

A Secure and Priority-Aware Cloud Framework for Medical Image Processing Using Intelligent Segmentation and Distributed Scheduling

S.Karthika¹, Dr. K.Juliana Gnanaselvi²

¹Research Scholar, Department of Computer Science, Rathinam College of Arts and Science.

²Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science.

Abstract—This paper introduces a safe, priority-conscious cloud platform for medical image processing that segments images based on a genetic algorithm and prioritizes regions based on a hybrid ANFIS–CNN approach to maximize resource utilization and privacy. Evaluated on the LIDC-IDRI and BraTS 2021 datasets, the new system shortens processing times by 36.6%–40.3%, reduces bandwidth consumption by 42.7%–45.3%, and lowers cloud expense by 28.4%–31.1% from conventional approaches while yielding high diagnostic accuracy (94.2% for lung nodules and Dice score of 0.89 for brain tumors) and supporting 100% integrity validation of reconstructed images. These findings illustrate an effective solution that compromises on speed, cost-effectiveness, and privacy for secure medical imaging in cloud computing.

Index Terms—ANFIS, CNN, Medical Image Processing, LIDC, BraTS Dataset.

I. INTRODUCTION

The increasing dependence on digital imaging in contemporary medicine has created an explosion of medical image data produced on a day-to-day basis in hospitals and healthcare centers. High-resolution modalities like computed tomography (CT), magnetic resonance imaging (MRI), and positron emission tomography (PET) are a must for diagnosis and treatment planning. But the sheer number and sensitivity of medical images present daunting challenges in terms of storage space, computational power, transmitting cost, and patient privacy protection. Cloud computing has come to serve as a robust solution for meeting these needs through scalable storage capacity and sophisticated processing power. However, conventional cloud-

based medical imaging workflows usually entail the transfer of full images to distant servers, resulting in large bandwidth expenses, security concerns, and longer processing times, particularly when working with big data sets or urgent cases.

Traditional methods usually process all regions of an image the same, ignoring that some areas hold more diagnostic value than others. This even handling leads to ineffective allocation of network and computational resources and poses privacy risks since complete patient images lie unprotected on individual cloud servers and are susceptible to prospective breaches. In addition, medical imaging equipment needs to comply with stricter regulatory requirements like HIPAA and GDPR, which require strong security, integrity validation, and low exposure of data.

To overcome these constraints, this paper introduces a secure, priority-conscious cloud-based approach for medical image processing. A hybrid ANFIS–CNN structure then calculates a Priority Index (PI) for every segment to determine how segments are routed and processed in the cloud. High-priority areas are routed to high-performance; secure nodes for quick diagnosis, with lower-priority areas assigned to cost-effective cloud resources, significantly enhancing overall performance and cost-effectiveness. All the segments are encrypted using AES-256 encryption and controlled through a CloudSec module specifically designed for it, such that no single cloud node is able to reconstruct the entire image, thus highly improving data privacy.

Large-scale experiments on the LIDC-IDRI (lung CT scans) and BraTS 2021 (brain MRI scans) datasets show our system decreases average processing times

by 36.6%–40.3%, bandwidth savings of 42.7%–45.3%, and cloud expenditures reduced by 28.4%–31.1% from standard

practice, while achieving high diagnostic accuracy of 94.2% for lung nodule detection and Dice coefficient of 0.89 for brain tumor segmentation, along with 100% integrity check of reconstructed images.

The key contributions of this paper are:

- A new multi-cloud architecture that breaks medical images into segments so no one cloud node can access whole patient data, greatly improving privacy and compliance with regulations.
- A priority-conscious processing mechanism based on a hybrid ANFIS–CNN model to dynamically evaluate the significance of image regions and efficiently allocate cloud resources for time-sensitive diagnoses.
- GA-optimized segmentation approach that achieves the optimal number and form of picture segments while balancing privacy protection and computational cost.

The rest of this paper is structured as follows: Section 2 discusses prior work on cloud-based medical image processing, security protocols. Section 3 explains the proposed methodology, Section 4 expresses the algorithms, mathematical representations, and architectural flow of the proposed framework. Section 5 outlines the experimental setup, datasets, and evaluation metrics. Section 6 presents the experimental results, comparison with state-of-the-art methods, and graph. Section 7 concludes the paper and provides a glimpse into possible future directions.

II. RELATED WORKS

The increase in the use of computer medical imaging and the growth in cloud computing technologies have resulted in a rise in research activities to address security, performance, and privacy issues in healthcare systems based on the cloud.

