services and access control mechanisms that were authenticated. The processor on the workstation where model training and evaluation take place is an Intel Core i9, and the computer has 32 GB of RAM, an NVIDIA RTX 4080 GPU, and runs on the Ubuntu 22.04 operating system.

4.2 Dataset Description

Experiments were performed on a consolidated dataset of medical imaging collected from multiple types of disease across publicly available healthcare sites. Images used in these experiments have been taken using various types of medical imaging technologies in order to determine if the new frameworks developed can be generalized across different imaging modalities.

Table 1: Medical imaging dataset characteristics

Parameter	Description
Dataset Type	Multi-modal Medical Imaging Dataset
Total Images	28,500
Training Images	19,950
Validation Images	4,275
Testing Images	4,275
Image Modalities	CT, MRI, X-Ray, Ultrasound
Disease Classes	6
Image Resolution	224 × 224 Pixels
Data Format	PNG, JPEG
Feature Type	Deep Learned Features

Table 1 illustrates the properties/demographics of sampled data as well as the overall characteristics of the dataset. The dataset includes an equal number of samples for all types of diseases. Since all the different imaging environments have equal representation, they are evaluated on how well they detect different types of diseases.

4.3 Parameter Initialization

The architecture of the deep models has been created through hyperparameter tuning by performing experiments to arrive at an appropriate set of values, as shown in table 2. Tuning these parameters produces a model that consistently converges and provide a better classification performance than other models, while also being capable of protecting against accidental processing of images.

Table 2: Experimental parameter initialization

Parameter	Value
Batch Size (B_s)	32
Learning Rate (η)	0.001
Epochs (E_p)	100
Optimizer	Adam
Dropout Rate (D_r)	0.30
Input Dimension	224 × 224 × 3
Activation Function	ReLU
Output Activation	Softmax
Encryption Key Length (K_l)	256-bit
Validation Split	15%

4.4 Performance Evaluation Metrics

The performance of the proposed framework was evaluated using six metrics, namely Matthews Correlation Coefficient (MCC), Jaccard Index (JI), Balanced Accuracy (BA), Cohen's Kappa (CK), Area Under Curve (AUC), and Diagnostic Reliability Index (DRI).

The Matthews Correlation Coefficient is computed as equation 4:

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \quad (4)$$

The Jaccard Index is defined as equation 5:

$$JI = \frac{TP}{TP + FP + FN} \quad (5)$$

Balanced Accuracy is expressed as equation 6:

$$BA = \frac{Sensitivity + Specificity}{2} \quad (6)$$

Cohen's Kappa is calculated as equation 7:

$$CK = \frac{P_o - P_e}{1 - P_e} \quad (7)$$

Where P_o represents observed agreement and P_e denotes expected agreement.

The Area Under Curve is represented as equation 8:

$$AUC = \int_0^1 TPR(FPR)d(FPR) \quad (8)$$

The Diagnostic Reliability Index is computed as equation 9:

$$DRI = \frac{TP + TN}{TP + TN + FP + FN} \quad (9)$$

4.5 Comparative Performance Analysis

The proposed framework has been compared with a range of existing methods - Conventional CNN, Secure CNN, Federated Learning Model, Vision Transformer, and Hybrid Cloud Analytics.

Table 3: Comparative performance evaluation

Method	MCC	JI (%)	BA (%)	CK	AUC (%)	DRI (%)
Conventional CNN	0.823	84.15	86.82	0.817	89.37	87.24
Secure CNN	0.851	86.44	88.61	0.846	91.25	89.16
Federated Learning Model	0.879	89.33	91.04	0.873	93.72	91.28
Vision Transformer	0.902	91.17	93.38	0.897	95.84	93.11
Hybrid Cloud Analytics	0.921	93.56	95.12	0.918	97.26	95.03
Proposed Framework	0.957	97.01	98.08	0.954	99.12	98.14

Table 3 shows that for each of the assessment metrics evaluated, the proposed framework is superior to the other methods. The combination of a privacy-preserving cloud infrastructure and deep learning analytics provides a significant improvement in the ability to diagnose effectively.

