Journal of Engineering for THERMAL ENERGY AND POWER

ISSN: 1001-2060
Vol. 22 No. 1, 2019

FEDERATED LEARNING FOR PRIVACY-PRESERVING ENGINEERING ANALYTICS

Damanjit Kaur
*1Department of Civil Engineeing, Navkar Institute of technology, Malegaon, India

Received: 05/01/2019
Revised: 19/02/2019
Accepted: 22/03/2019

DOI:
10.12060/jet-ep-v22.i1-1

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Abstract

Engineering analytics increasingly depend on data-driven insights derived from distributed data sources such as IoT devices, sensor networks, and industrial systems. Conventional centralized analytics approaches require the aggregation of raw data into a central server, raising privacy concerns and violating regulatory constraints. Federated learning (FL) has emerged as a paradigm that enables collaborative model training without sharing raw data, thereby facilitating privacy-preserving engineering analytics across distributed environments. This paper discusses FL architectures, privacy mechanisms, and engineering use cases. We propose a federated analytics framework tailored for engineering applications, evaluate its performance, and analyze privacy guarantees. Results from IoT and industrial datasets illustrate that FL can reduce privacy risks while maintaining analytical utility and scalability. Challenges and future research directions in privacy-preserving FL are discussed.

Keyword: Federated Learning, Privacy Preservation, Engineering Analytics, Distributed Machine Learning, Differential Privacy, Homomorphic Encryption

1. INTRODUCTION

Engineering systems, from smart manufacturing to structural health monitoring, generate massive quantities of digital data. Traditional machine learning approaches centralize this data for model training, exposing sensitive information, violating privacy regulations, and increasing communication overhead. **Federated learning (FL)** shifts model training to the edge by aggregating model updates from distributed clients, thereby keeping raw data local and **preserving privacy**. This characteristic makes FL suitable for engineering analytics where privacy, scalability, and regulatory compliance are critical. FL incorporates mechanisms such as differential privacy and secure aggregation to further protect sensitive information during collaborative training. This research explores FL architectures and evaluates their suitability for engineering analytics.

2. LITERATURE REVIEW

2.1 Fundamentals of Federated Learning

Federated learning enables collaborative model training across multiple clients while preventing raw data exchange. It is inherently designed to **preserve data locality** and support scalable distributed computing, significantly reducing privacy risks compared to centralized learning.

2.2 Privacy-Preserving Techniques

Key techniques used to enhance privacy in FL include:

- **Differential Privacy (DP):** Injects noise into model updates to prevent inference of sensitive information.
- **Secure Aggregation:** Ensures that the server aggregates client updates securely without seeing individual updates.
- **Homomorphic Encryption (HE):** Allows encrypted model updates to be aggregated without decryption, offering strong privacy guarantees.

2.3 FL in Distributed Analytics

Prior research has applied FL in healthcare, finance, and IoT. Decentralized analytics frameworks demonstrate improved privacy and regulatory compliance while facilitating scalable model training.

2.4 Challenges in Engineering Contexts

Engineering analytics often involves data heterogeneity and non-IID (non-independent and identically distributed) data across clients. Communication overhead, fault tolerance, and privacy-utility trade-offs complicate FL deployment in engineering applications.

3. METHODOLOGY

3.1 Research Objectives

The research aims to:

1. Develop a conceptual framework for FL-based privacy-preserving engineering analytics.
2. Implement core privacy mechanisms within the FL paradigm.
3. Evaluate the framework in terms of performance, accuracy, and privacy guarantees.

3.2 Data Environment

The study considers IoT and engineering datasets typically representing distributed sensors, such as:

- Smart manufacturing process logs
- Structural health monitoring sensor time series
- Energy consumption records from smart grids

3.3 FL Architecture

The proposed architecture comprises:

- **Edge Clients:** Local devices that train models on local data
- **Central Aggregator:** Receives encrypted model updates for global aggregation
- **Privacy Layer:** Implements differential privacy and secure aggregation

FL training proceeds in rounds where models are locally updated and securely aggregated at the server. Differential privacy is applied to protect individual client updates.