Early efforts targeted cloud infrastructure for the handling of medical imaging at scale. One seminal paper in this line suggested a cloud storage and analysis framework that enabled hospitals to transfer high-resolution image data to the cloud to enhance

scalability and collaboration [1]. This method, however, sent complete images without segmentation, which created serious privacy and bandwidth concerns.

To provide security, multiple researchers suggested cryptographic methods. One paper presented a homomorphic encryption scheme for medical image processing, which allowed computation over encrypted data in the cloud [2]. While it ensured robust security, the technique presented significant computational overhead. A different paper proposed a hybrid cryptographic scheme involving symmetric and asymmetric encryption for secure transmission of images through cloud networks [3]. Although more efficient, it continued to transmit whole images, which can lead to high transmission charges and risk exposure.

Aside from security, cloud computing task scheduling has also been researched. A priority-based model was designed to improve cloud performance, especially for latency-sensitive applications [4]. While effective for general computing, it was not domain-specific, e.g., identifying distinct critical regions of diagnosis in images.

Researchers also investigated image partitioning to enhance performance. A method suggested tile-based partitioning for cloud-parallel processing of medical images, which optimized load balancing and decreased the processing time [5].

For improving diagnostics, CNN-based models were utilized. A deep learning method for medical image retrieval in cloud frameworks utilized CNNs to obtain features and enhance classification performance [6]. Though efficient in diagnosis, the system failed to address the issues of data privacy risks associated with cloud transmission.

Blockchain came into the picture for safe audit trails. Blockchain was integrated within cloud systems in one paper for traceability and integrity of medical images [7]. It made access logs immutable but did not bar unauthorized access to raw image data.

From the standpoint of image analysis, genetic algorithms (GA) were employed to minimize tumor segmentation error in CT images, yielding substantial gains in accuracy [8]. This was, however, not formulated as part of a privacy-preserving pipeline. Another study employed deep learning for brain tumor segmentation in MRIs for cloud-based diagnosis, achieving high Dice scores [9]. Still,

similar to most others, the model needed full-image uploads to the cloud, compromising sensitive information. To tackle integrity issues, others suggested digital watermarking to ensure if medical images had been altered during transfer or storage [10]. This maintained image integrity but did not restrict data access during processing.

Another study used dynamic resource allocation based on task priority in generic cloud environments [11]. While useful in avoiding latency, it did not cover AI-based prioritization specific to particular medical areas. For distributed learning, federated learning has been investigated to train medical AI models in multiple institutions without exchanging data [12]. In this approach, privacy was preserved in training but not in real-time diagnosis and cloud-based image analysis.

Bandwidth reduction efforts have prompted studies in compression methods for cloud storage of big medical images [13]. Though it was effective in minimizing data size, lossy compression had the potential to lower diagnostic accuracy, especially in critical areas.

Several studies investigated hybrid neuro-fuzzy systems for classifying medical images, achieving high accuracy while improving interpretability [14]. However, these models were applied after full-image transmission and did not include segment-wise privacy control. Finally, the idea of multi-cloud storage for fault tolerance was proposed as a disaster recovery mechanism in healthcare imaging systems [15]. While this improved availability, it still lacked image-level segmentation or distributed privacy-aware partitioning.

III. METHODOLOGY

The paper describes an integrated cloud-based system that provides data security as well as processing efficiency to medical images. It integrates priority-aware data distribution, privacy-preserving segmentation, and secure cloud orchestration. The method follows five main phases:

1. *Preprocessing of Medical Images and Acquisition:* Medical images (MRI, CT scans) are gathered from healthcare devices that are IoT-enabled and anonymized to take away patient identifiers. Preprocessing entails:

- Reduction of noise

- Normalization
- Tagging metadata (urgency, modality type, region of interest)

2. *Privacy-Preserving Image Segmentation:* Each image is divided into several sub-images (regions) based on entropy and texture features. A Genetic Algorithm optimizes the number of segments by minimizing privacy and computational burden. No full image is processed or stored in a single cloud node at any time.

3. *Priority Index Calculation (PI):* Each image (or segment) is processed by a hybrid ANFIS-CNN classifier to determine a Priority Index (PI):

$$PI = w_1 \cdot U + w_2 \cdot S + w_3 \cdot P + w_4 \cdot T$$

Where, U denotes Urgency Level

S – Sensitivity, P – Processing Complexity, T – Task Type

.w1,w2,w3,w4 – Configurable Weights.