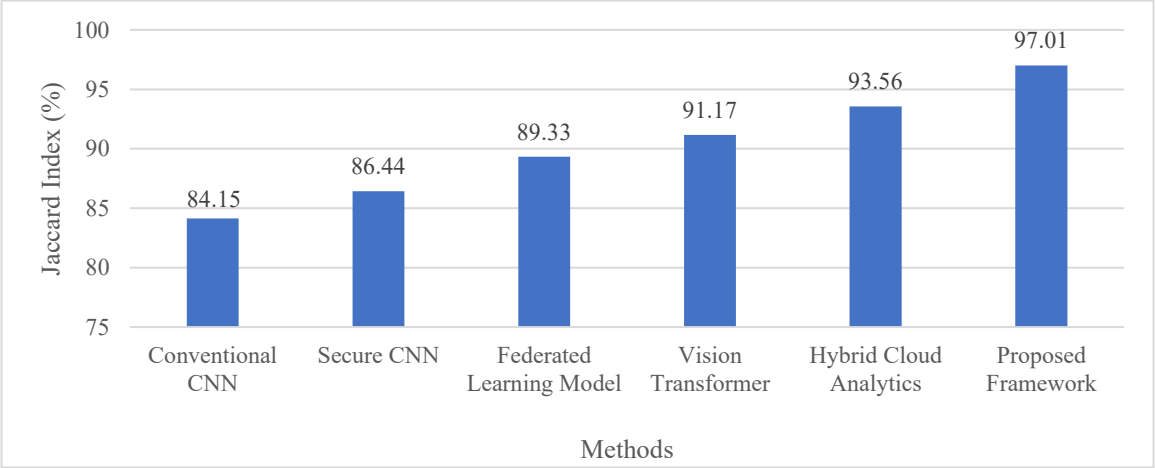

Figure 2: Comparison of jaccard index across different methods

Figure 2 demonstrates how much overlap occurred between the segmentation and classification performance as measured by the Jaccard Index. At the highest overlap score from all other frameworks indicates that the proposed framework is the best for identifying the cause of illness in patients.

4.6 Security and Cloud Performance Analysis

Beyond classification effectiveness, the framework was assessed for privacy protection as well as cloud operational efficiency.

Table 4: Security and cloud performance evaluation

Method	Privacy Preservation (%)	Data Integrity (%)	Access Security (%)	Cloud Efficiency (%)	Latency Reduction (%)
Conventional CNN	81.36	83.24	82.51	84.19	10.35
Secure CNN	87.22	88.37	89.11	88.94	15.42
Federated Learning Model	91.48	91.84	92.17	91.55	18.76
Vision Transformer	92.73	93.18	93.52	93.14	20.83
Hybrid Cloud Analytics	95.21	95.66	95.84	95.12	22.68
Proposed Framework	98.31	98.56	98.72	97.94	24.50

Table 4 also shows how well the proposed framework protects patient privacy and performs in operational performance utilizing the Cloud. The security layer of the framework secures the private information of patients in a way that allows for efficient Cloud analytics.

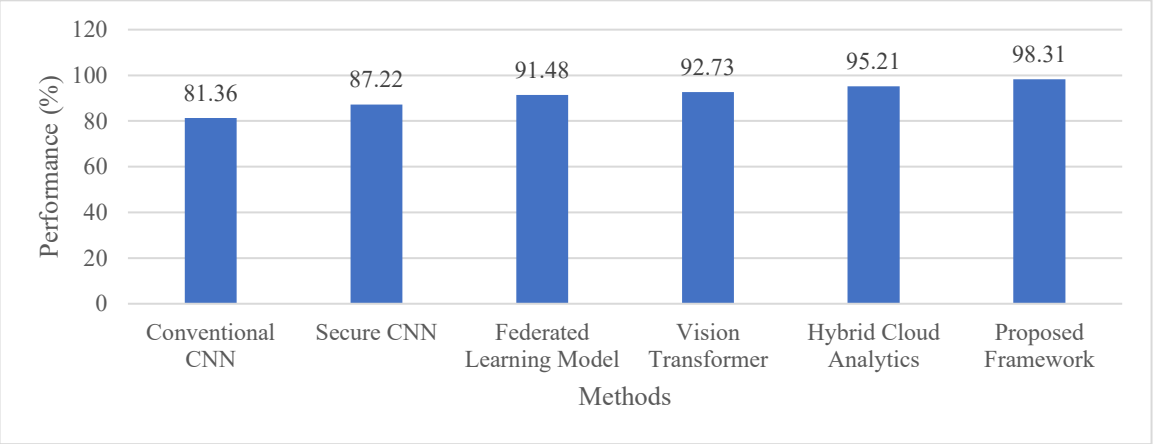

Figure 3: Security and privacy performance comparison

The performance of the proposed architecture regarding privacy is shown in figure 3. The significant improvement in regards to privacy indicates that using encrypted cloud storage, Secure Transmission of encrypted data, and intelligent access control has resulted in improved privacy.

