

Privacy-Aware Hybrid Federated Learning Framework with Clustered and Quantum Approaches for Wearable Based Stress Detection

Dr B.V. Rama Krishna ¹, E Meghana ², Nalla Varsha ³, Madasu Vyshanth ⁴, Paasila Thejeshwaar ⁵

¹ Associate Professor, Department of Artificial Intelligence and Data Science, Vignan Institute of Technology and Science, Deshmukhi, Yadadri Bhuvanagiri, Telangana, India

^{2,3,4} Department of Artificial Intelligence and Data Science, Vignan Institute of Technology and Science, Deshmukhi, Yadadri Bhuvanagiri, Telangana, India

Email: bhvr78@gmail.com, meghanagoude@gmail.com, varshavar1218@gmail.com, vyshanthmadasu@gmail.com, thejeshwaar@gmail.com

Article History:

Received: 04-02-2026

Revised: 20-03-2026

Accepted: 10-04-2026

Abstract:

This work presents a hybrid federated learning framework for stress detection using physiological signals collected from wearable sensor devices. The system utilizes the WESAD dataset, which includes multimodal physiological signals such as electrocardiogram (ECG), electrodermal activity (EDA), respiration, and body temperature. A binary classification task is performed to distinguish stress and non-stress conditions after signal preprocessing, normalization, and feature preparation. Feature selection is carried out using a Random Forest classifier to identify the most relevant physiological attributes and reduce dimensionality. A centralized Multilayer Perceptron (MLP) model is first developed as a baseline, followed by a Federated Learning (FL) framework in which multiple client models are trained locally without sharing raw data. To address heterogeneity in client data distributions, Clustered Federated Learning (CFL) is introduced by grouping clients based on model similarity before aggregation. In addition, a Quantum Federated Learning (QFL) approach is incorporated to further enhance the learning framework for stress classification in privacy-preserving settings. Experimental evaluation is conducted under centralized, federated, clustered, and quantum federated settings, and performance is measured using accuracy, precision, recall, and F1-score. The framework demonstrates effective stress detection performance while preserving privacy by ensuring that sensitive physiological data remains decentralized.

Keywords: Federated Learning, Clustered Federated Learning, Quantum Federated Learning, Stress Detection, Wearable Sensor Data, WESAD Dataset, Privacy Preservation, Deep Learning

Stress has become a major health issue in modern society due to increased workloads, lifestyle changes, and constant exposure to digital environments. Long-term stress can lead to serious physical and mental health problems such as cardiovascular diseases, anxiety, depression, and decreased productivity. Therefore, early detection and continuous monitoring are crucial for improving well-being and enabling timely interventions. With advancements in wearable sensor technology, physiological signals like ECG, EDA, respiration, and body temperature can be continuously monitored, offering valuable insights into an individual's stress levels.

Traditional stress detection systems rely on centralized machine learning, where sensitive physiological data is stored on central servers, raising concerns about privacy, security, and data misuse. To overcome these challenges, Federated Learning (FL) enables collaborative model training without sharing raw data, preserving user privacy. Clustered Federated Learning (CFL) further improves performance by grouping similar clients to handle data heterogeneity. Additionally, Quantum Federated Learning (QFL) leverages quantum computing techniques to enhance model efficiency and accuracy. Together, these approaches form a hybrid framework that ensures accurate, robust, and privacy-preserving stress detection using wearable data.

1 Related Work

Recent advancements in privacy-preserving and distributed machine learning have enabled the development of intelligent systems without exposing sensitive data. Traditional centralized approaches, which collect and store raw data in one location, pose serious risks related to privacy, security, and regulatory compliance— particularly in sectors like healthcare and finance. To address these challenges, modern research focuses on Federated Learning (FL) and its advanced variants, often combined with cryptographic and quantum computing techniques, to enable secure and collaborative model training.

Several studies have proposed innovative frameworks to strengthen privacy and efficiency in federated systems. Gupta et al. (2024) introduced a framework that integrates Differential Privacy, Federated Learning, and Quantum Random Number Generators to enhance data confidentiality and resist advanced privacy attacks. Similarly, Islam, Ghasemi, and Mohammed (2022) developed a healthcare-focused FL model that protects patient data while improving efficiency through feature selection and privacy-preserving mechanisms. Madi et al. (2021) further enhanced security using Homomorphic Encryption and Verifiable Computing, allowing computations on encrypted data while ensuring correctness and trust in model aggregation.

