

Federated Deep Learning for Privacy-Preserving Data Fusion in Sustainable AI-Driven Healthcare Systems

R Neelaveni

neelavenir50@gmail.com

AIML Mangayarkarasi College of Engineering

Bhuvan Unhelkar

University of South Florida

Research Article

Keywords: Multi-Modal Data, Data Fusion, Multi-Convolution Spatial and Efficient Squeeze-Excitation Network, Privacy-Preserving Asynchronous Federated Learning, Bulyan-based Adaptive Differential Privacy Mechanism

Posted Date: October 16th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-9810291/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: No competing interests reported.

FEDERATED DEEP LEARNING FOR PRIVACY- PRESERVING DATA FUSION IN SUSTAINABLE AI- DRIVEN HEALTHCARE SYSTEMS

Dr.Neelaveni R^{1*}, Bhuvan Unhelkar²,

*^{1*}Associate Professor & Academic Coordinator ,Department of CSE&AIML
Mangayarkarasi College of Engineering, Madurai,Tamilnadu INDIA - 625402*

*²Professor, Muma College of Business, University of South Florida, 8350 N. Tamiami
Trail Sarasota, Florida. USA.*

*³Professor & Head IPR, Department of Computer Science and Engineering, KG
Reddy College of Engineering and Technology, RR district , Telangana,INDIA –
501504*

^{1*}Corresponding author email: neelavenir50@gmail.com

Abstract

The growing volume and complexity of heterogeneous medical data create challenges in extracting diagnostic knowledge while preserving privacy because centralized models face high computation costs and security risks. To overcome this limitation, the novel Asynchronous Federated Multi-Convolution Spatial and Efficient Squeeze-Excitation Network (AFL-MCSESEN) with Bulyan-Based Adaptive Differential Privacy (BADP) was proposed for Privacy-Preserving Multi-Modal Data Fusion in Sustainable AI-Driven Healthcare Systems (HS) (AFL-MCSESEN-BADP-HS). Initially, Multi-modal data such as structured, semi-structured, and unstructured Knee Osteoarthritis data are collected and stored in Apache Spark managed by data lake. These heterogeneous sources are integrated using the Unified Element Tree Fusion method. Then, these fused data are processed through Z-score normalization and feature vector encoding. Simultaneously, the knee joint images are standardized for attaining consistent visual representation of pathological changes. Then, these pre-processed inputs are processed for Local Feature Extraction and Refinement using a Multi-Convolution Spatial and Efficient Squeeze-Excitation Network. Here, ResNet-34 backbone integrated with a Condensed Depthwise Squeeze-Excitation (CDSE) module and Multi-Convolution Spatial Attention (MCSA) was utilized to isolate subtle clinical indicators. To maintain institutional privacy, these features are trained within an privacy-preserving asynchronous federated learning framework, where ten institutional clients compute local gradients on vertically partitioned data using secure inner-product

evaluations. Finally, a Bulyan-Based Adaptive Differential Privacy mechanism is utilized for further enhancing robustness and privacy. By this, the proposed AFL-MCSESEN-BADP-HS system provide sustainable, high-accuracy diagnostic tool for classifying Kellgren-Lawrence (KL) Grades of Knee Osteoarthritis such as Grade 0 (Healthy), Grade 1 (Doubtful), Grade 2 (Mild), Grade 3 (Moderate) and Grade 4 (Severe). Here, the proposed AFL-MCSESEN-BADP-HS system attains an Accuracy of 99.64%, an Area Under curve value as 0.998, Communication Overhead as 285MB, Data Integration Latency as 703.33ms, Spark Query Throughput as 516.67QPS, Attack Success Rate as 1.8 and Privacy-Utility Index (PUTI) as 0.96. By this results, the proposed AFL-MCSESEN-BADP-HS system provides the promising solution for Privacy-Preserving Healthcare Systems.

Keywords: *Multi-Modal Data, Data Fusion, Multi-Convolution Spatial and Efficient Squeeze-Excitation Network, Privacy-Preserving Asynchronous Federated Learning, Bulyan-based Adaptive Differential Privacy Mechanism.*

1. INTRODUCTION

In recent years, high-tech medical devices are utilized for collecting multi-modal and heterogeneous medical data [1]. Generally, multi-modal data includes structured data such as Electronic Medical Records (EMRs), semi-structured data in formats like Comma-Separated Values (CSV) and JavaScript Object Notation (JSON), and unstructured data such as magnetic resonance imaging (MRI), computed tomography (CT), X-ray, and positron emission tomography (PET) scans [2-5]. This escalating volume and complexity of heterogeneous medical data generated by diverse medical devices impose significant challenges on the extraction of diagnostic knowledge while ensuring robust data protection [6-8].

Existing deep learning models are often suffer from high computational expenses and a deficiency in real-time processing, because it fails to integrate fragmented multi-modal data such as structured EMRs, semi-structured files, and unstructured imaging into a single and cohesive model [9-10]. Moreover gathering all data in a single centralized location introduces significant security risks because a single breach or malicious participant can inject corrupted information and thereby compromise model integrity and lead to the leakage of sensitive personal data [11-15]. In addition, these systems also face efficiency limitations due to imbalanced computation capacity and communication resources across participating healthcare institutions [16-22]. To overcome this issues, novel Asynchronous Federated Multi-Convolution Spatial and

Efficient Squeeze-Excitation Network with Bulyan-Based Adaptive Differential Privacy was introduced for Privacy-Preserving Multi-Modal Data Fusion in Sustainable AI-Driven Healthcare Systems (AFL-MCSESEN-BADP-HS).

The motivation of the proposed AFL-MCSESEN-BADP-HS system arises due to the requirement for an efficient and privacy-aware learning architecture capable of supporting large-scale collaborative healthcare analytics. Here, asynchronous federated learning strategy is utilized to improve training stability and computational efficiency across heterogeneous institutional participants while avoiding direct data exchange. Also, the Multi-Convolution Spatial and Efficient Squeeze-Excitation mechanisms is incorporated, which strengthens the feature discrimination by emphasizing clinically relevant spatial patterns and channel interrelations in Knee Osteoarthritis imaging. In addition, the Bulyan-Based Adaptive Differential Privacy mechanism is introduced, which enhances robustness by filtering adversarial updates and maintaining global model integrity. By this, the proposed AFL-MCSESEN-BADP-HS system provide accurate and resilient classification of Kellgren–Lawrence grades within a distributed and sustainable AI-driven healthcare environment. The contribution of the proposed AFL-MCSESEN-BADP-HS system is given below,

- The Unified Element Tree Fusion method is implemented to integrates heterogeneous medical sources including structured EMRs, semi-structured healthcare records, and unstructured imaging into a queryable Spark-managed data lake.
- The MCSESEN architecture is utilized, which has ResNet-34 backbone with Condensed Depthwise Squeeze-Excitation and Multi-Convolution Spatial Attention modules for isolating subtle pathological indicators for Kellgren-Lawrence grading.
- The privacy-preserving asynchronous federated learning framework is implemented for reducing communication costs, energy consumption, and privacy risks.
- The Bulyan-based robust aggregation strategy was employed, which incorporates Multi-Krum and coordinate-wise trimmed mean filters for eliminating adversarial updates and maintaining global model integrity.
- The adaptive differential privacy mechanism was utilized, which applies scheduled Gaussian noise to aggregated updates for attaining high diagnostic utility with strict institutional data protection standards.

The remainder of this paper is organized as follows. Section 2 delves into the related work related to Federated Deep Learning for Privacy-Preserving Data Fusion in Sustainable AI-Driven Healthcare Systems. Section 3 provides details about the proposed AFL-MCSESEN-BADP-HS system. Section 4 illustrates the obtained results and discussion. Finally, Section 5 concludes the paper with future research directions.

2. RELATED WORKS

This section presents a review of recent Federated Deep Learning for Privacy-Preserving Data Fusion in Sustainable AI-Driven Healthcare Systems. Some of the recent related works are given below,

In 2025, Wang, J., et al. [16] proposed privacy preserving framework for heterogeneous multi-modal sensor fusion within smart healthcare system (PHMS-Fed). Here, collection of diverse sensor data across multiple institutions was taken as input. Then, these data are fused using adaptive tensor decomposition method. These fused data are fed into privacy preserving federated learning for attaining smart healthcare system. It achieves physiological monitoring accuracy as 0.9386 and privacy protection score as 0.9845. However, it has high computational overhead.

In 2025, Aanjankumar, S., et al. [17] developed an enhanced consumer healthcare data protection system utilizing AI-driven TinyML and privacy-preserving techniques (FL-TinyML-DP-HS). Initially, ECG readings and arrhythmia data from resource-constrained edge devices was utilized as input. This data are fed into Tiny Machine Learning for local feature extraction. After this, Federated Learning are utilized to train models without the removal of sensitive information from the local environment. Here, Differential Privacy is integrated for attaining robust defense against malicious data recovery. However, it has low accuracy.

In 2025, Dubey, P., et al. [18] proposed federated learning framework for privacy-enhanced mental health prediction utilizing multimodal data integration (FL-CNN-LSTM-DPET-HS). Here, physiological signals (heart rate variability, sleep patterns) and behavioural data (online activity, social media interactions) was utilized as input. These input data are fed into Convolutional Neural Network (CNN) with Long Short-Term Memory (LSTM) network for local feature extraction. After this, federated learning environment (FL) are utilized to train models, where differential privacy and encryption techniques (DPET) is integrated for attaining secured healthcare systems. It achieves accuracy of 92% and an AUC-ROC score of 0.90. However, it has lower Privacy-Utility Index.

In 2025, Siva, O.V. and Anbarasi, M.S., [19] developed federated graph-based multimodal AI framework for privacy-preserving and explainable osteoporosis detection. Here, structured clinical data, DXA scans, and biochemical markers was utilized as input. These data are fed into Graph Neural Networks (GNNs) for attaining trabecular bone connectivity. Then, Federated Learning (FL) was utilized as a collaborative training across decentralized hospitals, while SHAP-based feature importance analysis was utilized for explainable diagnostic outputs. It achieves 94.2% accuracy and a ROC-AUC score of 0.96 with a low inference latency of 45 ms. However, it has higher Attack Success Rate.

In 2025, Haripriya, R., et al. [20] suggested a federated adaptive aggregation framework for privacy and scalability in healthcare AI. Initially, tuberculosis chest X-rays, brain MRI scans, and diabetic retinopathy images are taken as input. These data are fed into ResNet and EfficientNet models for feature extraction. Then, dynamic switching mechanism was employed to alternate between Federated Stochastic Gradient Descent (FedSGD) for high data divergence and Federated Averaging (FedAvg) for low divergence scenarios. It attains accuracy of 96%, communication overhead is reduced by 23.5% and enhanced convergence speed. However, it has high computational complexity.

In 2025, Rawas, S. and Samala, A.D., [21] developed a dual-layer security framework for privacy-preserving AI-driven healthcare edge-cloud system. Here, hybrid edge-cloud setup was implemented. In which, raw medical data are utilized for real-time processing. Here, adaptive encryption and proactive security mechanisms was utilized for anomaly detection. Then, Federated learning and differential privacy are used to secure model by distributing computations between edge nodes and the cloud. It attains 98% attack detection accuracy and latency as low as 30–50 ms, throughput as 10,000 data points per second. However, it has lower Privacy-Utility Index.

In 2025, Haripriya, R., et al. [22] developed a privacy-enhanced framework for collaborative Big Data analysis in healthcare using adaptive federated learning aggregation. Here, tuberculosis X-rays, brain MRIs, and diabetic retinopathy images was taken as input. These input data are fed into ResNet and VGG16 architectures for extracting features. Here, adaptive aggregation methodology was employed to dynamically switch between Federated Averaging (FedAvg) and Federated Stochastic Gradient Descent (FedSGD) based on real-time client data divergence. It achieves 96.3% accuracy rate and 20% reduction in execution time. However, it has lower F1-Score.

