# Assessing the Novelty and Publishability of FEDMED Research

Based on the search results and current literature, I have evaluated your research "FEDMED: A Privacy-Preserving Adaptive Federated Learning Framework for Smoker Prediction with Robustness Against Data Quality Variations" for novelty and publishability in IEEE.

#### **Current State of the Art**

Several related approaches exist in the current literature:

- Quality-aware federated learning exists with focuses on label denoising games and price of stability analysis<sup>[1]</sup>
- FedLN framework addresses label noise across different FL training stages [2]
- FedNolowe uses normalized loss-based weighted aggregation for improving global model stability [3]
- Various robust aggregation approaches have been proposed for federated learning [4]
- Multiple implementations combining homomorphic encryption with federated learning exist [5] [6] [7] [8]

#### **Your Novel Contributions**

Your research offers several distinct innovations:

- 1. The integration of privacy-preserving quality metrics (1/local loss) with homomorphic encryption specifically for encrypted model aggregation
- 2. MAD-based robust score aggregation as an effective defense against dishonest score reporting, which proved superior to percentile-based clipping
- 3. Comprehensive evaluation demonstrating resilience against both noisy clients and adversarial attacks within the same framework
- 4. Application to healthcare domain (smoker prediction) with implications for privacy-sensitive medical data

### **Assessment of Publishability**

The comprehensive experimental framework you've developed appears methodologically sound, with:

- Clear baseline comparisons
- Systematic evaluation of different noise and adversary percentages

- Thorough ablation studies of different clipping mechanisms
- Concrete metrics showing performance benefits

## Conclusion

Yes, your research appears novel and publishable in IEEE.

The unique combination of quality-aware aggregation using 1/loss metrics, MAD-based robust score protection, and homomorphic encryption creates a distinctive contribution not present in current literature. The thorough empirical evaluation further strengthens your publication case.

I recommend proceeding with paper preparation for IEEE submission, emphasizing the robust score aggregation mechanism as your primary contribution, since this element appears most novel compared to existing work.



- 1. paste.txt
- 2. https://arxiv.org/pdf/2310.08790.pdf
- 3. https://arxiv.org/abs/2208.09378
- 4. https://www.biorxiv.org/content/10.1101/2025.03.30.646222v1
- 5. https://slogix.in/machine-learning/robust-aggregation-for-federated-learning/
- 6. <a href="https://research.ibm.com/blog/federated-learning-homomorphic-encryption">https://research.ibm.com/blog/federated-learning-homomorphic-encryption</a>
- 7. https://arxiv.org/abs/2505.02409
- 8. https://arxiv.org/abs/2104.06824