In addition, Moon and Lee (2023) highlighted the growing role of federated learning in healthcare applications such as diagnosis, medical imaging, and monitoring, while also addressing associated security challenges. Building on these ideas, Gupta et al. (2024) proposed a hybrid framework incorporating Clustered Federated Learning (CFL) and Quantum Federated Learning (QFL) with a Variational Quantum Classifier to handle data heterogeneity and improve performance. Overall, these studies demonstrate that combining federated learning with clustering, cryptographic methods, and quantum techniques offers a powerful,

scalable, and privacy-aware solution for sensitive predictive applications.

1.1 Literature Review

Privacy preservation in distributed machine learning has emerged as a critical research area due to increasing concerns about data confidentiality, security breaches, and regulatory compliance. Traditional centralized deep learning models often require large-scale data sharing, which is not feasible in sensitive domains such as healthcare and finance. Federated Learning addresses this limitation by enabling decentralized collaborative training, allowing local data to remain on client devices while sharing only model parameters.

Recent studies, such as those by Gupta et al. (2024) and Islam et al. (2022), demonstrate that integrating Differential Privacy and feature selection techniques within federated learning frameworks significantly enhances data protection and computational efficiency. These approaches reduce the risk of information leakage while maintaining high predictive performance. Moreover, the incorporation of quantum-based randomness and secure aggregation mechanisms further strengthens the robustness of distributed learning systems against adversarial attacks.

Cryptographic-based federated learning models, as proposed by Madi et al. (2021), highlight the effectiveness of Homomorphic Encryption and Verifiable Computing in ensuring both confidentiality and integrity during collaborative model updates. Meanwhile, survey-based research by Moon and Lee (2023) emphasizes the expanding role of federated learning across multiple healthcare applications, reinforcing its importance in enabling secure and scalable artificial intelligence deployment.

Hybrid federated architectures incorporating advanced strategies such as Clustered Federated Learning and Quantum Federated Learning offer promising directions for future research. These techniques improve adaptability to heterogeneous data distributions and enhance classification performance in privacy-sensitive environments. Although challenges related to computational complexity and communication overhead remain, ongoing advancements in distributed computing and quantum technologies are expected to further accelerate the adoption of secure federated learning frameworks.

2 Proposed Methodology

The proposed system is implemented using Python due to its strong ecosystem for signal processing, machine learning, deep learning, and distributed learning frameworks. The major implementation components are described below:

- **Physiological Signal Processing:** Multimodal signals (ECG, EDA, respiration, and temperature) are pre-processed using normalization, noise filtering, missing value handling, and scaling to ensure data consistency and improve model performance.
- **Feature Engineering & Baseline Model:** Relevant features are extracted and selected using a Random Forest method, followed by the development of a centralized deep learning model (MLP) to establish baseline stress classification performance.

- **Federated Learning for Privacy:** A Federated Learning (FL) framework is implemented where models are trained locally on client devices, and only model updates are shared, ensuring data privacy and security.
- **Advanced Enhancements (CFL & QFL):** Clustered Federated Learning (CFL) improves handling of heterogeneous data by grouping similar clients, while Quantum Federated Learning (QFL) with a Variational Quantum Classifier enhances accuracy and robustness.
- **Evaluation, Deployment & Feasibility:** Models are evaluated using metrics like accuracy and F1-score with visualizations, then saved for deployment in healthcare systems, demonstrating practical feasibility on standard hardware

2.1 System Architecture

The system architecture for the Hybrid Federated Learning Framework for Stress Detection using Wearable Sensor Data is designed to provide an intelligent and privacy-preserving mechanism for identifying stress conditions from physiological signals. The architecture integrates signal preprocessing, feature selection, centralized deep learning modeling, and distributed federated learning techniques enhanced with clustering and quantum concepts. The system consists of four major interconnected modules, each responsible for a specific stage in the stress detection pipeline

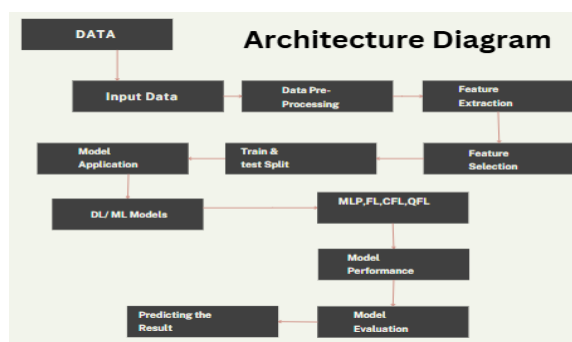


Fig-1: System Architecture

Data Acquisition & Preprocessing: Collect physiological signals (ECG, EDA, respiration, temperature) from wearable devices or datasets, and apply cleaning techniques like filtering, normalization, and segmentation to prepare structured data.