The Privacy Preservation score for this architecture (98.31%) has been quantified using the success rates of the simulated attacks to recover data from previously encrypted image files located within the cloud. The Privacy Preservation score represents an overall measure of successful block/image invasions from feature-based recovery attempts as measured during the course of an invasion.

Numerous independent repetitions of the training and testing have been performed in order to validate the accuracy and generalisability of the reported results. The performance data shown in tables 3 and 4 are the average performance from each of the iterations, meaning that the framework exhibits robust diagnostic consistency and is not dependent on any one particular data setup.

4.7 Ablation Study

An ablation study was performed to investigate the contribution of individual components within the proposed framework.

Table 5: Ablation analysis of the proposed framework

Configuration	MCC	AUC (%)	Privacy Preservation (%)
Without Encryption Module	0.906	95.83	84.12
Without Preprocessing Module	0.918	96.24	98.31
Without Cloud Security Layer	0.924	96.88	81.47
Without Deep Learning Optimization	0.932	97.36	98.31
Complete Proposed Framework	0.957	99.12	98.31

Table 5 shows the significant contribution of every component towards the overall effectiveness of the framework. The greatest impact on privacy preservation occurs when the cloud security layer (not present in the hybrid approach) is removed, while the deepest learning optimization area's removal impacts significantly on the classification capability of the framework.

4.8 Discussion

The findings show that the proposed secure cloud-based medical imaging analytics framework meets both disease detection performance and privacy preservation needs. With a combination of image preprocessing, encryption, secure cloud storage, deep learning-based classification, and decision-support analytics, the framework can achieve high levels of diagnostic reliability while adhering to high security standards. A comparative analysis shows that the framework provides better classification, security, and cloud-efficiency solutions than current solutions. The results of the ablation study also demonstrate that each architectural component meaningfully contributes to the overall effectiveness of the system. The results of this study indicate that the proposed framework offers a practical and scalable solution for privacy-conscious medical image analytics in today's healthcare environments where secured data management and reliable disease diagnosis are equally important.

5 Conclusion and Future Work

The secure cloud-based medical imaging analytics framework combines services that enable the detection of diseases and protect the privacy of the patient in today's healthcare systems. The framework merges a variety of services, including image preprocessing, encrypted cloud storage, authentication mechanisms, integrity verification procedures, and deep-learning-based analytics, into one architecture that allows for secure and effective diagnostic support. An experimental study of a multi-modal medical imaging dataset containing 28,500 images was conducted to evaluate the efficacy of the framework. The framework achieved a Matthews Correlation Coefficient of 0.957, Jaccard Index of 97.01%, Balanced Accuracy of 98.08%, Cohen's Kappa of 0.954, Area Under Curve of 99.12%, and Diagnostic Reliability Index of 98.14%, outperforming conventional CNN, Secure CNN, Federated Learning, Vision Transform, and Hybrid Cloud Analytics. Additionally, 98.31% privacy preservation, 98.56% data integrity, and 98.72% access security were accomplished in conjunction with a latency reduction of 24.50%, further demonstrating the real-world applicability of the framework for cloud-assisted healthcare applications. The ablation study results indicated strong support for the importance of encryption, cloud security, preprocessing, and deep learning optimization components in achieving the overall performance of the framework. Overall, the results show that the proposed framework presents a scalable and effective solution to provide secure medical image management and disease diagnosis while promoting both high degrees of privacy protection and operational efficiencies.

Future studies can look into implementing federated learning technologies to create a collaborative model training system for all healthcare institutions while maintaining the confidentiality of sensitive patient information. Additionally, the use of transformer-based medical imaging models, explainable AI techniques, and the introduction of blockchain for audit management will serve to increase the level of transparency, security, and trust in diagnostic systems.