2.1 Problem Statement and Motivation

The growing volume and complexity of heterogeneous medical data from diverse sources create challenges in extracting diagnostic knowledge while preserving privacy because centralized models faces challenges like high computation costs and security risks [16-22]. Therefore, the proposed AFL-MCSESEN-BADP-HS system is introduced, which employs asynchronous federated learning for secure collaboration across institutions. Along with this, the proposed Multi-Convolution Spatial and Efficient Squeeze-Excitation Network is integrated to capture subtle clinical patterns in Knee Osteoarthritis imaging. Moreover, the Bulyan-Based Adaptive Differential Privacy mechanism is utilized, which ensures robustness against adversarial updates and protects sensitive information. Consequently, proposed AFL-MCSESEN-BADP-HS system provide accurate and privacy-preserving classification of Kellgren–Lawrence grades in distributed healthcare environments.

3. PROPOSED METHODOLOGY

In this section, the proposed Asynchronous Federated Multi-Convolution Spatial and Efficient Squeeze-Excitation Network (AFL-MCSESEN) with Bulyan-Based Adaptive Differential Privacy (BADP) for Privacy-Preserving Multi-Modal Data Fusion in Sustainable AI-Driven Healthcare Systems (HS) (AFL-MCSESEN-BADP-HS) was discussed. The block diagram of the proposed AFL-MCSESEN-BADP-HS system is given in Figure 1. The detail description of the proposed AFL-MCSESEN-BADP-HS system is given below,

3.1 Multi-Modal Data Acquisition and Fusion process

In this section, multi-modal information regarding Knee Osteoarthritis disease from Beijing Tsinghua Changgung Hospital is collected. The collection includes Structured Data such as Electronic Medical Records (EMRs) containing patient demographics and clinical history, Semi-Structured Data such as Healthcare records in CSV, JSON, and XML formats and Unstructured Data such as Medical imaging like X-ray, MRI, CT, and PET scans. This medical data is stored in a data lake with the help of Apache Spark to manage the high volume and variety of medical information. Also, metadata (for example, In X-ray: date, the patient’s ID, and the machine used information) and file paths are recorded to verify traceability back to original clinical records. Subsequently, all collected heterogeneous medical data are fused using Unified Element Tree Fusion method, which merges the matching keys across different modalities and integrates the individual feature vectors into Delta tables or a single queryable Spark DataFrame for

Knee Osteoarthritis analysis [23]. These integrated datasets serve as the input for the following analysis.

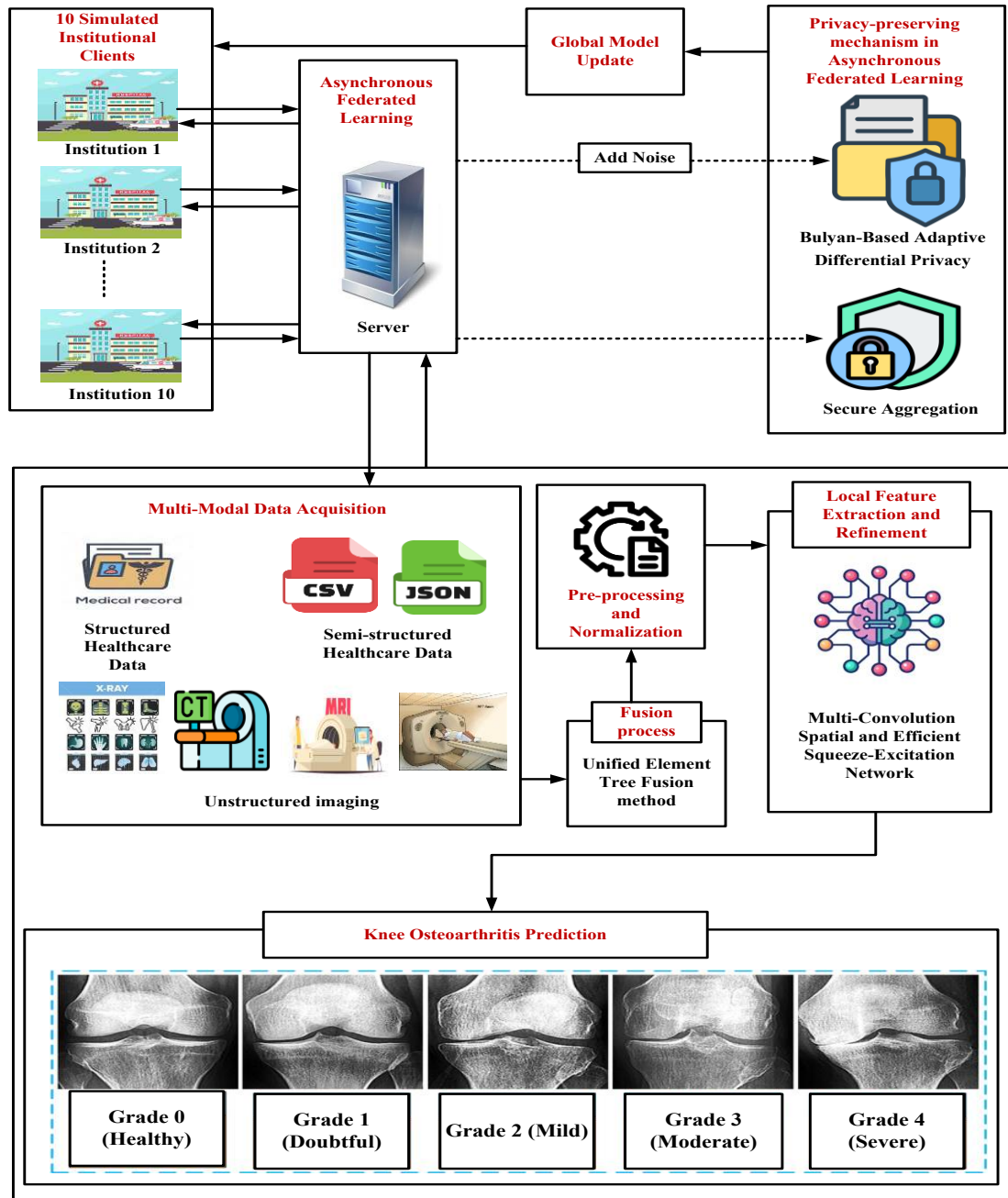


Figure 1: Block diagram of the proposed AFL-MCSESEN-BADP-HS system

3.2 Pre-processing and Normalization

Let assume fused medical datasets related to Knee Osteoarthritis is based on the following equation (1)

$$FD = \sum_{i=1}^N \{A_{CA}^i, A_{image}^i\} \quad (1)$$

Where A_{CA}^i depicts the structured and semi-structured clinical features related to Knee Osteoarthritis, A_{image}^i depicts the knee joint imaging modalities (X-ray, MRI, CT, PET) and N depicts the total number of fused Knee Osteoarthritis cases. After this, the Clinical features such as age, body mass index, pain score, joint stiffness indicators, and diagnostic codes are normalized [24] using the following equation (2)

$$CF_{Normalization} = \frac{CF - \mu}{\sigma} \quad (2)$$

Where CF depicts the Knee Osteoarthritis clinical feature, μ depicts the mean of the Knee Osteoarthritis clinical feature and σ depicts the standard deviation of the Knee Osteoarthritis clinical feature. By this, it handles variations in patient demographics. After normalization, all clinical Knee Osteoarthritis features are encoded into a single feature vector using following equation (3)

$$F_E = [CF_{Normalization\ 1}, CF_{Normalization\ 2}, \dots, CF_{Normalization\ D_{CF}}] \quad (3)$$

Where F_E depicts encoded clinical feature vector for a Knee Osteoarthritis case and D_{CF} depicts the total number of clinical features. Then, knee joint images are retrieved and standardized using the following equation (4-5)

$$KI \in \mathbb{R}^{224 \times 224 \times 3} \quad (4)$$

$$KI_{Normalization} = \frac{KI - KI_{Min}}{KI_{Max} - KI_{Min}} \quad (5)$$

This normalized knee image provides a consistent visual representation of joint space narrowing, osteophyte formation, cartilage degradation, and subchondral bone changes.

3.3 Local Feature Extraction and Refinement using Multi-Convolution Spatial and Efficient Squeeze-Excitation Network

Following the pre-processing stage, a feature extraction process is utilized to capture visual patterns relevant to knee osteoarthritis. The architecture diagram of the Multi-Convolution Spatial and Efficient Squeeze-Excitation Network is given in Figure 2. This normalized knee image $KI_{Normalization}$ is passed through a convolutional backbone (ResNet-34) to extract multi-level Knee Osteoarthritis (KOA) visual features as defined using equation (6)

$$F_{KOA} \in \mathbb{R}^{H_t \times W_t \times C}$$

(6)

where F_{KOA} depicts multi-level Knee Osteoarthritis visual features such as joint space narrowing, osteophyte formation, cartilage degradation, and subchondral bone changes [25]. To enhance feature representation, a channel and spatial attention mechanism is applied to capture subtle pathological changes such as cartilage thinning, osteophytes, joint space narrowing, and subchondral bone alterations.

Here, Condensed Depthwise Squeeze-Excitation (CDSE) module is utilized which prioritizes channels associated with pathological joint features. In this, Channel Feature Extract (CFE) block processes the intermediate feature map $F_{KOA} \in \mathbb{R}^{H_t \times W_t \times C}$ using the following equation (7)

$$F_{CFE} = \text{Mish}[CFE_{RES}(F_{KOA}) + CFE_{Skip}(F_{KOA})]$$

(7)

Where CFE_{RES} and CFE_{Skip} represent the residual and skip connections of the CFE block. And, the Mish activation function is defined using the following equation (8)

$$\text{Mish}(y) = y * \tanh[\ln(1 + e^y)]$$

(8)

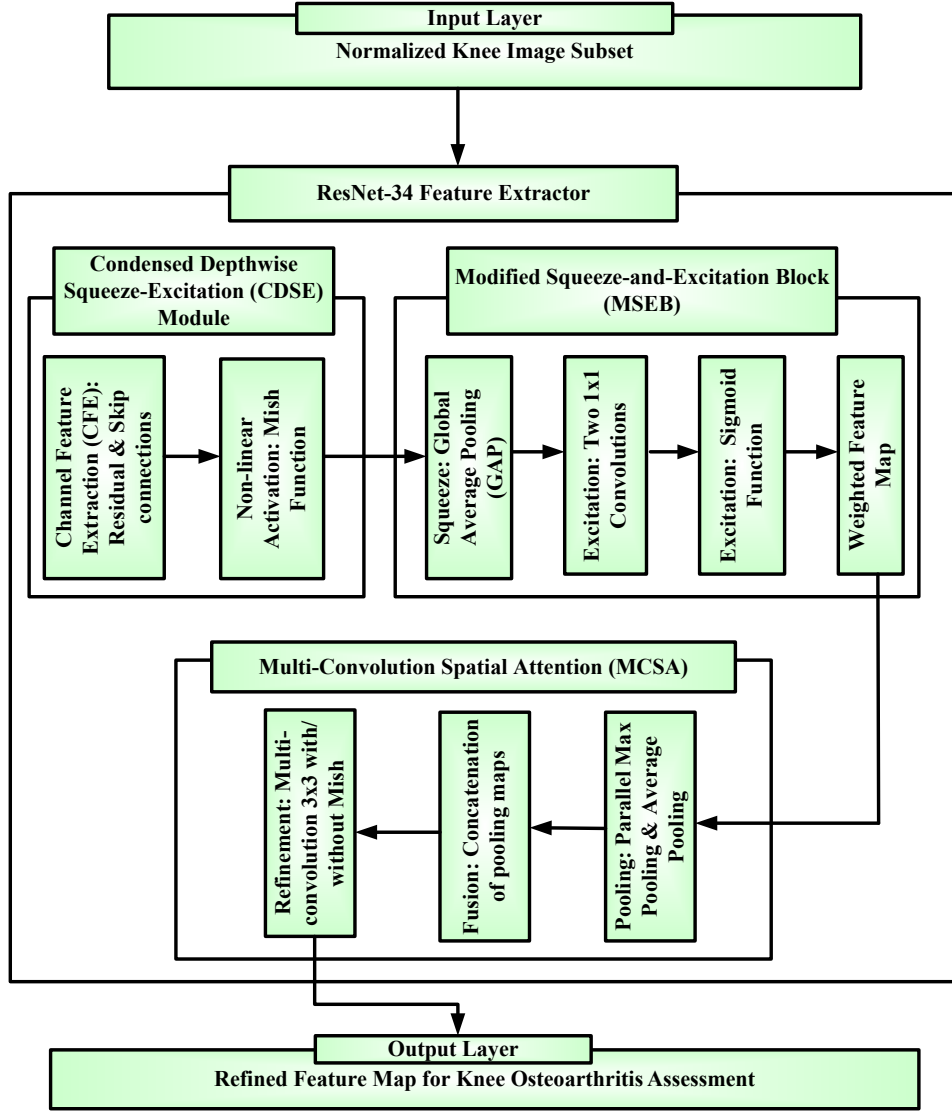


Figure 2: Architecture diagram of the Multi-Convolution Spatial and Efficient Squeeze-Excitation Network