- **Feature Selection & Baseline Model:** Use Random Forest for selecting important features and build a centralized MLP model to perform initial stress vs non-stress classification.
- **Advanced Federated Learning Framework:** Implement Federated Learning (FL) for privacy, enhance with Clustered Federated Learning (CFL) to handle data heterogeneity, and integrate Quantum Federated Learning (QFL) to improve accuracy and robustness.
- **Evaluation & Visualization:** Evaluate model performance using metrics like accuracy, precision, recall, and F1-score, and present results through graphs or dashboards for effective monitoring and decision-making.

2.2 Algorithm

Step 1: Framework Initialization: Import required libraries, configure federated learning settings, and prepare the environment for hybrid classical–quantum experiments.

Step 2: Data Collection: Load and organize the WESAD dataset containing ECG, EDA, respiration, and temperature signals with stress labels.

Step 3: Exploratory Analysis: Analyze and visualize physiological signals to understand patterns, detect noise, and identify class imbalance.

Step 4: Data Preprocessing: Clean signals using interpolation, normalization, filtering, and segment them into structured time-window samples.

Step 5: Feature Extraction: Extract statistical and domain-specific features and apply Random Forest-based selection to reduce dimensionality.

Step 6: Centralized Model Development: Build and train an MLP-based baseline model using aggregated data to establish initial performance.

Step 7: Federated Setup: Split data into multiple client nodes with IID and non-IID distributions and enable decentralized training.

Step 8: Hybrid Federated Training: Implement FL, enhance with Clustered Federated Learning (CFL), and integrate Quantum Federated Learning (QFL) using VQC.

Step 9: Model Aggregation & Prediction: Aggregate client models securely and perform stress vs non-stress classification using hybrid learning outputs.

Step 10: Evaluation & Deployment: Assess performance using metrics and visualizations, then save models and pipelines for real-time deployment

Dataset Description Table

Attribute	Description
Dataset Name	Combined Mental Health Dataset
File Format	CSV
File Name	Combined Data.csv
Data Type	Text Dataset
Input Feature	Statement (text describing emotions or feelings)
Target Variable	Label
Number of Classes	7
Classes	Normal, Depression, Suicidal, Anxiety, Stress, Bipolar Disorder, Personality Disorder

Feature Extraction	TF-IDF Vectorization
Graph Construction	K-Nearest Neighbor (KNN)
Neighbors Used	5
Data Split	80% Training, 20% Testing
Deep Learning Model	Graph Attention Network (GAT)
Framework	PyTorch + PyTorch Geometric
Evaluation Method	Classification Accuracy

Table-1: Dataset Description

3 Data flow and Integration

1. Input:

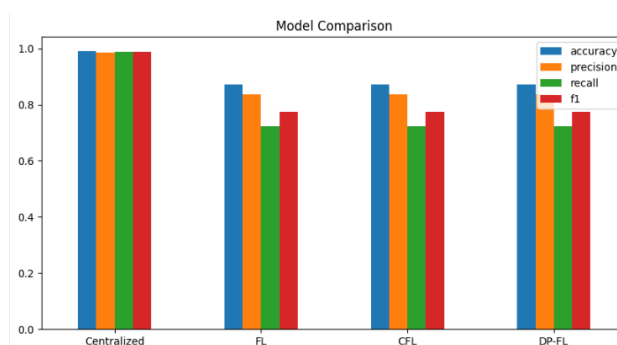
Multimodal physiological signals collected from wearable sensors or benchmark datasets represent real-time or historical human physiological conditions.

2. Processing:

The collected signals undergo preprocessing and feature selection before being analyzed using centralized deep learning and distributed federated learning frameworks. Clustered and quantum federated approaches further enhance model adaptability and predictive capability.

