A Secure Federated Learning for Stock and Investment Recommendations

Thota Sanjana,G.SN MURTHY,N.G.M.S.PARIKSHIT,V.Bala vardhan

Guide: Andavarapu Sravani

Introduction

Traditional investment platforms risk privacy by storing user data centrally. Our framework uses secure federated learning, keeping data on local devices and sharing only encrypted updates. It integrates SMPC and differential privacy to enable confidential, intelligent investment recommendations while enhancing trust and security.

Literature Review

Recent studies have explored privacy-preserving techniques in financial forecasting, but key challenges remain unaddressed:

- Zhao et al. (2023) – Deep learning improved accuracy but risked privacy in centralized setups.
- Liu et al. (2024) – Used FL for confidentiality but lacked strong encryption.
- Patel et al. (2024) – Added differential privacy but reduced accuracy.
- Wang et al. (2025) – Hybrid CNN–LSTM worked well but used centralized data.
- Chen et al. (2025) – Used secure aggregation but missed multi-layer privacy.

Research Gaps

Current stock recommendation systems rely on centralized models that risk user data privacy. Few combine federated learning with advanced techniques like SMPC, differential privacy, and homomorphic encryption. Most ignore user sentiment and risk profiles under privacy constraints, and real-world testing on scalability and trust remains limited.

Project Objectives

1. Develop a secure federated learning framework for stock and investment recommendations.
2. Ensure data privacy through decentralized training and encryption techniques.
3. Enhance model accuracy and personalization using hybrid deep learning approaches.
4. Implement a scalable cloud–client system for real-time financial insights.

Proposed Methodology

1. Collect user financial and market data locally on individual devices.
2. Train MLP–LSTM and Collaborative Filtering models on each client for personalized insights.
3. Implement privacy-preserving techniques such as SMPC, Federated Differential Privacy, and Secure Aggregation.
4. Aggregate encrypted model updates on the cloud server to build a global model.
5. Distribute the updated global model back to clients for improved predictions.
6. Evaluate system performance on accuracy, privacy, and scalability metrics.

Identification of Tools/ Technology / Algorithms

- Frameworks & Libraries: TensorFlow Federated, PySyft, Scikit-learn, Pandas, NumPy.
- Programming Languages: Python for modeling and implementation.
- Privacy Mechanisms: Secure Aggregation, SMPC, Homomorphic Encryption, Federated Differential Privacy.
- Models Used: Hybrid MLP–LSTM for time-series prediction and Collaborative Filtering for recommendations.
- Optimization Algorithm: Federated Averaging for global model updates.
- Cloud client architecture using AWS or Oracle Cloud for distributed training.

References

- Kumarappan, J. et al. (2024). Federated Learning Enhanced MLP–LSTM Modeling for Stock Market Prediction. International Journal of Computer and Information Systems.
- Zhang, Y. et al. (2024). Federated Meta Embedding Concept Stock Recommendation. IEEE Transactions on Big Data.
- Kairouz, P. et al. (2021). Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning.
- Li, T. et al. (2023). Federated Learning for Privacy-Preserving Recommender Systems. ACM Computing Surveys.