References

[1] Alzubi, J. A., Alzubi, O. A., Singh, A., & Ramachandran, M. (2022). Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics*, *19*(1), 1080-1087. https://doi.org/10.1109/tii.2022.3189170

[2] Chen, X., Wang, X., Zhang, K., Fung, K. M., Thai, T. C., Moore, K., ... & Qiu, Y. (2022). Recent advances and clinical applications of deep learning in medical image analysis. *Medical image analysis*, *79*, 102444. https://doi.org/10.1016/j.media.2022.102444

[3] Gayathri, S., & Gowri, S. (2023). Securing medical image privacy in cloud using deep learning network. *Journal of Cloud Computing*, *12*(1), 40. https://doi.org/10.1186/s13677-023-00422-w
[4] Haripriya, R., Khare, N., & Pandey, M. (2025). Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Scientific Reports*, *15*(1), 12482. https://doi.org/10.1038/s41598-025-97565-4
[5] Islam, M. M., Rahaman, A., & Islam, M. R. (2020). Development of smart healthcare monitoring system in IoT environment. *SN computer science*, *1*(3), 185. https://doi.org/10.1007/s42979-020-00195-y
[6] Jayagopalan, S., Alkhouli, M., & Aruna, R. (2023). Intelligent privacy preserving deep learning model for securing IoT healthcare system in cloud storage. *Journal of Intelligent & Fuzzy Systems*, *45*(4), 5223-5238. https://doi.org/10.3233/jifs-231713
[7] Kaissis, G., Ziller, A., Passerat-Palmbach, J., Ryffel, T., Usynin, D., Trask, A., ... & Braren, R. (2021). End-to-end privacy preserving deep learning on multi-institutional medical imaging. *Nature Machine Intelligence*, *3*(6), 473-484. https://doi.org/10.1038/s42256-021-00337-8
[8] Khan, R., Taj, S., Ma, X., Noor, A., Zhu, H., Khan, J., ... & Khan, S. U. (2024). Advanced federated ensemble internet of learning approach for cloud based medical healthcare monitoring system. *Scientific Reports*, *14*(1), 26068. https://doi.org/10.1038/s41598-024-77196-x
[9] Li, C., Wang, L., & Li, Y. (2022). Transformer and group parallel axial attention co-encoder for medical image segmentation. *Scientific Reports*, *12*(1), 16117. https://doi.org/10.1038/s41598-022-20440-z
[10] Li, X., Gu, Y., Dvornek, N., Staib, L. H., Ventola, P., & Duncan, J. S. (2020). Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results. *Medical image analysis*, *65*, 101765. https://doi.org/10.1016/j.media.2020.101765
[11] Lyu, M., Ni, Z., Chen, Q., & Li, F. (2024). Edge-DPSDG: An edge-based differential privacy protection model for smart healthcare. *IEEE Transactions on Big Data*, *11*(1), 21-34. https://doi.org/10.1109/tbdata.2024.3366071
[12] Nazir, S., & Kaleem, M. (2023). Federated learning for medical image analysis with deep neural networks. *Diagnostics*, *13*(9), 1532. https://doi.org/10.3390/diagnostics13091532
[13] Orthi, S. M., Rahman, M. H., Siddiqa, K. B., Uddin, M., Hossain, S., Al Mamun, A., & Khan, M. N. (2025). Federated learning with privacy-preserving big data analytics for distributed healthcare systems. *Journal of computer science and technology studies*, *7*(8), 269-281. https://doi.org/10.32996/jcsts.2025.7.8.31
[14] Sharma, P. K., Chen, M. Y., & Park, J. H. (2017). A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE access*, *6*, 115-124. https://doi.org/10.1109/access.2017.2757955
[15] Stoian, D. I., Leonte, H. A., Vizitiu, A., Suciu, C., & Itu, L. M. (2023). Deep Neural Networks in Medical Imaging: Privacy Preservation, Image Generation and Applications. *Applied Sciences*, *13*(21), 11668. https://doi.org/10.3390/app132111668
[16] Yan, Z., Wicaksana, J., Wang, Z., Yang, X., & Cheng, K. T. (2020). Variation-aware federated learning with multi-source decentralized medical image data. *IEEE Journal of Biomedical and Health Informatics*, *25*(7), 2615-2628. https://doi.org/10.1109/jbhi.2020.3040015
[17] Yu, H., Samuels, D. C., Zhao, Y. Y., & Guo, Y. (2019). Architectures and accuracy of artificial neural network for disease classification from omics data. *BMC genomics*, *20*(1), 167. https://doi.org/10.1186/s12864-019-5546-z
[18] Yu, Q., Zhang, H., Xu, H., & Kong, F. (2023). POMIC: privacy-preserving outsourcing medical image classification based on convolutional neural network to cloud. *Applied Sciences*, *13*(6), 3439. https://doi.org/10.3390/app13063439
[19] Zhou, S. K., Greenspan, H., Davatzikos, C., Duncan, J. S., Van Ginneken, B., Madabhushi, A., ... & Summers, R. M. (2021). A review of deep learning in medical imaging: Imaging traits,

technology trends, case studies with progress highlights, and future promises. *Proceedings of the IEEE*, *109*(5), 820-838. https://doi.org/10.1109/jproc.2021.3054390