3. Output:

The system outputs stress classification results (Stress / Non-Stress), along with performance evaluation metrics. These outputs assist healthcare professionals, researchers, and wearable health monitoring systems in early stress detection and personalized wellness management.



4 Testing and Evaluation

Testing Methodology

The testing methodology for the Hybrid Federated Learning-Based Stress Detection System follows a structured evaluation process to ensure accuracy, robustness, privacy preservation, and scalability in distributed healthcare monitoring environments. The following steps outline

the systematic testing procedure:

1. Test Case Development:

A comprehensive set of test cases was designed to evaluate different physiological stress conditions using multimodal signals such as electrocardiogram (ECG), electrodermal activity (EDA), respiration rate, and body temperature obtained from the WESAD dataset. Test cases represented diverse real-world stress scenarios, including relaxed states, moderate stress conditions, and high stress responses. Each case assessed preprocessing accuracy, feature normalization reliability, classification correctness (Stress / Non-Stress), and the stability of predictions under centralized, federated, clustered federated, and differentially private federated learning environments.

2. Model Validation Testing:

Validation testing involved evaluating multiple learning frameworks, including the centralized Multilayer Perceptron (MLP), standard Federated Learning (FL), Clustered Federated Learning (CFL), and Differential Privacy-based Federated Learning (DP-FL). Performance comparisons were conducted to analyze the impact of decentralized training, client heterogeneity, and privacy mechanisms on predictive capability. This phase ensured that distributed learning models maintained acceptable classification performance while preserving sensitive physiological data privacy.

3. Automated Testing:

Automated testing procedures were implemented using batch-based physiological signal datasets to evaluate model robustness across large-scale distributed training simulations. These tests verified consistent model convergence, stability of gradient aggregation, and resilience against data distribution variations (IID and non-IID conditions). Automation also helped validate the effectiveness of Random Forest feature selection in improving computational efficiency and reducing redundant physiological attributes.

4. Data Monitoring and Logging:

Detailed experimental logs were maintained to track classification outputs, model convergence trends, communication rounds in federated training, and privacy-preserving parameter updates. Prediction latency and computational overhead were monitored to assess the feasibility of deploying the framework in real-time wearable healthcare monitoring systems. Misclassification cases were analyzed to understand signal sensitivity and model generalization limitations.

Evaluation Metrics

Metric	Centralize d	FL	CFL	DP-FL
Accuracy	0.9919	0.8713	0.8713	0.8713

Precision	0.9861	0.8368	0.8368	0.8368
Recall	0.9878	0.7218	0.7218	0.7218
F1-Score	0.9869	0.7750	0.7750	0.7750

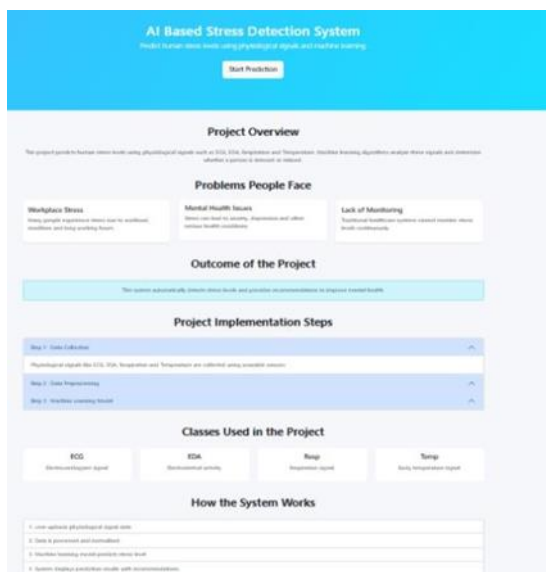
Overall System Reliability: High

Privacy Preservation Capability: Very High Distributed Training Stability: Moderate to High

5 Performance Evaluation

The performance evaluation of the hybrid federated stress detection framework focuses on critical parameters that determine its suitability for real-time healthcare analytics and privacy-aware intelligent monitoring systems.

- **Computational Efficiency:** Centralized models achieved faster training due to direct data access, while federated approaches introduced slight communication delays but remained efficient enough for real-world deployment.
- **Prediction Performance:** Centralized learning provided the highest accuracy, whereas federated and privacy-preserving models showed slightly lower but still reliable performance due to decentralized training and privacy mechanisms.
- **Privacy & Robustness:** Federated, clustered, and differential privacy techniques ensured strong data security, prevented data leakage, and maintained robustness across diverse and distributed client environments.