This condensed features are fed into the modified Squeeze-and-Excitation block (MSEB). Here, a Global Average Pooling (GAP) operation is utilized, which unifies the joint-level information using the following equation (9)

$$f = \frac{1}{Ht \times Wt} \sum_{u=1}^{Ht} \sum_{v=1}^{Wt} k_i(u, v) \quad (9)$$

Where Ht , Wt depicts the height and width of the feature map; k_i represents the i^{th} channel. By this, the final weighted feature map is calculated using the following equation (10)

$$F_{\text{CDSE Out}} = \beta \left[\text{conv}^2 \left[\text{GAP}(F_{\text{MSEB}}) \right] \right] \otimes F_{\text{KOA}} \quad (10)$$

Where GAP denotes global average pooling, $conv^2$ indicates two 1×1 convolutional layers, and β is the Sigmoid function. This process enhances the discriminative features linked to cartilage thinning, osteophytes, and sclerosis.

Multi-Convolution Spatial Attention (MCSA) for Spatial Refinement

In this, the MCSA block focus on anatomically relevant knee regions such as the tibiofemoral regions and cartilage surfaces. Here, Max and average pooling is employed to extract spatial information using the following equation (11) and (12)

$$F_{Max} = \text{Max}[k_i(u, v)] \quad (11)$$

$$F_{Average} = \frac{1}{C} \sum_{i=1}^C [k_i(u, v)] \quad (12)$$

Where k_i represents the i^{th} channel of the input maps. Then, Max and average pooling are concatenated using the following equation (13)

$$F_{Cat} = \text{Concat}[F_{Max}, F_{Average}] \quad (13)$$

Here, spatial-refined feature map is produced with the help of the following equation (14)

$$F_{MCSA \text{ Out}} = \beta \left[\text{conv}[\text{ConM}^2(F_{Cat})] \right] \otimes F_{MCSA \text{ In}} \quad (14)$$

Where conv and ConM^2 represent 3×3 convolutional layers without and with the Mish function respectively. This attention mechanism prioritizes knee joint space, tibiofemoral regions, and cartilage surfaces relevant to Knee Osteoarthritis assessment.

3.4 Privacy-Preserving Asynchronous Federated Learning

Here, privacy-preserving asynchronous federated learning (AFL) framework was employed to support sustainable AI-driven Knee Osteoarthritis (KOA) diagnosis across distributed healthcare institutions without centralized data sharing. By this, sustainability is achieved through reduced communication cost, energy consumption, and privacy risk [26]. This Privacy-Preserving Asynchronous Federated Learning optimized a regularized empirical risk minimization problem for vertically partitioned data using the following equation (15)

$$\min_{\theta} f(\theta) = \frac{1}{M} \sum_{h=1}^M LF(\theta^T p_h, q_h) + g(\theta) \quad (15)$$

where p_h denotes the input feature vector, q_h denotes the corresponding label, $LF(.)$ represents the loss function, $g(\theta)$ denotes the regularization term, θ depicts Global model weights, and M denotes the number of samples.

Vertically Partitioned Healthcare Data

Here, each Knee Osteoarthritis (KOA) feature vector is vertically partitioned across R healthcare institutions using equation (16)

$$f = [f_{G_1}, f_{G_2}, \dots, f_{G_R}] \quad (16)$$

where $f_{G_q} \in \mathbb{R}^{d_q}$ represents the feature subset stored at the q^{th} healthcare institution and $[\sum_{q=1}^R d_q = d]$.

Asynchronous Local Gradient Computation

At each iteration, an unbiased stochastic gradient update was performed using the following equation (17)

$$\theta \leftarrow \theta - \delta \times \omega \quad (17)$$

where δ denotes the learning rate and ω represents the stochastic gradient. For AFL, the stochastic gradient was defined using the following equation (18)

$$\omega = \nabla f_h(\theta) \quad (18)$$

where $f_h(\theta)$ corresponds to the loss associated with the sampled instance (p_h, q_h) .

Privacy-Preserving Inner Product Evaluation

Here, each of the ten simulated institutional clients was locally computed a partial inner products $\vartheta_{G_q}^T(p_h)_{G_q}$ for preventing the exposure of raw patient features $(p_h)_{G_q}$. For secure transmission, a tree-structured asynchronous communication protocol was implemented based on the following equation (19)

$$\eta = \sum_{q=1}^{10} [\vartheta_{G_q}^T(p_h)_{G_q}] \quad (19)$$

Where q denotes the 10 simulated institutional clients. To mitigate inference attacks, a random mask was added using the following equation (20)

$$\vartheta_{G_q}^T(p_h)_{G_q} + mk_q \quad (20)$$

The true value is recovered using the following equation (21)

$$\sum_{q=1}^{10} [\vartheta_{G_q}^T(p_h)_{G_q} + mk_q] - \sum_{q=1}^{10} mk_q = \vartheta^T(p_h) \quad (21)$$

where mk_q denotes a random masking number generated by the q^{th} institutional client for a specific instance h .

Sustainable Asynchronous Optimization Strategies

To further stabilize training under asynchronous execution and address the staleness caused by varying communication speeds between institutions, Asynchronous Federated Stochastic Gradient Descent for Vertical Partitioning (AFSGD-VP) algorithms was integrated. Here, AFSGD-VP updates the local parameters using equation (22)

$$\vartheta_{t+1} = \vartheta_t - \delta \times X_{\varphi(t)\omega_t^{\varphi(t)}} \quad (22)$$

Where δ denotes the learning rate and $\varphi(t) \in \{1, 2, \dots, 10\}$ represents the specific institutional client completing the update at time t . This strategy confirms the global model convergence even when the ten distributed institutions possessed unbalanced computational resources.

3.5 Bulyan-Based Adaptive Differential Privacy

In this section, robustness and privacy are enhanced in asynchronous federated learning by integrating Bulyan aggregation with adaptive differential privacy.

Bulyan-Based Robust Aggregation

To mitigate Byzantine and poisoned updates, Bulyan aggregation is applied at the server side. Initially, reliable gradients are selected using Multi-Krum by computing the Krum score [27] for each update Δz_a based on the following equation (23)

$$Score(a) = \sum_{b \in NN_a} \|\Delta z_a - \Delta z_b\|_2^2 \quad (23)$$

Where NN_a represents the set of $(N - mc - 2)$ nearest neighbors. mc depicts the maximum number of malicious clients. $\|\Delta z_a - \Delta z_b\|_2^2$ represents the squared Euclidean distance between updates from client a and client b . Following the selection of the candidate set I , the Bulyan aggregator performs coordinate-wise trimmed mean for each parameter dimension dim to produce the final aggregated update using the following equation (24)

$$\Delta z_{AU}[dim] = \frac{1}{|I| - 2 \times \rho \times |I|} \sum_{a \in I / \text{Outliers}} s_a[dim] \quad (24)$$

Where $\Delta z_{AU}[dim]$ depicts the robust aggregated update for dimension dim . It represents the candidate set of updates selected by the Multi-Krum stage. ρ depicts the trim ratio, which is commonly proportional to the fraction of malicious clients. $s_a[dim]$ represents the value of the dim dimension for the s^{th} candidate update. This two-stage aggregation filters out adversarial and noisy updates while preserving informative gradients relevant to Knee Osteoarthritis learning.

Adaptive Differential Privacy

To maintain strict (ϵ, δ) privacy while preserving model utility, an adaptive noise-scheduling mechanism is utilized. The standard deviation of the Gaussian noise σ_g is adjusted across training rounds using an exponential decay schedule and it is given in the equation (25)

$$\sigma_g = 0.30 \exp(-0.01g) \quad (25)$$

Where σ_g depicts the noise multiplier for differential privacy in round g . 0.30 represents the initial noise level at the start of training. 0.01 depicts the decay constant for noise reduction. g represents the current federated learning round. Then, each institutional Δz_a update is masked before aggregation using the following equation (26)

$$\tilde{n}g_a = \Delta z_a + N(0, \sigma_g^2 \times C^2 \times IM_{dim}) \quad (26)$$

Where, $\tilde{n}g_a$ depicts the noised gradient update for client a . Δz_a represents the local gradient update from the institutional client. $N(0, \sigma_g^2 \times C^2 \times IM_{dim})$ depicts the Gaussian noise distribution with mean zero. C represents the clipping threshold for the gradient norm to bound sensitivity. IM_{dim} depicts the identity matrix for the dim dimensional parameter space. Through the joint application of Bulyan aggregation and adaptive differential privacy, the proposed framework achieves resilience against malicious clients, mitigates inference attacks, and sustains privacy-aware learning for distributed Knee Osteoarthritis diagnosis.

By this, the proposed AFL-MCSESEN-BADP-HS system attains robust, privacy-preserved global Knee Osteoarthritis diagnostic model by integrating Bulyan-based aggregation with adaptive differential privacy under asynchronous federated learning.

4. RESULTS AND DISCUSSION

In this section, the performance of the proposed Asynchronous Federated Multi-Convolution Spatial and Efficient Squeeze-Excitation Network (AFL-MCSESEN) with Bulyan-Based Adaptive Differential Privacy (BADP) for Privacy-Preserving Multi-Modal Data Fusion in Sustainable AI-Driven Healthcare Systems (HS) (AFL-MCSESEN-BADP-HS) was evaluated. The experiments evaluation of the AFL-MCSESEN-BADP-HS system were conducted on high-performance workstation equipped with an Intel Core i7 CPU, 32GB RAM, and an NVIDIA GPU for supporting deep learning operations and multi-modal data processing. The proposed AFL-MCSESEN-BADP-HS system is implemented in Python. Here, PyTorch was utilized for the proposed MCSESEN architecture and Apache Spark was utilized for the management of the heterogeneous data lake containing structured Electronic Medical Records (EMRs), semi-structured CSV/JSON healthcare records, and unstructured imaging such as X-ray, MRI, CT, and PET scans. The dataset was divided into training (60%), validation (20%), and testing (20%) sets. The dataset distribution is categorized by Kellgren-Lawrence (KL) grades for the assessment of Knee Osteoarthritis and it is given in Table 1. During the data acquisition phase, structured, semi-structured, and unstructured medical information from Beijing Tsinghua Changgung Hospital is fused into a unified element tree structure using matching keys to create a queryable Spark DataFrame. Also, Asynchronous federated learning make decentralized training across ten simulated institutional clients. To mitigate inference attacks, random masking variables are integrated into the inner product evaluations. Furthermore, Bulyan-based adaptive differential privacy is utilized against adversarial threats while maintaining strict data protection standards. This experimental setup provides sustainable, high-accuracy diagnostic tool for Knee Osteoarthritis. The experimental results of the proposed AFL-MCSESEN-BADP-HS system is compared with the existing system like Healthcare System based on Federated Learning (PHMS-Fed) [16], Federated Learning, Tiny Machine Learning, and Differential Privacy for Healthcare Systems (FL-TinyML-DP-HS) [17] and Federated Learning with Convolutional Neural Networks, Long Short-Term Memory, Differential Privacy, and Encryption Techniques for Healthcare Systems (FL-CNN-LSTM-DPET-HS) [18] respectively. The confusion matrix of the proposed AFL-MCSESEN-BADP-HS system is given in Figure 3.

