FENITH: A Privacy-Preserving Federated Learning Framework for Italian Healthcare Network

FENITH Research Team

Italian Healthcare Innovation Initiative

November 22, 2024

Abstract

Research Context

Current healthcare ML models suffer from:

- Data silos limiting model robustness
- Privacy concerns blocking data sharing
- Regulatory constraints (GDPR)
- Limited cross-institution collaboration

Proposed Solution

FENITH introduces a novel federated learning framework specifically designed for Italian healthcare institutions, enabling:

- Distributed model training across institutions
- Privacy-preserving knowledge sharing
- GDPR-compliant data governance
- Scalable research collaboration

Methodology

System Architecture

1. **Edge Computing Layer**
   - Local model training
   - Data preprocessing
   - Privacy preservation
2. **Aggregation Layer**
   - Secure model averaging
   - Differential privacy guarantees
   - Convergence optimization
3. **Orchestration Layer**
   - Training coordination
   - Model versioning
   - Performance monitoring

Technical Framework

Federated Learning Algorithm

$$w_{t+1} = w_t - \eta \sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k(w_t)$$

where:

$$F_k(w) = \frac{1}{n_k} \sum_{i \in \mathcal{D}_k} f_i(w)$$

- w_t: Global model at iteration t
- η: Learning rate
- n_k: Local dataset size
- F_k: Local objective function

Privacy Guarantees

Differential Privacy Implementation

- ϵ-differential privacy with adaptive clipping
- Secure aggregation protocol
- Homomorphic encryption for model updates

Security Measures

- End-to-end encryption
- Secure multi-party computation
- Zero-knowledge proofs for integrity

Initial Use Cases

Medical Imaging Analysis

- CT scan anomaly detection
- MRI segmentation
- X-ray classification

Performance Metrics:

- AUC-ROC: 0.92-0.95
- Sensitivity: 0.89-0.93
- Specificity: 0.88-0.91

System Scalability

Performance Analysis

- Communication complexity: $O(md)$
- Computation overhead: $O(n \log n)$
- Storage requirements: $O(m)$
  where:
  - m: number of institutions
  - d: model parameters
  - n: local dataset size

Research Opportunities

Open Research Questions

- Model heterogeneity handling
- Non-IID data challenges
- Dynamic participant management
- Adaptive aggregation strategies

Collaboration Framework

- Multi-institution research protocols
- Standardized evaluation metrics
- Shared validation datasets
- Publication guidelines

Implementation Timeline

2024-2025 Roadmap

1. **Phase I: Infrastructure Development**
   - Core platform development
   - Security audit and certification
   - Initial node deployment
2. **Phase II: Clinical Validation**
   - Pilot studies
   - Performance benchmarking
   - Protocol optimization
3. **Phase III: Network Expansion**
   - Node scaling
   - Use case diversification
   - International collaboration

Research Impact

Expected Outcomes

- Enhanced model robustness
- Reduced bias in healthcare AI
- Accelerated clinical research
- Privacy-preserved collaboration

Future Directions

- Multi-modal data integration
- Real-time learning systems
- Automated model adaptation
- Cross-border collaboration

Contact Information

Research Collaboration

- Website: `http://fenith.org/`
- Email: research@fenith.org
- GitHub: github.com/fenith

References

Key publications and technical documentation available at: `http://fenith.org/publications`