[20] Ziller, A., Usynin, D., Braren, R., Makowski, M., Rueckert, D., & Kaissis, G. (2021). Medical imaging deep learning with differential privacy. *Scientific Reports*, *11*(1), 13524. https://doi.org/10.1038/s41598-021-93030-0

Authors Biography

Soniya Milmile working as an Assistant Professor in Department of Electronics and Communication Engineering at Ramdeobaba University, Nagpur. She is currently pursuing a Ph.D. in Electronics Engineering with a research focus on medical signal processing. She has over five years of teaching experience in the field of Electronics and Communication Engineering. Her research interests include signal processing, embedded systems, and the Internet of Things (IoT). She has published research articles in UGC CARE- journals and actively contributes to academic research, innovation, and professional development. Her ongoing research aims to develop advanced signal processing techniques for healthcare and biomedical applications.

Dr.P. Adlene Ebenezer is currently working as Assistant Professor in the Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, Tamil Nadu, India. She holds a first-class in Bachelor's degree in Computer Science and Engineering from Apollo Engineering College, affiliated to Anna University, Chennai, Tamil Nadu in 2012, and Master's Degree in Computer Science and Engineering from Easwari Engineering College, Anna University, Chennai in 2014. She completed her Ph.D. full time in SRM Institute of Science and Technology, Vadapalani Campus, Chennai. Her research interest includes working with real time multispectral and hyper spectral data in the field of remote sensing.

Dr.T. Amitha is a Senior Professor in the Department of Computer Science and Engineering at S.A. Engineering College, Chennai. She has extensive experience in teaching, research, and academic administration. Her areas of expertise include Machine Learning, Computer Networks, Video Processing, High-Speed Networks, and Data Mining. In addition to her academic contributions, she actively participates in institutional development and serves as a member of the Student Grievance Redressal Committee (SGRC). Dr. Amitha has contributed significantly to research through numerous publications in emerging areas of computer science and engineering.

Dr.A. Jahir Husain is presently working as Senior Assistant Professor in the department of Computer Science and Engineering in Vel Tech High Tech Dr. Ranagarajan Dr. Sakunthala Engineering College, Avadi, Chennai. He is having more than 26 years of experience in teaching computer science subjects at various Engineering colleges and Deemed Universities. His research interests include Internet of Things, Machine Learning, Distributed Computing and Ad hoc networks.

Dr.J. Sivadasan is currently working as Associate Professor, in the Department of Electronics and Communication Engineering, P.S.R Engineering College, Sivakasi, Tamil Nadu, India. He received his B.E degree in Electrical and Electronics Engineering from National Engineering College, Kovilpatti, Tamilnadu, India, in the year 2003. He completed his M.E degree in Applied Electronics from Mohamed Sathak Engineering College, Ramanathapuram, Tamilnadu, India, in the year 2008. He completed his Ph. D from Anna University, Chennai in 2020. He has more than 15 years of teaching experience and 1 Year Industry Experience. He published 8 research papers in reputed journals and 6

Patents. His research interest includes High Voltage Engineering, Nonlinear PID Control, Image processing.

Madhavan Babu is a Senior AI & Data Systems Consultant, Enterprise Cloud Architect, Researcher, Reviewer, and Technology Judge with more than 24 Years of Experience in Cloud Computing, Artificial Intelligence, Enterprise Data Platforms, and Digital Transformation. He has led the Design and Implementation of Large-Scale Cloud and Analytics Solutions Supporting Mission-Critical Business Operations Across Global Organizations. His Research Interests Include Autonomous AI Agents, Multi-Agent Systems, Intelligent Data Integration, Machine Learning, And Scalable Distributed Architectures. Madhavan Actively Contributes to the Professional and Scholarly Community Through Peer Review Activities, Industry Judging Engagements, And Technology Leadership Initiatives. He is a Professional Member of ACM, a Member of ACM SIGAI, a Web of Science Reviewer, and a 2026 CODiE Awards Judge. His work Reflects the Intersection of Applied Industry Innovation and Advanced Research in Artificial Intelligence and Data Systems.