Table 1: Dataset distribution is categorized by Kellgren-Lawrence (KL) grades for the assessment of Knee Osteoarthritis

Knee Osteoarthritis Stage (KL Grade)	Total Cases	Training (60%)	Validation (20%)	Testing (20%)
Grade 0 (Healthy)	1,420	852	284	284
Grade 1 (Doubtful)	1,240	744	248	248
Grade 2 (Mild)	1,160	696	232	232
Grade 3 (Moderate)	990	594	198	198
Grade 4 (Severe)	770	462	154	154
Total	5,580	3,348	1,116	1,116

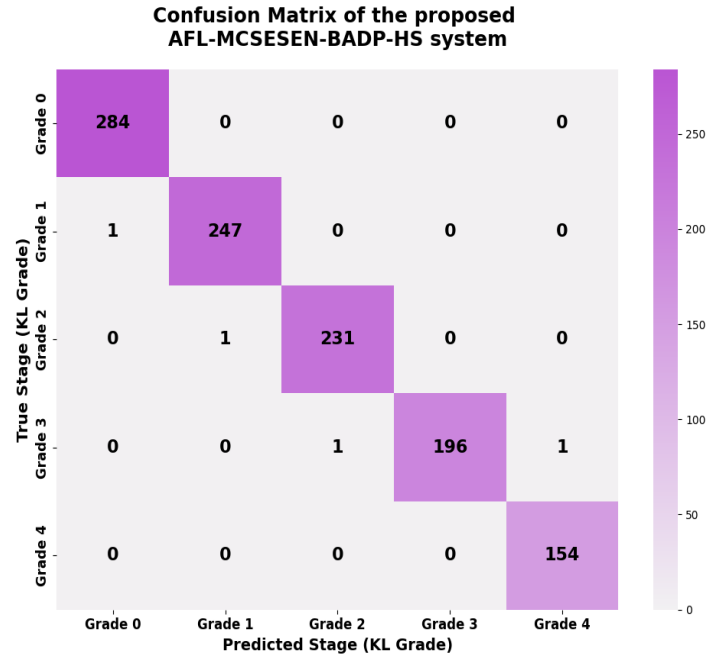


Figure 3: Confusion Matrix of Proposed AFL-MCSESEN-BADP-HS System

4.1 Performance Metrics

In this section, various metrics used to evaluate the proposed AFL-MCSESEN-BADP-HS system for sustainable Knee Osteoarthritis diagnosis are defined below,

4.1.1 Multi-Modal Fusion & Data Management

A. Data Integration Latency

Data integration latency is defined as the total time required to perform data acquisition, processing, and fusion of heterogeneous sources (structured, semi-structured, and unstructured) into a single queryable Spark DataFrame. It is calculated using following equation (27)

$$\text{Data integration latency} = \text{Time}_{\text{acquisition}} + \text{Time}_{\text{processing}} + \text{Time}_{\text{fusion}} \quad (27)$$

Where, $\text{Time}_{\text{acquisition}}$ represents Time taken to retrieve data from the decentralized institutional clients and the Beijing Tsinghua Changgung Hospital sources. $\text{Time}_{\text{processing}}$ represents the Time required for PyTorch and Spark to analyse EMRs and extract features from high-resolution imaging (X-ray, MRI, etc.). $\text{Time}_{\text{fusion}}$ represents the Time taken to execute the matching keys logic and merge diverse data types into the Unified Element Tree.

B. Spark Query Throughput

It is calculated using following equation (28)

$$\text{Spark Query Throughput} = \frac{\text{Total successful diagnostic queries}}{\left[\text{Execution time per query (includes model inference)} + \text{Idle time (network bottlenecks or asynchronous lag)} \right]} \quad (28)$$

4.1.2 Diagnostic Performance Metrics

In this section, various Diagnostic Performance Metrics are used to evaluate the ability of the proposed AFL-MCSESEN-BADP-HS system for classifying Kellgren-Lawrence (KL) grades correctly.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad (29)$$

Where TP (True Positives) depicts Correct classification of a specific Knee Osteoarthritis KL grade (e.g., the model correctly identifies a “Grade 3” image as “Grade 3”); FP (False Positives) indicates model incorrectly assigns a different grade to a specific category (e.g., a “Grade 2” image is wrongly labeled as “Grade 3”). FN (False Negatives) denotes model fails to identify the actual KL stage (e.g., a “Grade 3” image is missed and labeled as “Grade 4”). TN (True Negatives) depicts Correct identification of the absence of a specific KL stage (e.g., correctly deciding that a “Grade 0” image is not “Grade 3”).

$$\text{Sensitivity (Recall)} = \frac{TP}{(TP + FN)} \quad (30)$$

$$F1 \text{ Score} = \frac{2 \times (\text{Precision} \times \text{Sensitivity})}{(\text{Precision} + \text{Sensitivity})} \quad (31)$$

$$\text{Precision} = \frac{TP}{(TP + FP)} \quad (32)$$

$$\text{Specificity} = \frac{TN}{(TN + FP)} \quad (33)$$

4.1.3 Federated Learning Performance Metrics

a. Convergence Rate

Convergence rate measures the reduction in error across successive communication rounds. It is calculated using the following equation (34)

$$\text{Convergence Rate} = \frac{\Delta \text{Accuracy}}{\Delta \text{Communication rounds}} \quad (34)$$

b. Communication Overhead

Communication overhead quantifies the total volume of data transmitted between the decentralized institutional clients and the central server. It is calculated using the following equation (35)

$$\text{Communication Overhead} = \sum_{r=1}^R (S_{\text{upload}} + S_{\text{download}}) \times N_{\text{clients}} \quad (35)$$

Where S_{upload} and S_{download} represents Size of uploaded/downloaded model updates. N_{clients} represents the Total number of participating institutional clients. R depicts the Total communication rounds.

4.1.4 Privacy and Robustness Metrics

Privacy Budget

The Privacy Budget measures the privacy loss.

Byzantine Resilience Rate

$$\text{Byzantine Resilience Rate} = \frac{\text{Number of correctly aggregated updates after Bulyan filtering}}{\text{Total number of participating clients}} \quad (36)$$

Attack Success Rate

$$\text{Attack Success Rate} = \frac{\text{Number of attacks that successfully infer sensitive information or corrupt the global model}}{\text{Total number of simulated attacks}} \quad (37)$$

Privacy–Utility Trade-off Index (PUTI)

$$\text{Privacy–Utility Trade-off Index (PUTI)} = \frac{\text{Accuracy}}{\text{Differential privacy budget}} \quad (38)$$

4.2 Performance Metrics Analysis

4.2.1 Multi-Modal Fusion & Data Management Analysis

Figures 4 visually illustrate the Multi-Modal Fusion & Data Management Analysis. Here, comparative evaluation of Data Integration Latency and Spark Query Throughput

between the proposed AFL-MCSESEN-BADP-HS system is compared with the existing system like PHMS-Fed [16], FL-TinyML-DP-HS [17] and FL-CNN-LSTM-DPET-HS [18] respectively.

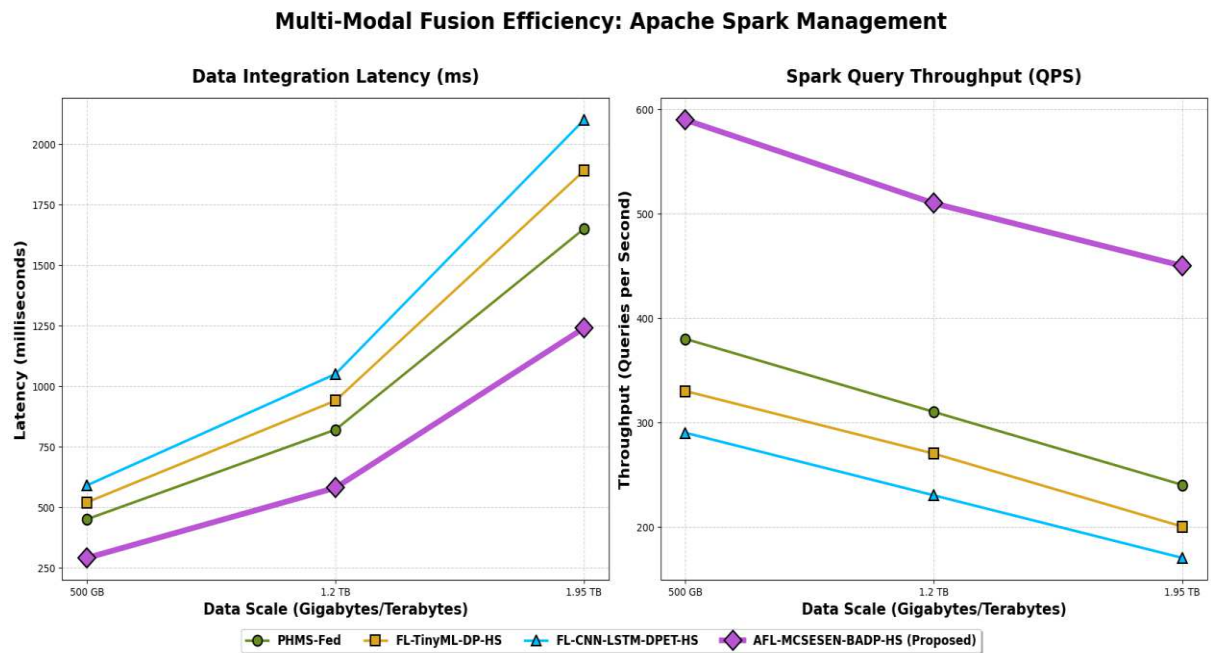


Figure 4: Multi-Modal Fusion & Data Management Analysis

Figure 4 depicts the Multi-Modal Fusion & Data Management Analysis. Here, the proposed AFL-MCSESEN-BADP-HS system achieved reductions in Data Integration Latency of 35.56%, 44.23% and 50.85% for 500 GB data volume; 29.27%, 38.30% and 44.76% for 1.2 TB data volume and 24.85%, 34.39% and 40.95% for 1.95 TB data volume when compared to existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively. Also, the proposed AFL-MCSESEN-BADP-HS system demonstrated a notable enhancement in Spark Query Throughput. Specifically, it exhibited a 35.59%, 44.06% and 50.84% improvement in Spark Query Throughput for 500 GB data volume, 39.21%, 47.05% and 54.901% higher Spark Query Throughput for 1.2 TB data volume and 46.66%, 55.55% and 62.22% higher Spark Query Throughput for 1.95 TB data volume compared with the existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively. These results demonstrate superior efficiency in handling large-scale heterogeneous medical data.

4.2.2 Diagnostic Performance Metrics

Figures 5-10 visually illustrate the Knee Osteoarthritis Diagnostic Performance Metrics Analysis of the proposed AFL-MCSESEN-BADP-HS system is compared with the

existing system like PHMS-Fed [16], FL-TinyML-DP-HS [17] and FL-CNN-LSTM-DPET-HS [18] respectively.