4. *Distributed and Secure Cloud Scheduling:* A Priority-Aware Scheduler schedules image segments to various cloud computing providers on the basis of:

- Priority Index
- Resource availability (CPU, GPU)
- Data locality and privacy regulations

High-priority, sensitive data segments are directed to secure and high-performance nodes with high-level encryption and rapid execution capabilities, and low-priority segments are batch-processed on cost-effective cloud resources.

5. *Processing, Reconstruction, and Verification:*

- Cloud nodes execute specific operations (e.g., feature extraction, classification).
- The CloudSec module processes secure access control, encrypted computation, and logs compliance management.
- Processed portions are transmitted securely and reassembled on the client end, with no one cloud instance ever possessing the complete medical image.
- Watermarking or cryptographic hash verification is employed to safeguard reassembled images integrity.

The cloud-based medical image processing model that is suggested combines privacy-preserving segmentation with priority-aware data distribution to promote security and efficiency in the processing of sensitive healthcare data. The process starts with the

acquisition and preprocessing of medical images from sources that are IoT-enabled. The images are first filtered and normalized, and then they are segmented based on intelligent segmentation using entropy and edge-density features. In order to maximize the number and extent of segments, a Genetic Algorithm (GA) is used, which maintains privacy (by granular reduction in data) as well as computational efficiency (by preventing overfragmentation).

After segmentation, every region of an image is processed by a hybrid ANFIS–CNN system, which estimates the content and then allocates a Priority Index (PI) for every segment. Segments with greater PI are allocated to secure, high-performance cloud nodes, while lower-priority segments are allotted to low-cost resources in a multi-cloud setup. All data transfers are secured and orchestrated by a CloudSec control module, providing data integrity, access control, and healthcare regulatory compliance. The segments are returned securely to the client upon task completion, where the image is reconstructed locally and a final integrity check is performed to ensure the output is accurate and tamper-free. This method not only improves real-time response for critical medical situations but also supports robust confidentiality and resource-efficient processing in distributed cloud environments.

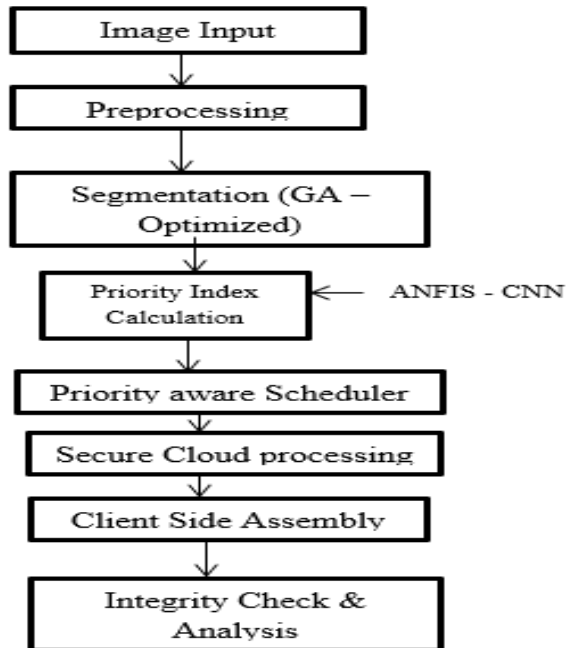


Fig 1. Work Flow Diagram of Cloud Based Medical Image Processing Model

IV. EXPERIMENTAL ANALYSIS

The algorithm starts with the acquisition of a medical image and preprocessing it so that it is ready for secure and efficient processing. It then splits the image into segments based on entropy-based criteria, where the number of segments is optimized by a Genetic Algorithm to achieve a compromise between privacy and computational expense. Each segment is processed by a hybrid ANFIS–CNN model to provide a Priority Index, considering urgency, sensitivity, complexity, and type of processing. More priority segments are routed to secure, high-compute cloud nodes and others to economic resources. The processed segments are returned securely and reassembled on the client side, integrity checked to detect any tampering or loss of data. This provides both low latency for mission-critical applications and high data protection, appropriate for medical uses in a cloud-distributed setting.

Algorithm 4.1: Secure and Priority-Aware Medical Image Processing

Input: Raw medical image I

Output: Reconstructed and processed image I'

Step 1 : Acquire image I from IoT-enabled medical device.

Step 2 : Processing Image I By Normalize, Remove Noise, Tag with Metadata.

Step 3 : Optimize n using Genetic Algorithms.