3.4 Evaluation Metrics

ISSN: 1001-2060
Vol. 22 No. 1, 2019

To assess performance, the following metrics are measured:

- **Accuracy:** Predictive performance on validation data
- **Communication Overhead:** Amount of data transmitted per round
- **Privacy Loss (ε):** Differential privacy parameter indicating privacy level
- **Latency:** Time per FL round

4. PROCESS

4.1 System Setup

Simulation environments were created using Python and TensorFlow Federated. Clients represent edge nodes with local datasets, and a central server performs aggregation. Secure aggregation and DP mechanisms are implemented as part of the FL pipeline.

4.2 Model Training Flow

1. Each client trains a local model using local data.
2. Clients apply differential privacy to model updates.
3. Local updates are encrypted by homomorphic encryption (optional).
4. The server performs secure aggregation of updates.
5. The global model is updated and redistributed.

4.3 Privacy Integration

Differential privacy parameters (ε, δ) are tuned to balance privacy and utility. Secure aggregation protocols ensure updates cannot be linked to specific clients.

5. RESULTS

5.1 Performance Evaluation

The FL system shows high predictive performance across engineering tasks, with accuracy comparable to centralized models while maintaining privacy. Communication overhead was significantly lower due to local model update transmission without raw data sharing.

5.2 Privacy Guarantees

Applying differential privacy reduced privacy leakage according to measured ε values. Secure aggregation ensured that individual model updates remained confidential, protecting client data during aggregation.

5.3 Scalability

The federated setup demonstrated scalability across increasing numbers of clients, with manageable overhead and maintained accuracy.

6. DISCUSSION

The results confirm that FL can effectively facilitate privacy-preserving analytics in distributed engineering environments. Key strengths include reduced data exposure and enhanced compliance with data protection regulations. However, challenges remain in heterogeneity management and the privacy-utility trade-off, particularly for non-IID datasets common in engineering systems.

7. CONCLUSION

Federated learning provides a promising framework for **privacy-preserving engineering analytics**, enabling decentralized collaborative learning without sharing raw data. The

ISSN: 1001-2060
Vol. 22 No. 1, 2019

integration of differential privacy and secure aggregation enhances data protection while maintaining analytical performance. Future work should address optimization of privacy parameters, adaptive aggregation techniques, and deployment in real-world engineering systems with mixed data distributions.

REFERENCES

1. Reshma Hussain, Federated Learning Approaches for Privacy Preserving AI Applications, Int. J. Eng. & Ext. Tech. Res., 2024.
2. Guru Pramod Rusum & Kiran Kumar Pappula, Federated Learning in Practice: Building Collaborative Models While Preserving Privacy, IJERET, 2025.
3. Yesu Vara Prasad Kollipara, Privacy-Preserving and Federated Learning for Regulated Data Ecosystems, Int. J. Comp. & Exp. Sci. Eng., 2025.
4. Advanced Privacy-Preserving Federated Learning in 6G Networks, Int. J. Intell. Syst. Appl. Eng., 2024.
5. Shreya Gupta, Federated Learning: Advancing Privacy-Preserving Machine Learning at Scale, Int. J. Sci. Res. CS Eng. Inf. Tech., 2025.
6. Edge Computing and Federated Learning for Privacy-Preserving IoT Analytics, EURASIP J. Wireless Comms & Networking, 2026.
7. N. V. R. Guduri & J. Jaidhan B., Scalable IoT Analytics with Federated Learning, Int. J. Intell. Syst. Appl. Eng., 2025.
8. Alexis Cameron, FL Approaches for Privacy-Preserving Knowledge Discovery, Int. J. Knowl. & Web Intelligence, 2024.
9. Milan Biswal et al., AMI-FML: Privacy-Preserving Federated ML Framework for AMI, arXiv, 2021.
10. Sinem Sav et al., POSEIDON: Privacy-Preserving Federated Neural Network Learning, arXiv, 2020.
11. M. Gayathri Hegde et al., FL-HE Method for CKD Prediction, Eng. Tech. & Appl. Sci. Res., 2025.
12. A Systematic Review of Preserving Privacy in Federated Learning, Int. Eng. J. Res. & Dev., 2025.