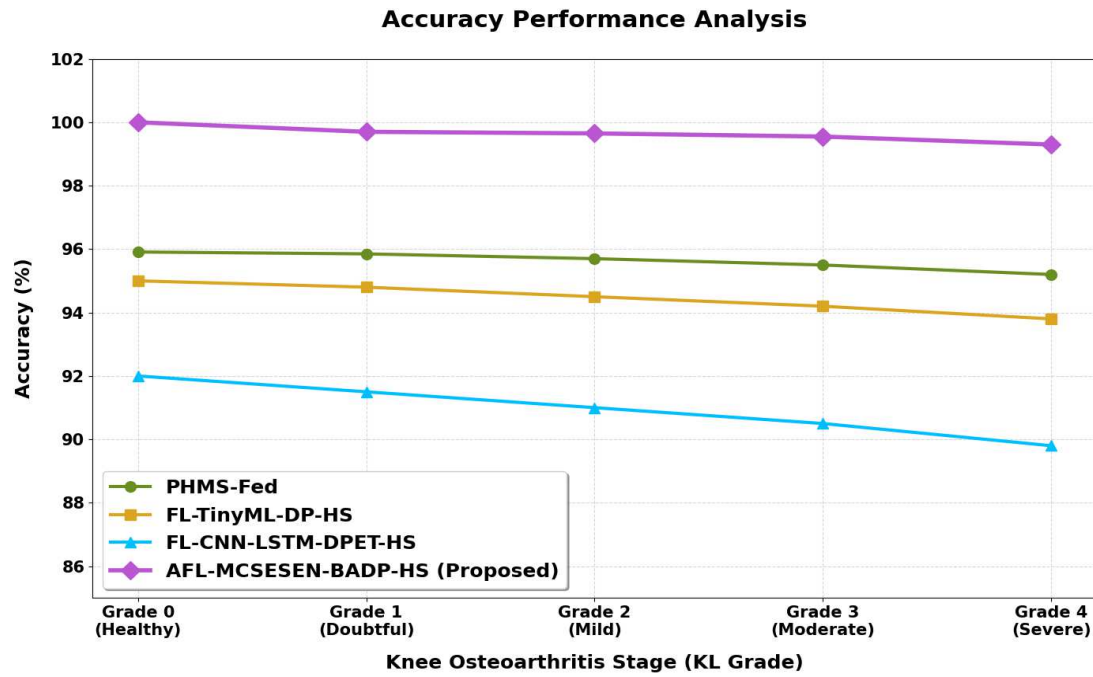


Figure 5: Accuracy analysis across various Knee Osteoarthritis Stage (KL Grade)

Figure 5 depicts the Accuracy analysis across various Knee Osteoarthritis Stage (KL Grade). For Grade 0 (Healthy) analysis, the proposed AFL-MCSESEN-BADP-HS system achieves an accuracy increase of 3.79% against PHMS-Fed, 4.55% over FL-TinyML-DP-HS, and 7.95% when compared to FL-CNN-LSTM-DPET-HS. In the detection of Grade 1 (Doubtful), the proposed AFL-MCSESEN-BADP-HS system shows an 3.85% higher accuracy against PHMS-Fed, a 4.73% increase over FL-TinyML-DP-HS, and a 8.13% improvement with respect to FL-CNN-LSTM-DPET-HS. For Grade 2 (Mild) analysis, the proposed AFL-MCSESEN-BADP-HS system achieves an accuracy increase of 3.91% against PHMS-Fed, 4.89% over FL-TinyML-DP-HS, and 8.32% when compared to FL-CNN-LSTM-DPET-HS. In the detection of Grade 3 (Moderate), the proposed AFL-MCSESEN-BADP-HS system shows an 3.91% higher accuracy against PHMS-Fed, a 5.01% increase over FL-TinyML-DP-HS, and a 8.44% improvement with respect to FL-CNN-LSTM-DPET-HS. Finally, for Grade 4 (Severe) analysis, the proposed AFL-MCSESEN-BADP-HS system achieves an accuracy increase of 3.96% against PHMS-Fed, 5.24% over FL-TinyML-DP-HS, and 8.69% when compared to FL-CNN-LSTM-DPET-HS.

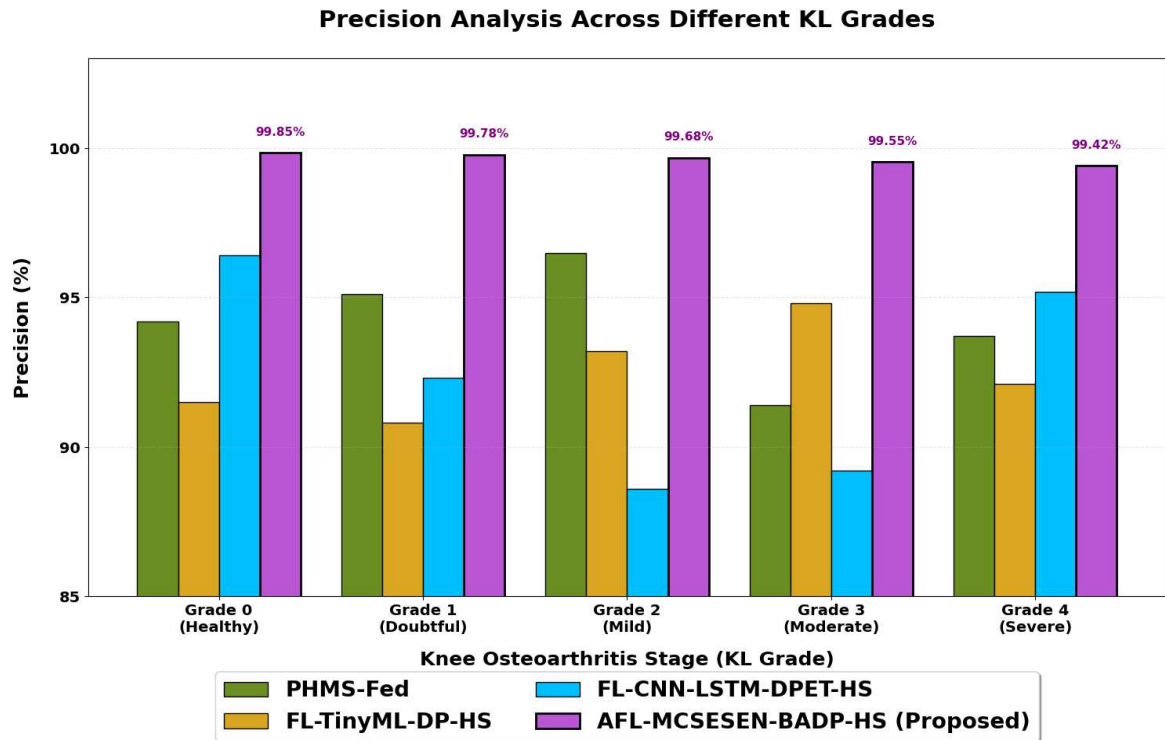


Figure 6: Precision analysis across various Knee Osteoarthritis Stage (KL Grade)

Figure 6 depicts the Precision analysis across various Knee Osteoarthritis Stage (KL Grade). Here, the proposed AFL-MCSESEN-BADP-HS system attains 6.00%, 9.13% and 3.58% higher precision for Grade 0 (Healthy) analysis; 4.92%, 9.89% and 8.10% higher precision for Grade 1 (Doubtful) analysis; 3.30%, 6.95% and 12.51% higher precision for Grade 2 (Mild) analysis; 8.92%, 5.01% and 11.60% higher precision for Grade 3 (Moderate) analysis; 6.10%, 7.95% and 4.43% higher precision for Grade 4 (Severe) analysis compared with the existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively.

Figure 7 depicts the recall analysis across various Knee Osteoarthritis Stage (KL Grade). For Grade 0 (Healthy) analysis, the proposed AFL-MCSESEN-BADP-HS system achieves an recall increase of 8.09% against PHMS-Fed, 4.26% over FL-TinyML-DP-HS, and 10.85% when compared to FL-CNN-LSTM-DPET-HS. In the detection of Grade 1 (Doubtful), the proposed AFL-MCSESEN-BADP-HS system shows an 10.22% higher recall against PHMS-Fed, a 8.31% increase over FL-TinyML-DP-HS, and a 4.34% improvement with respect to FL-CNN-LSTM-DPET-HS. For Grade 2 (Mild) analysis, the proposed AFL-MCSESEN-BADP-HS system achieves recall increase of 5.08% against PHMS-Fed, 11.43% over FL-TinyML-DP-HS, and 9.23% when compared to FL-CNN-LSTM-DPET-HS. In the detection of Grade 3 (Moderate), the proposed AFL-

MCSESEN-BADP-HS system shows an 11.92% higher recall against PHMS-Fed, a 6.42% increase over FL-TinyML-DP-HS, and a 7.22% improvement with respect to FL-CNN-LSTM-DPET-HS. Finally, for Grade 4 (Severe) analysis, the proposed AFL-MCSESEN-BADP-HS system achieves an recall increase of 6.63% against PHMS-Fed, 9.21% over FL-TinyML-DP-HS, and 11.04% when compared to FL-CNN-LSTM-DPET-HS.

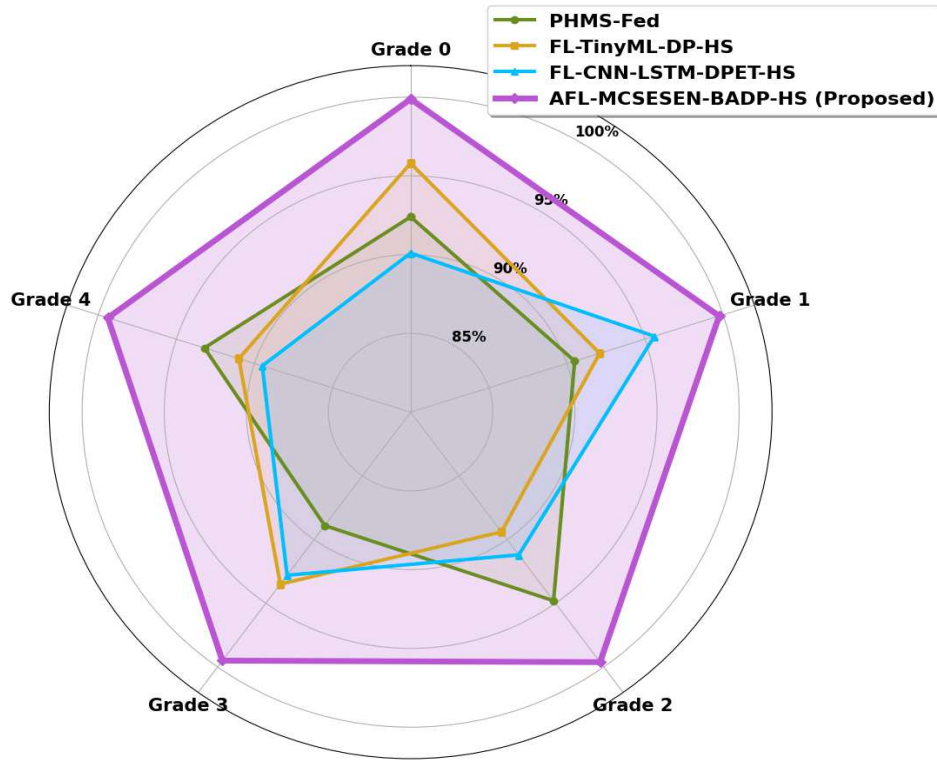


Figure 7: Recall analysis across various Knee Osteoarthritis Stage (KL Grade)