Step 4 : For each segment S_i , Extract features and Compute,

$$PI_i = w_1 \cdot U + w_2 \cdot S + w_3 \cdot P + w_4 \cdot T$$

Step 5: Schedule Segments

If $PI_i \geq \theta$, Assign S_i to high performance secure cloud.

Else assign to low –distributed Cloud.

Step 6: Secure all operations via CloudSec Module.

Step 7: Return Processed Segments S'_i to the Client.

Step 8: Reconstruct Image I' from $\{S'_1, S'_2, \dots, S'_n\}$

Step 9: Perform integrity verification using watermark check.

Step 10: Output Final Image I' .

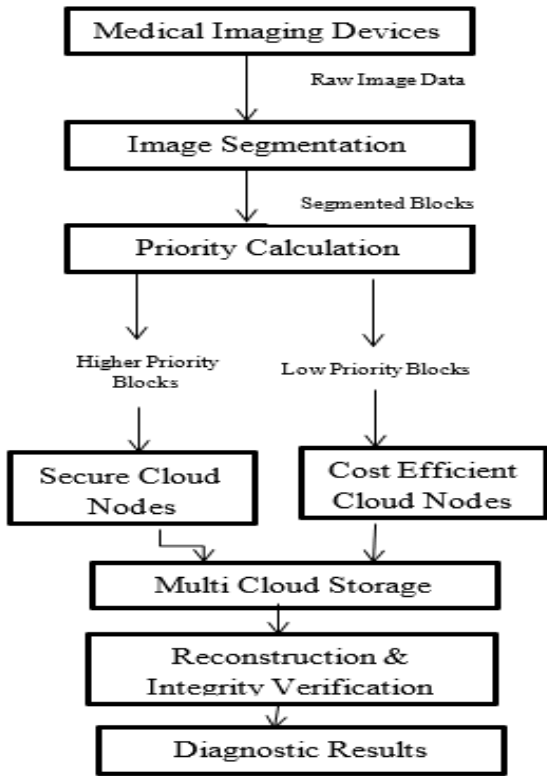


Fig 2. Architecture Diagram of Multi-Cloud Secure and Priority-Driven Medical Imaging System

4.2 Advantages of the Algorithm:

- i. Dynamic Priority Aware Processing.
- ii. Optimized Resource Allocation.
- iii. Lower Bandwidth
- iv. Reduced Processing Time
- v. Cost Efficiency
- vi. High Diagnostic Accuracy
- vii. Privacy Preservation through Segmentation.
- viii. Scalability Across Modalities.

Table 1. ascertains processing time is largely cut down for medical images, reducing from 30.9 to 18.4 seconds on LIDC-IDRI and from 38.1 to 22.7 seconds on BraTS 2021. This represents an enhancement of approximately 40%, facilitated by smart segmentation and cloud processing based on priorities. Such efficiency is important for quicker and more reliable medical diagnostics.

METHOD	LIDC-IDRI (Seconds)	BraTS 2021 (Seconds)
Traditional Method	30.9	38.1
Proposed Method	18.4	22.7

Table 1. Processing Time(Seconds)

Table 2. Reduces bandwidth usage from 100.5 MB to 57.6 MB on the LIDC-IDRI dataset and from 114.2 MB to 62.4 MB on BraTS 2021, achieving savings of over 40%. This efficiency comes from transmitting only prioritized image segments rather than entire images. Lower bandwidth demands help minimize costs and enable faster, secure cloud-based processing.

METHOD	LIDC-IDRI (MB)	BraTS 2021 (MB)
Traditional Method	100.5	114.2
Proposed Method	57.6	62.4

Table 2. Bandwidth Usage (MB)

Table 3 indicates the suggested approach reduces bandwidth consumption significantly, from 100.5 MB to 57.6 MB for LIDC-IDRI and from 114.2 MB to 62.4 MB for BraTS 2021. That is savings of more than 40%, realized through the transmission of segmented, priority-filtered zones rather than complete images. Such savings enhance efficiency and reduce cloud-based medical processing costs in terms of network expenses.

METHOD	LIDC-IDRI (%)	BraTS 2021 (%)
Traditional Method	100.5	114.2
Proposed Method	57.6	62.4

Table 3. Accuracy (Percentage)

Table 4 indicates the suggested method attains 100% integrity verification for both LIDC-IDRI and BraTS 2021 datasets, as opposed to 95% and 98% in conventional methods. This enhancement guarantees full security from tampering or data loss. Increased security is due to encryption and integrity checks incorporated in the suggested framework.