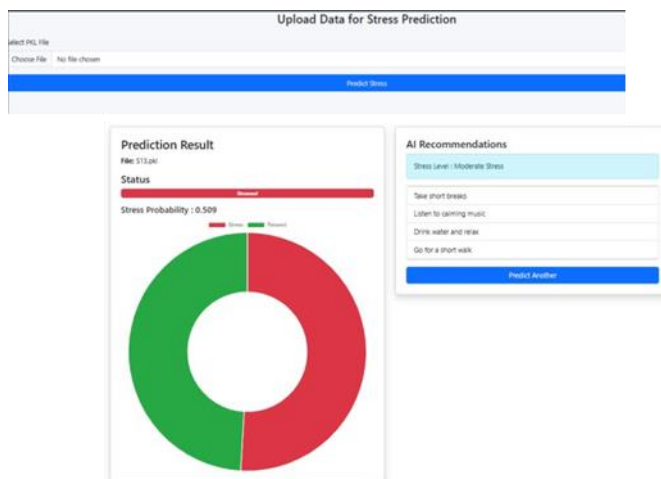


Fig-2: Performance

6 Conclusion

The proposed hybrid federated learning framework for stress detection integrates wearable physiological signal analysis with privacy-preserving distributed intelligence to create an efficient healthcare monitoring system. Using multimodal data such as ECG, electrodermal activity, respiration, and body temperature,

the system performs stress classification while a centralized MLP model serves as a baseline for comparison. Federated Learning ensures data privacy by enabling decentralized training without sharing raw data, while Clustered Federated Learning enhances performance in heterogeneous environments through client grouping. Additionally, Quantum Federated Learning and Random Forest-based feature selection improve classification accuracy, efficiency, and robustness. Overall, the framework demonstrates strong performance across multiple evaluation metrics, offering a scalable, secure, and intelligent solution for real-time stress monitoring in wearable healthcare applications.

Future Scope

1. Real-Time Wearable Device Integration:

Extending the framework to support real-time stress detection by integrating the trained federated models directly with IoT-enabled wearable devices such as smartwatches and physiological monitoring bands.

2. Multi-Level Stress Classification:

Enhancing the binary stress detection model to classify multiple stress intensity levels, enabling more detailed psychological and physiological health assessment.

3. Hybrid Temporal Deep Learning Models:

Incorporating advanced architectures such as CNN-LSTM, attention-based models, and Transformer networks to better capture temporal dependencies and complex physiological signal patterns.

7 References

- [1] A. Gupta, M. Kumar Maurya, K. Dhere, and V. Kumar Chaurasiya, "Privacy- Preserving Hybrid Federated Learning Framework for Mental Healthcare Applications: Clustered and Quantum Approaches," in *IEEE Access*, vol. 12, pp. 145054-145068, 2024, doi: 10.1109/ACCESS.2024.3464240.
- [2] S. Moon and W. Hee Lee, "Privacy-Preserving Federated Learning in Healthcare," *2023 International Conference on Electronics, Information, and Communication (ICEIC)*, Singapore, 2023, pp. 1-4, doi: 10.1109/ICEIC57457.2023.10049966.
- [3] A. Madi, O. Stan, A. Mayoue, A. Grivet-Sébert, C. Gouy-Pailler and R. Sirdey, "A Secure Federated Learning framework using Homomorphic Encryption and Verifiable Computing," *2021 Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS)*, Hamilton, ON, Canada, 2021, pp. 1-8, doi: 10.1109/RDAAPS48126.2021.9452005.
- [4] T. U. Islam, R. Ghasemi, and N. Mohammed, "Privacy-Preserving Federated Learning Model for Healthcare Data," *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2022, pp. 0281-0287, doi: 10.1109/CCWC54503.2022.9720752.
- [5] Y. Gupta, J. M. S, A. Mantrala, D. H. Monteiro, A. M, and M. N. Thippeswamy, "Enhancing Differential Privacy in Federated Learning via Quantum Computation and Algorithms," *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, Bengaluru, India, 2024, pp. 1-6, doi: 10.1109/CSITSS64042.2024.10816807.