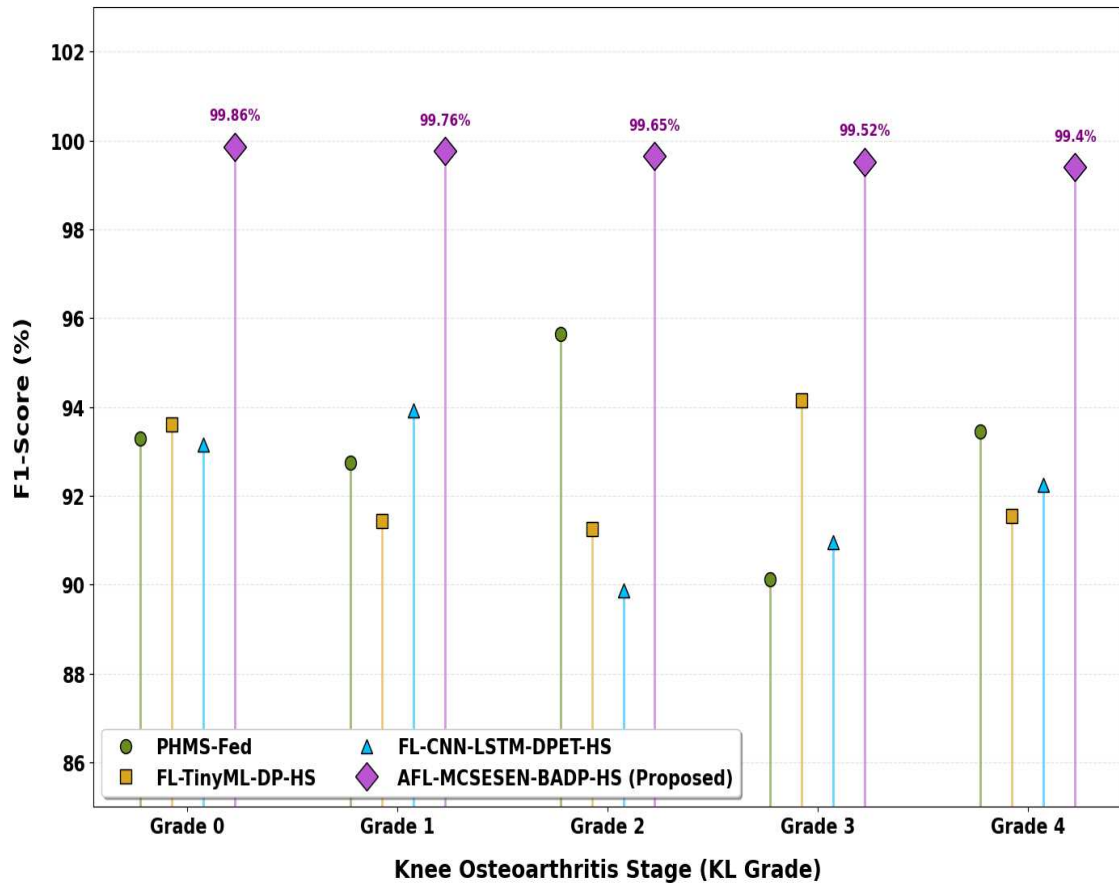


Figure 8: F1-Score analysis across various Knee Osteoarthritis Stage (KL Grade)

Figure 8 depicts the F1-Score analysis across various Knee Osteoarthritis Stage (KL Grade). Here, the proposed AFL-MCSESEN-BADP-HS system attains 7.04%, 6.69% and 7.20% higher F1-Score for Grade 0 (Healthy) analysis; 7.57%, 9.10% and 6.22% higher F1-Score for Grade 1 (Doubtful) analysis; 4.19%, 9.20% and 10.87% higher F1-Score for Grade 2 (Mild) analysis; 10.42%, 5.70% and 9.41% higher F1-Score for Grade 3 (Moderate) analysis; 6.37%, 8.57% and 7.74% higher F1-Score for Grade 4 (Severe) analysis compared with the existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively.

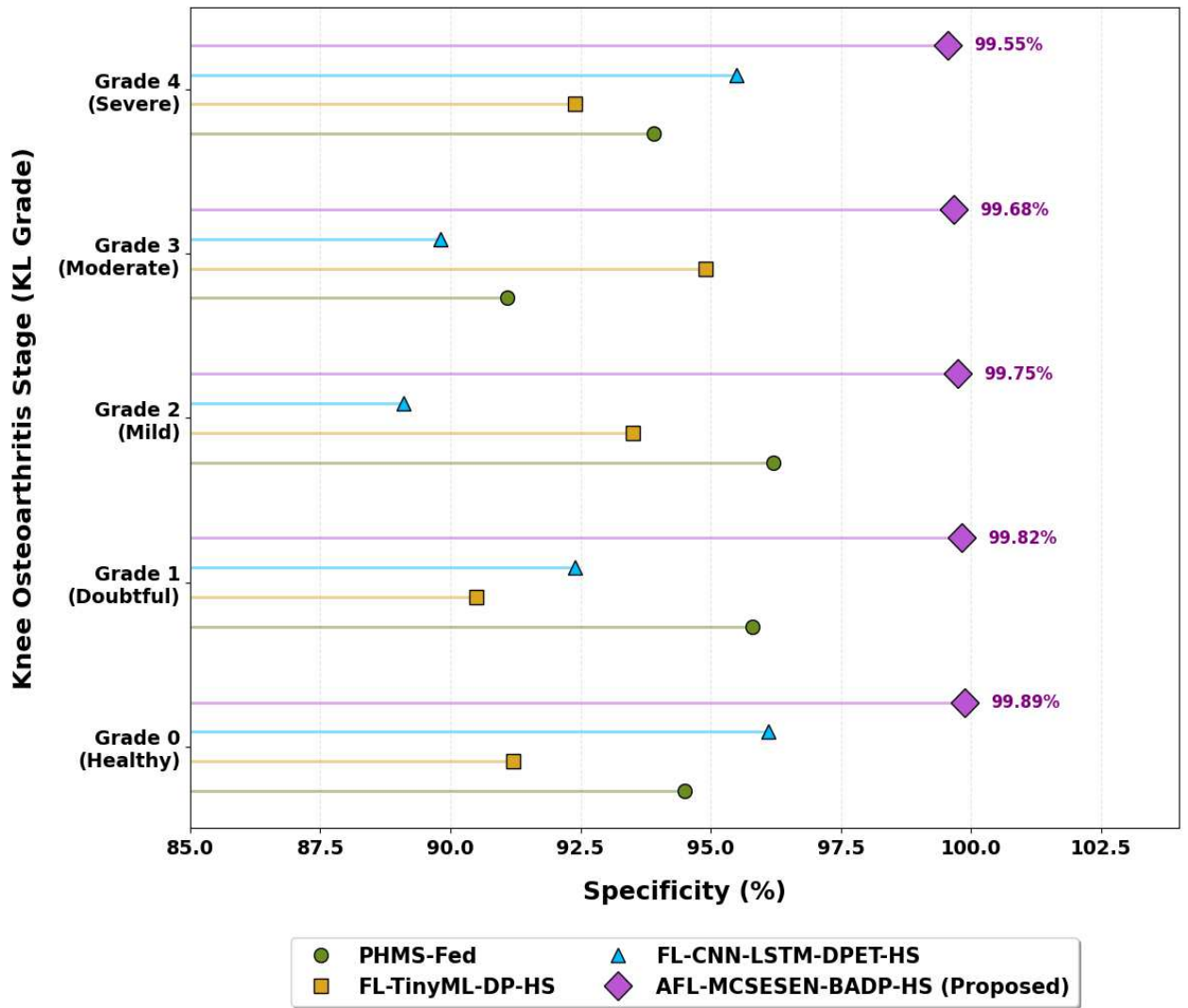


Figure 9: Specificity analysis across various Knee Osteoarthritis Stage (KL Grade)

Figure 9 depicts the Specificity analysis across various Knee Osteoarthritis Stage (KL Grade). Here, the proposed AFL-MCSESEN-BADP-HS system attains 5.70%, 9.53% and 3.94% higher Specificity for Grade 0 (Healthy) analysis; 4.20%, 10.30% and 8.03% higher Specificity for Grade 1 (Doubtful) analysis; 3.69%, 6.68% and 11.95% higher Specificity for Grade 2 (Mild) analysis; 9.42%, 5.04% and 11.00% higher Specificity for Grade 3 (Moderate) analysis; 6.02%, 7.74% and 4.24% higher Specificity for Grade 4 (Severe) analysis compared with the existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively.

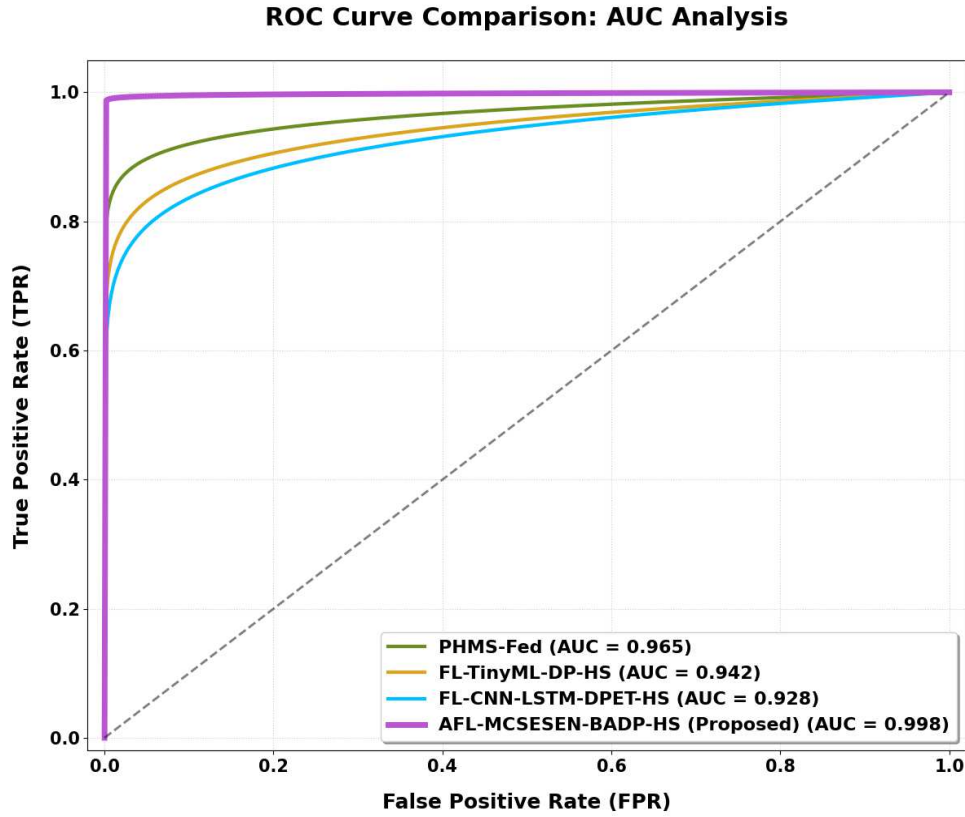


Figure 10: Receiver Operating Characteristic (ROC) Analysis

Figure 10 depicts the Receiver Operating Characteristic (ROC) Analysis. The proposed AFL-MCSESEN-BADP-HS system achieves a 3.40% higher AUC value against the PHMS-Fed. Furthermore, a 6.06% increase in AUC value against the FL-TinyML-DP-HS system. With respect to FL-CNN-LSTM-DPET-HS system, the framework attains a 7.62% higher AUC value. This elevated AUC performance signifies a lower false-positive rate and higher true-positive rate across all Kellgren-Lawrence grades of Knee Osteoarthritis diagnosis.

4.2.3 Federated Learning Performance Metrics

Figures 11-12 visually illustrate the Federated Learning Performance Metrics Analysis of the proposed AFL-MCSESEN-BADP-HS system is compared with the existing system like PHMS-Fed [16], FL-TinyML-DP-HS [17] and FL-CNN-LSTM-DPET-HS [18] respectively.

Figure 11 illustrates the convergence rate analysis across 50 communication rounds for 10 simulated clients. The proposed AFL-MCSESEN-BADP-HS system shows superior performance in both accuracy and loss reduction compared to existing system like PHMS-Fed, FL-TinyML-DP-HS, and FL-CNN-LSTM-DPET-HS respectively.

Figure 12 depicts the Communication Overhead analysis. The proposed AFL-MCSESEN-BADP-HS system achieves lower Communication Overhead of 20.83% against PHMS-Fed, 34.48% over FL-TinyML-DP-HS, and 10.85% when compared to FL-CNN-LSTM-DPET-HS. These results demonstrate superior operational efficiency within the evaluated privacy-preserving asynchronous federated healthcare setting.