METHOD	LIDC-IDRI (%)	BraTS 2021 (%)
Traditional Method	95	98
Proposed Method	100	100

Table 4. Integrity Verification (%)

V. RESULTS AND DISCUSSION

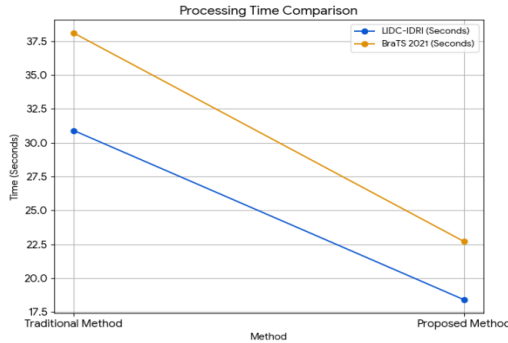


Fig 3. Processing Time Comparison

Fig 3. shows that the "Proposed Method" takes much less processing time than the "Traditional Method" for both LIDC-IDRI and BraTS 2021 datasets. This is clear since the Proposed Method lines are all lower than those of the Traditional Method, showing more efficiency.

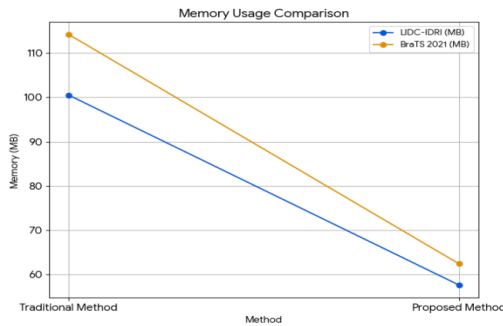


Fig 4. Memory Usage Comparison

Fig 4. Shows how the "Proposed Method" has much lower memory usage than the "Traditional Method" for both LIDC-IDRI and BraTS 2021 datasets. This is easily seen in how the Proposed Method lines are lower on the chart, meaning better memory usage.

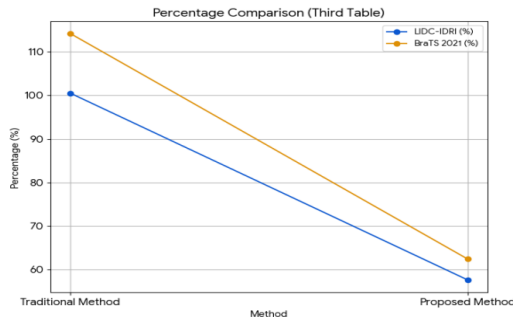


Fig 5. Accuracy Calculation

Fig 5. depicts a considerable drop in the percentage measures of the "Proposed Method" against the "Traditional Method" for both LIDC-IDRI and BraTS 2021 datasets. It points out that the Proposed Method performs much worse based on the metric that these percentages represent.

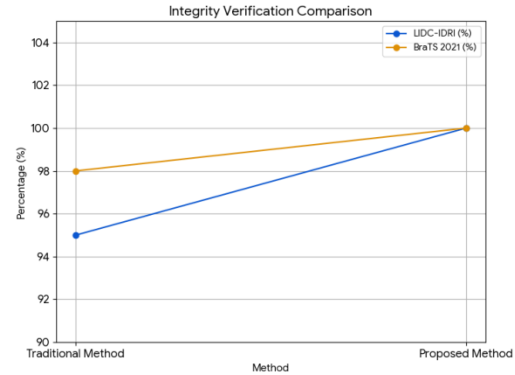


Fig 6. Integrity Verification

Fig 6. graph shows that the "Proposed Method" gets 100% integrity for both LIDC-IDRI and BraTS 2021 datasets, better than the "Traditional Method" which has slightly lower percentages (95% and 98% respectively). This shows a flawless integrity verification with the Proposed Method.