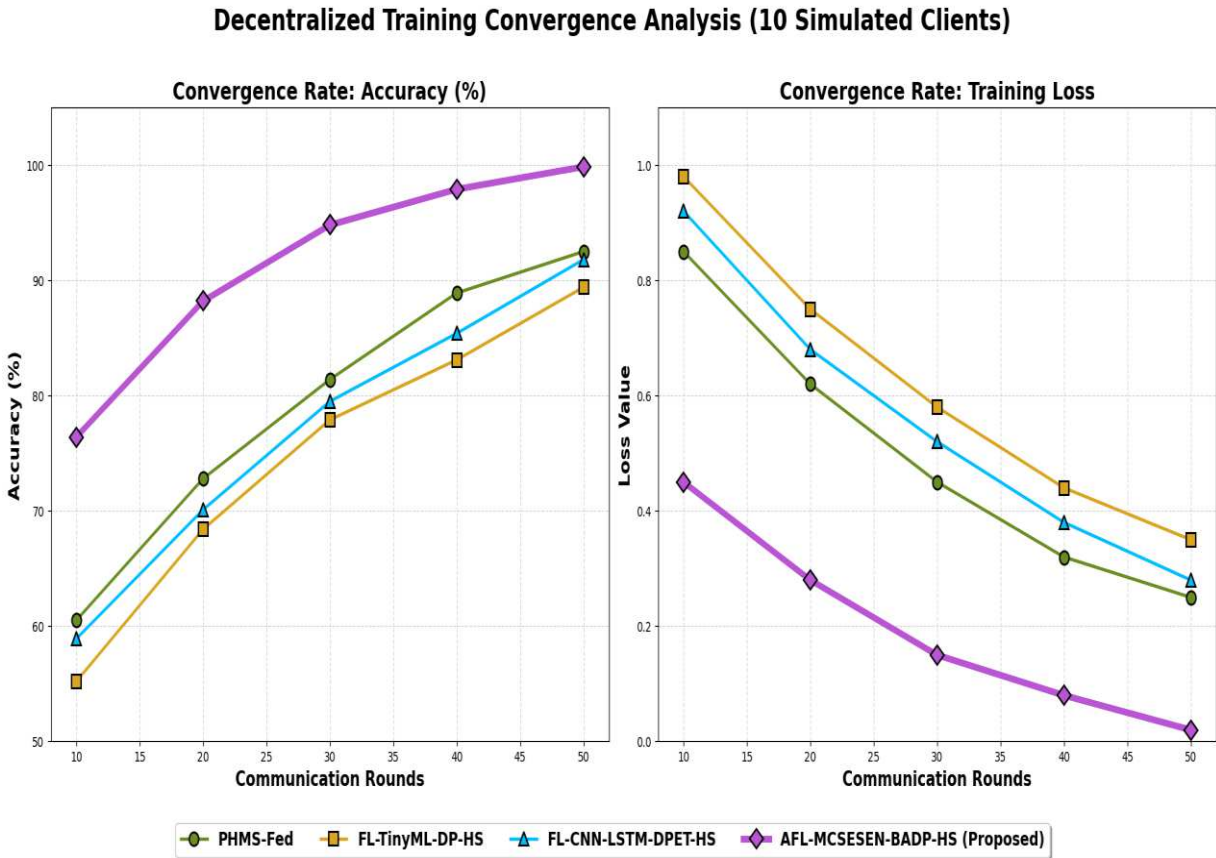


Figure 11: Convergence Rate Analysis

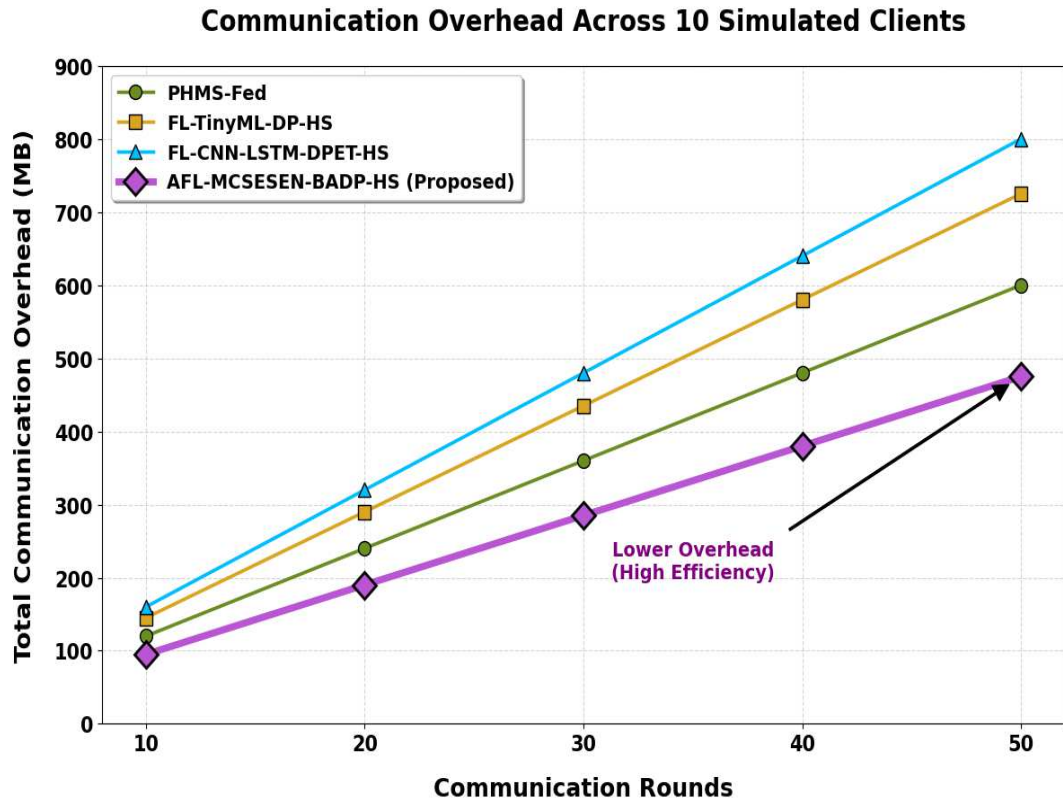


Figure 12: Communication Overhead Analysis

4.2.4 Privacy and Robustness Metrics

Figures 13 visually illustrate the Privacy and Robustness Metrics Analysis of the proposed AFL-MCSESEN-BADP-HS system is compared with the existing system like PHMS-Fed [16], FL-TinyML-DP-HS [17] and FL-CNN-LSTM-DPET-HS [18] respectively.

Figure 13 illustrates the comparative analysis of privacy and robustness metrics for the AFL-MCSESEN-BADP-HS framework. The proposed AFL-MCSESEN-BADP-HS system attains 66.67%, 53.13% and 46.43% lower Privacy Budget (ϵ); 30.56%, 20.51% and 16.05% higher Byzantine Resilience (BRR %); 85.60%, 78.57% and 75.00% lower Attack Success Rate (ASR %) and 41.18%, 21.52% and 17.07% higher Privacy-Utility Index (PUTI) compared with the existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively. These results shows that the integration of Bulyan-based adaptive differential privacy effectively mitigates adversarial threats while maintaining high diagnostic utility in sustainable healthcare environments.

Privacy & Robustness Metrics: AFL-MCSESEN-BADP-HS System Analysis

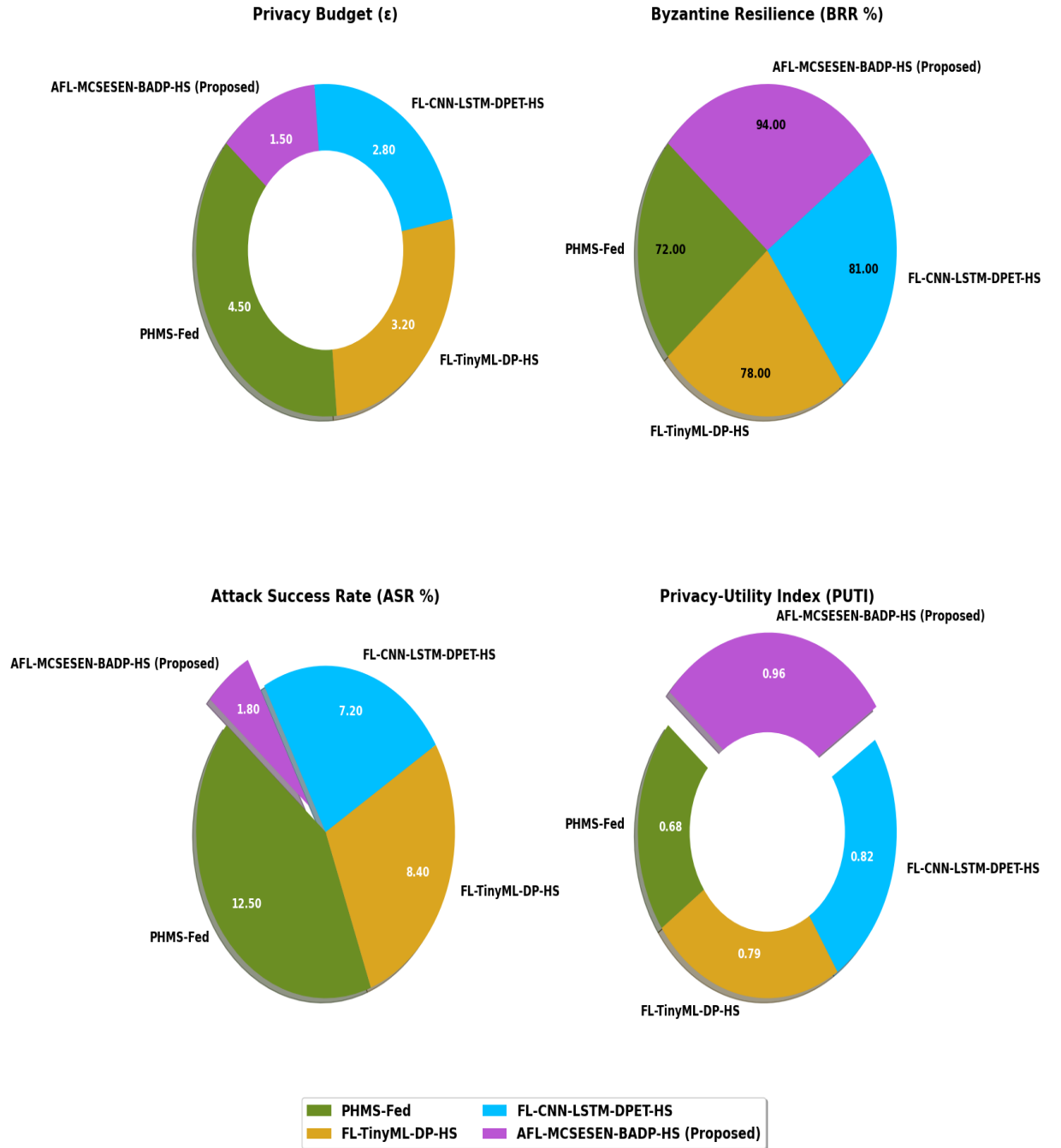


Figure 13: Privacy and Robustness Metrics Analysis

4.4 Discussion

Here, proposed Asynchronous Federated Multi-Convolution Spatial and Efficient Squeeze-Excitation Network (AFL-MCSESEN) with Bulyan-Based Adaptive Differential Privacy (BADP) was successfully implemented for Privacy-Preserving

Multi-Modal Data Fusion in Sustainable AI-Driven Healthcare Systems (HS) (AFL-MCSESEN-BADP-HS). It successfully integrates multi-modal healthcare data through the Unified Element Tree Fusion method to optimize decentralized record management. By combining specialized attention modules for precise Kellgren-Lawrence grading with a Bulyan-based asynchronous federated learning framework, the the AFL-MCSESEN-BADP-HS sytem guarantees high diagnostic utility while mitigating adversarial threats and institutional latency.

Table 2: Overall Average Performance Analysis

	PHMS- Fed	FL- TinyML- DP-HS	FL-CNN- LSTM- DPET-HS	AFL-MCSESEN- BADP-HS (Proposed)
Accuracy (%)	95.91	95	92	99.64
Precision (%)	94.18	92.48	92.34	99.66
Recall (%)	91.96	92.36	91.84	99.63
F1-Score (%)	93.05	92.4	92.03	99.64
Specificity (%)	94.3	92.5	92.58	99.738
AUC	0.965	0.942	0.928	0.998
Communication Overhead (MB)	360	435	480	285
Data Integration Latency (ms)	973.33	1116.67	1246.67	703.33
Spark Query Throughput (QPS)	310	266.67	230	516.67
Privacy Budget (€)	4.5	3.2	2.8	1.5
Byzantine Resilience (%)	72	78	81	94
Attack Success Rate (%)	12.5	8.4	7.2	1.8
Privacy-Utility Index (PUTI)	0.68	0.79	0.82	0.96

Table 2 and Figure 3-13depicts the Overall Average Performance Analysis. The proposed AFL-MCSESEN-BADP-HS method attains notable improvements in the

accuracy values by achieving increases of 3.88%, 4.88% and 8.30%; 5.85%, 7.79% and 8.03% higher precision; 8.39%, 7.93% and 8.54% higher Recall; 7.12%, 7.85% and 8.29% higher F1-Score; 5.806%, 7.858% and 7.832% higher specificity; 3.40%, 6.06% and 7.62% higher AUC Value; 20.83%, 34.48% and 40.62% lower Communication Overhead; 27.73%, 37.01% and 43.58% lower Data Integration Latency; 40.49%, 48.89% and 55.99% higher Spark Query Throughput; 66.67%, 53.13% and 46.43% lower Privacy Budget (ϵ); 30.56%, 20.51% and 16.05% higher Byzantine Resilience (BRR %); 85.60%, 78.57% and 75.00% lower Attack Success Rate (ASR %) and 41.18%, 21.52% and 17.07% higher Privacy-Utility Index (PUTI) compared with the existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively.

In Futurework, applicability of the MCSESEN architecture will be enhanced for additional musculoskeletal disorders and degenerative conditions to validate diagnostic versatility across diverse medical domains. Moreover, refinement of tree-structured communication and gradient masking techniques will be done to minimize bandwidth requirements for institutions with limited infrastructure.

5. CONCLUSION

In this study, the proposed Asynchronous Federated Multi-Convolution Spatial and Efficient Squeeze-Excitation Network with Bulyan-Based Adaptive Differential Privacy was successfully developed and validated to address the challenge faced during Privacy-Preserving Multi-Modal Data Fusion in Sustainable AI-Driven Healthcare Systems. Initially, structured Electronic Medical Records (EMRs), semi-structured CSV/JSON healthcare records, and unstructured imaging such as X-ray, MRI, CT, and PET scans are gathered into a data lake managed by Apache Spark. Subsequently, all collected heterogeneous medical data are fused using Unified Element Tree Fusion method. Here, it merges the matching keys across different modalities and integrates the individual feature vectors into Delta tables or a single queryable Spark DataFrame for Knee Osteoarthritis analysis. Then, these fused data are fed into Z-score normalization and feature vector encoding. Likewise, knee joint images are standardized for getting consistent visual representation of pathological changes. These normalized images are processed through a ResNet-34 backbone followed by a Condensed Depthwise Squeeze-Excitation (CDSE) module and Multi-Convolution Spatial Attention (MCSA) for prioritizing anatomically relevant regions like the tibiofemoral surfaces. Then these resulting local features are utilized within a privacy-

preserving asynchronous federated learning framework where ten institutional clients compute local gradients on vertically partitioned data. Here, tree-structured protocol and random masking was utilized for secure transmission. On the server side, a Bulyan-based robust aggregation strategy was utilized, which has Multi-Krum and a coordinate-wise trimmed mean for filtering adversarial updates. Subsequently, an adaptive differential privacy mechanism was utilized, which applies Gaussian noise to these aggregated updates to maintain strict privacy standards while preserving model utility. Then the finalized global model is redistributed to institutional clients for accurate diagnostic prediction. Here, the proposed AFL-MCSESEN-BADP-HS system attains 3.88%, 4.88% and 8.30% high accuracy; 5.85%, 7.79% and 8.03% higher precision; 8.39%, 7.93% and 8.54% higher Recall; 7.12%, 7.85% and 8.29% higher F1-Score; 5.806%, 7.858% and 7.832% higher specificity; 3.40%, 6.06% and 7.62% higher AUC Value; 20.83%, 34.48% and 40.62% lower Communication Overhead; 27.73%, 37.01% and 43.58% lower Data Integration Latency; 40.49%, 48.89% and 55.99% higher Spark Query Throughput; 66.67%, 53.13% and 46.43% lower Privacy Budget (ϵ); 30.56%, 20.51% and 16.05% higher Byzantine Resilience (BRR %); 85.60%, 78.57% and 75.00% lower Attack Success Rate (ASR %) and 41.18%, 21.52% and 17.07% higher Privacy-Utility Index (PUTI) compared with the existing system like PHMS-Fed, FL-TinyML-DP-HS and FL-CNN-LSTM-DPET-HS respectively. Future research will focus on the diagnostic expansion to musculoskeletal disorders while optimizing communication protocols to minimize bandwidth requirements.

Compliance with Ethical Standards

Conflict of interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Informed Consent

Informed consent does not apply as this was a retrospective review with no identifying patient information.

Funding: Not applicable

Conflicts of interest Statement: Not applicable

Consent to participate: Not applicable

Consent for publication: Not applicable

Availability of data and material:

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Code availability: Not applicable

References

- [1] Sahoo, S.K., Dash, A., Mishra, S.K. and Humayun, M., 2025. Ensembling AI and Federated Learning for Industry 4.0: A Privacy-Preserving Approach in Edge Computing. In *Convergence of AI, Federated Learning, and Blockchain for Sustainable Development* (pp. 49-69). Cham: Springer Nature Switzerland.
- [2] Dhinakaran, D., Raja, S.E., Jasmine, J.J., Kumar, P.V. and Ramani, R., 2025. The Future of Well-Being: AI-Powered Health Management with Privacy at its Core. *Wellness Management Powered by AI Technologies*, pp.363-402.
- [3] Amin, M.S., Ahmad, S. and Loh, W.K., 2025. Federated learning for Healthcare 5.0: a comprehensive survey, taxonomy, challenges, and solutions. *Soft Computing*, 29(2), pp.673-700.
- [4] Huda, M.N., Talukder, M.B. and Kumar, S., 2025. Securing Healthcare AI: Applied Federal Learning. In *Revolutionizing Healthcare 5.0: The Power of Generative AI: Advancements in Patient Care Through Generative AI Algorithms* (pp. 255-272). Cham: Springer Nature Switzerland.
- [5] Bandaru, V.K.R. and Gondi, D.S., 2025, June. Enhancing Oncology Care with IoT and AI: A Federated Learning Approach for Predictive Cancer Analytics. In *International Conference on Data Analytics & Management* (pp. 541-554). Cham: Springer Nature Switzerland.
- [6] Wang, J., Manna, S., Aksoy, M., Sarkar, A., Rahman, M.A., Noorwali, A., Othman, K.M. and Alenazi, M.J., 2025. Empowering secure and sustainable healthcare through federated learning and blockchain synergies in a Medical Internet of Things. *International Journal of Machine Learning and Cybernetics*, pp.1-33.
- [7] Samantray, B.S. and Reddy, K.H.K., 2025. A Federated Learning Approach Towards Hybrid Blockchain, Quantum-Key-Encryption based Distributed System: A Futuristic Healthcare Architecture for Smart Cities. *Blockchain: Research and Applications*, p.100385.
- [8] Karthiga, B., Praneeth, K.R., Saravanan, V. and Rao, T.R.K., 2025. Enhancing cancer detection in medical imaging through federated learning and explainable

artificial intelligence: A hybrid approach for optimized diagnostics. *Egyptian Informatics Journal*, 31, p.100751.

[9] Sharma, S. and Gour, R., 2025. Artificial Intelligence-Enabled Federated Learning Techniques in Healthcare Sector. In *Convergence of AI, Federated Learning, and Blockchain for Sustainable Development* (pp. 71-87). Cham: Springer Nature Switzerland.

[10] Alzoubi, Y.I., Topcu, A.E. and Elbasi, E., 2025. A systematic review and evaluation of sustainable AI algorithms and techniques in healthcare. *IEEE Access*.

[11] Nithyavani, G. and Raja, G.N., 2025. A comprehensive survey on security and privacy challenges in internet of medical things applications: Deep learning and machine learning solutions, obstacles, and future directions. *IEEE Access*.

[12] Singh, Bhupinder, Anand Nayyar, and Christian Kaunert. "Multi-modal Legal Application on Advanced Federated Learning Technique for Healthcare Industry 4.0: Applications, Taxonomies, and Security-Privacy Issues." In *Convergence of AI, Federated Learning, and Blockchain for Sustainable Development*, pp. 89-101. Cham: Springer Nature Switzerland, 2025.

[13] Khan, S., Perumal, K., Alsolai, H. and Aljohani, A., 2025. FedTinyMed: Federated learning enabled tiny multi task machine learning model for smart healthcare monitoring for IoMT. *Computers and Electrical Engineering*, 128, p.110761.

[14] Pais, V., Rao, S. and Muniyal, B., 2025. Healthcare federated learning: a survey of applications and frameworks. *International Journal of Computers and Applications*, pp.1-20.

[15] Ranjan, A.K. and Kumar, P., 2025. A survey on blockchain-based privacy preserving techniques for edge internet of things. *International Journal of Computers and Applications*, pp.1-12.

[16] Wang, J., Quasim, M.T. and Yi, B., 2025. Privacy-preserving heterogeneous multi-modal sensor data fusion via federated learning for smart healthcare. *Information Fusion*, 120, p.103084.

[17] Aanjankumar, S., Muchahari, M.K., Urooj, S., Kaur, I., Dhanaraj, R.K., Mengash, H.A., Poonkuntran, S. and Kaveri, P.R., 2025. Enhanced Consumer Healthcare Data Protection through AI-Driven TinyML and Privacy-Preserving Techniques. *IEEE Access*.

[18] Dubey, P., Dubey, P. and Bokoro, P.N., 2025. Federated learning for privacy-enhanced mental health prediction with multimodal data integration. *Computer*

Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 13(1), p.2509672.

[19] Siva, O.V. and Anbarasi, M.S., 2025. A Federated Graph-Based Multimodal AI Framework for Privacy-Preserving and Explainable Osteoporosis Detection. International Journal on Artificial Intelligence Tools.

[20] Haripriya, R., Khare, N., Pandey, M. and Biswas, S., 2025. Federated adaptive aggregation: improving privacy and scalability in healthcare AI. Cluster Computing, 28(10), p.617.

[21] Rawas, S. and Samala, A.D., 2025. Dual layer security framework for privacy preserving AI driven healthcare edge cloud analytics. Discover Networks, 1(1), p.8.

[22] Haripriya, R., Khare, N., Pandey, M. and Biswas, S., 2025. A privacy-enhanced framework for collaborative Big Data analysis in healthcare using adaptive federated learning aggregation. Journal of Big Data, 12(1), p.113.

[23] Zhang, Y., Sheng, M., Liu, X., Wang, R., Lin, W., Ren, P., Wang, X., Zhao, E. and Song, W., 2022. A heterogeneous multi-modal medical data fusion framework supporting hybrid data exploration. Health Information Science and Systems, 10(1), p.22.

[24] Kim, Y.S., Kim, M.K., Fu, N., Liu, J., Wang, J. and Srebric, J., 2025. Investigating the impact of data normalization methods on predicting electricity consumption in a building using different artificial neural network models. Sustainable Cities and Society, 118, p.105570.

[25] Feng, Y., Yang, X., Qiu, D., Zhang, H., Wei, D. and Liu, J., 2022. Pcxrnet: Pneumonia diagnosis from chest x-ray images using condense attention block and multiconvolution attention block. IEEE Journal of Biomedical and Health Informatics, 26(4), pp.1484-1495.

[26] Gu, B., Xu, A., Huo, Z., Deng, C. and Huang, H., 2020. Privacy-Preserving Asynchronous Federated Learning Algorithms for Multi-Party Vertically Collaborative Learning. CoRR abs/2008.06233 (2020). arXiv preprint arXiv:2008.06233.

[27] Pandey, S., Singh, O., Pandey, A. and Pandey, C., 2025. Robust and privacy-preserving federated learning against malicious clients: A bulyan-based adaptive differential privacy framework. IEEE Access.