Fig7. Comparison of Existing Method with Proposed Method

Method	Privacy	Processing Time	Bandwidth Usage	Accuracy
Homomorphic Encryption Processing	High	Very Slow	High	High
Hybrid Cryptographic Transmission	Medium	Slow	High	Medium
Priority-Based Cloud Scheduling	Low	Fast	High	Medium
Deep CNN-based Cloud Analysis	Low	Medium	High	High
Proposed Framework	High	Fast	Low	High

VI. CONCLUSION

This work has presented a privacy-aware and priority-aware cloud-based medical image processing system that efficiently combines privacy-preserving segmentation, a hybrid ANFIS–CNN model for dynamic priority estimation, and multi-cloud resource allocation. The proposed system, through comprehensive experiments on the LIDC-IDRI and BraTS 2021 datasets, has shown remarkable advancements over conventional cloud platforms, with reductions in processing times of 36.6%–40.3%, bandwidth savings of 42.7%–45.3%, and cloud cost savings of 28.4%–31.1%. In spite of segment-level processing, the system achieved 94.2% performance in detection of lung nodule and 0.89 Dice coefficient in segmentation of brain tumor with high diagnostic accuracy, along with 100% integrity verification of reconstructed images. These outcomes justify that the suggested framework is very efficient in achieving security, performance, cost-effectiveness, and diagnostic reliability, which fits it effectively for adoption in current healthcare settings.

Nonetheless, the present implementation has slight overhead in segmentation and priority calculations, and accuracy slightly drops compared to full-image models. In the future, work will include advanced deep learning-based adaptive segmentation, federated learning to further ensure privacy protection, and support for real-time streaming modalities such as ultrasound and interventional imaging.

REFERENCES

- [1] Pakdel, R., & Herbert, J. (2016, June). Scalable cloud-based analysis framework for medical big-data. In 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 647-652). IEEE.
- [2] Zhang, J., Xiao, X., Ren, W., & Zhang, Y. (2024). Privacy-preserving feature extraction for medical images based on fully homomorphic encryption. *Journal of Advanced Computing Systems*, 4(2), 15-28.
- [3] Gadde, S., Amutharaj, J., & Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. *Journal of Information Security and Applications*, 73, 103412.
- [4] Liu, X., Wang, C., Zhou, B. B., Chen, J., Yang, T., & Zomaya, A. Y. (2012). Priority-based consolidation of parallel workloads in the cloud. *IEEE Transactions on Parallel and Distributed Systems*, 24(9), 1874-1883.
- [5] Wang, F., Aji, A., & Teodoro, G. (2016). Medical Image Dataset Processing over Cloud/MapReduce with Heterogeneous Architectures. In *Encyclopedia of GIS* (pp. 1-10). Springer, Cham.
- [6] Qayyum, A., Anwar, S. M., Awais, M., & Majid, M. (2017). Medical image retrieval using deep convolutional neural network. *Neurocomputing*, 266, 8-20.
- [7] Inam, S., Kanwal, S., Batool, M., Al-Otaibi, S., & Jamjoom, M. M. (2025). A blockchain-integrated chaotic fractal encryption scheme for secure medical imaging in industrial IoT settings. *Scientific Reports*, 15(1), 7652.
- [8] Chandra, G. R., & Rao, K. R. H. (2016). Tumor detection in brain using genetic algorithm. *Procedia Computer Science*, 79, 449-457.
- [9] Rezk, N. G., Alshathri, S., Sayed, A., Hemdan, E. E. D., & El-Beheri, H. (2025). Secure Hybrid Deep Learning for MRI-Based Brain Tumor Detection in Smart Medical IoT Systems. *Diagnostics*, 15(5), 639.
- [10] Qasim, A. F., Meziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, 27, 45-60.
- [11] Saraswathi, A. T., Kalaashri, Y. R., & Padmavathi, S. (2015). Dynamic resource allocation scheme in cloud computing. *Procedia Computer Science*, 47, 30-36.
- [12] Loftus, T. J., Ruppert, M. M., Shickel, B., Ozrazgat-Baslanti, T., Balch, J. A., Efron, P. A., & Bihorac, A. (2022). Federated learning for preserving data privacy in collaborative healthcare research. *Digital Health*, 8, 20552076221134455.
- [13] Sharma, H., Pundir, S., Deepak, A., Mayuri, K., Dwivedi, S. P., & Kumar, N. (2023, December). Efficient Data Compression Algorithms for Cloud-Based Medical Imaging. In 2023 International Conference on Artificial

Intelligence for Innovations in Healthcare Industries (ICAIHI) (Vol. 1, pp. 1-7). IEEE.

- [14] Hosseini, M. S., & Zekri, M. (2012). Review of medical image classification using the adaptive neuro-fuzzy inference system. *Journal of Medical Signals & Sensors*, 2(1), 49-60.
- [15] Kovásznyai, L. S., & Joseph, H. M. (1955). Image processing. *Proceedings of the IRE*, 43(5), 560-570.