GITAM
SCHOOL OF COMPUTER
SCIENCE AND ENGINEERING

A Secure Federated Learning Framework for Stock and Investment Recommendations

Presenter Names:

Thota Dakshyani Sanjana-VU22CSEN0101682
G.SN MURTHY-VU22CSEN0100802
N.G.M.S.PARIKSHIT-VU22CSEN0100286
V Bala vardhan-VU22CSEN0100805

Guide Name:

Andavarapu Sravani

Department of Computer Science and Engineering
GITAM School of CSE, GITAM (Deemed to be University),
Visakhapatnam.

Contents

1. Abstract
2. Introduction
3. Literature Survey
4. Problem Statements
5. Objectives
6. Work Breakdown & Task Allocation
7. Conclusion
8. References

Abstract

With the increasing reliance on personalized financial advice, traditional stock and investment recommendation systems often face privacy challenges due to centralized data collection. InvestSafe proposes a privacy-preserving recommendation system utilizing federated learning, where user data remains on-device, and only model updates are shared with a central server. By integrating user investment behavior, stock market data, and external financial indicators, the system generates secure, personalized investment suggestions. The approach leverages cloud-based aggregation to enhance model accuracy while maintaining data confidentiality, addressing regulatory constraints and user trust concerns.

Additionally, InvestSafe incorporates adaptive learning mechanisms to respond to changing market trends in real-time, ensuring that recommendations remain relevant and timely. Differential privacy techniques further safeguard sensitive information during model updates, mitigating potential data leaks. The system also supports multi-device synchronization, allowing users to receive consistent advice across platforms without compromising privacy. Overall, this framework demonstrates a scalable and secure solution for modern, data-driven investment advisory services.

Introduction

- Recommendation systems play a pivotal role in guiding investors toward profitable stocks, mutual funds, or ETFs. Conventional systems necessitate aggregating sensitive financial and behavioral data centrally, leading to potential privacy risks. InvestSafe integrates federated learning with cloud-based aggregation to provide secure, real-time, and personalized investment recommendations. The system combines user profiles, investment history, stock fundamentals, and market indicators to generate risk-adjusted suggestions while preserving privacy.

- By keeping data on-device and sharing only encrypted model updates, InvestSafe minimizes exposure of sensitive financial information. The system also adapts to changing market conditions, continuously refining recommendations based on the latest trends. Furthermore, regulatory compliance and user trust are reinforced, making the platform suitable for widespread adoption in the financial sector.

Literature Survey

Table 1: Literature Survey

S. No.	Paper Details	Summary	Techniques/Algorithms Used	Research Gap
1	Kumarappan, J., et al. Federated Learning Enhanced MLP–LSTM Modeling for Stock Market Prediction	Proposes a hybrid MLP-LSTM model within a federated learning framework for stock market prediction.	MLP, LSTM, Federated Learning	Limited exploration of sentiment analysis integration.
2	Zhang, Y., Wang, Y., & Li, H. Federated Meta Embedding Concept Stock Recommendation	Introduces a federated recommendation system leveraging private forum comments and public financial data.	Meta-embedding, Federated Learning	Lack of real-time market data integration.
3	Li, X., Chen, J., & Xu, K Leveraging Federated Learning and Edge Computing for Recommendation Systems	Explores the synergy between federated learning and edge computing in recommendation systems.	Federated Learning, Edge Computing	Insufficient evaluation on diverse datasets.

Literature Survey

Table 1: Literature Survey

S. No.	Paper Details	Summary	Techniques/Algorithms Used	Research Gap
4	Zhang, Y., et al. Federated Learning on Recommender Systems	Evaluates the performance of federated learning in recommender systems across various datasets.	Federated Learning, Collaborative Filtering	Need for domain-specific adaptation.
5	Tiwari, S. S., Gupta, R., & Singh, A. Federated Deep Reinforcement Learning for Privacy-Preserving Sentiment-Driven Stock Market Forecasting	Combines federated learning with deep reinforcement learning for sentiment-based stock market forecasting.	Deep Reinforcement Learning, Sentiment Analysis, Federated Learning	Limited scalability assessment.
6	Kumarappan, J., et al. Federated Learning for Financial Forecasting. arXiv preprint arXiv:2509.16393, 2025.	Investigates the application of federated learning in financial forecasting.	Federated Learning, Time-Series Analysis	Lack of integration with alternative data sources.

Literature Survey

GITAM
SCHOOL OF COMPUTER
SCIENCE AND ENGINEERING

Table 1: Literature Survey

S. No.	Paper Details	Summary	Techniques/Algorithms Used	Research Gap
7	Rafi, T. H., Khan, M., & Rahman, M. Fairness and Privacy Preserving in Federated Learning.	Discusses challenges in fairness and privacy in federated learning systems.	Federated Learning, Privacy Preservation	Need for fairness metrics in financial applications.
8	Qu, L., Xu, Y., & Zhou, H. Federated Graph Neural Network-based Recommender Systems.	Proposes a federated graph neural network approach for recommender systems.	Graph Neural Networks, Federated Learning	Limited evaluation on financial datasets.
9	Imran, M., et al. ReFRS: Resource-efficient Federated Recommender System	Introduces a resource-efficient federated recommender system considering dynamic user preferences.	Federated Learning, Variational Autoencoder	Lack of integration with financial data.
10	Wu, C., Chen, M., & Li, X. FedCL: Federated Contrastive Learning for Privacy-Preserving Recommendation.	Proposes a federated contrastive learning method for privacy-preserving recommendations.	Contrastive Learning, Federated Learning	Need for evaluation on financial recommendation tasks.

Problem Statement

Investors require personalized stock and investment recommendations to optimize returns based on risk profiles and financial goals. Centralized recommendation systems pose privacy risks since sensitive financial and behavioral data must be collected on a central server. InvestSafe aims to provide a secure, federated recommendation system where user data stays local while model updates are shared and aggregated in the cloud. Challenges include handling heterogeneous client data, ensuring privacy, maintaining recommendation accuracy, and integrating multiple data sources (historical, fundamental, sentiment).

To address these challenges, InvestSafe leverages federated learning combined with differential privacy and encrypted model aggregation techniques. The system continuously adapts to evolving market trends, delivering timely and risk-adjusted investment suggestions. By keeping user data on-device, it strengthens trust and compliance with data protection regulations, making it a scalable solution for modern, privacy-aware investment advisory services.

Objectives

1. Develop a federated learning-based stock and investment recommendation system.

2. Preserve user privacy by keeping raw financial and behavioral data on local devices.

3. Securely aggregate model updates in a cloud environment without exposing sensitive data.

4. Integrate multiple data sources, including stock fundamentals, historical prices, and market sentiment, into recommendations.

5. Optimize recommendations based on individual user risk profiles, preferences, and investment goals.

6. Adapt to changing market conditions to provide timely and relevant investment suggestions.

7. Ensure regulatory compliance and build user trust through privacy-preserving mechanisms.

Work Breakdown & Task Allocation

GITAM
SCHOOL OF COMPUTER
SCIENCE AND ENGINEERING

Thota Dakshyani Sanjana-VU22CSEN0101682

Project Initiation

- **Responsibilities:**
  - Define clear project objectives aligned with privacy-preserving recommendation systems.
  - Identify project scope and expected deliverables.
  - Select the final project topic/problem statement.
  - Conduct literature review and background study on Federated Learning and privacy-preserving techniques.
  - Coordinate with guide/mentor for approvals.
  - Form the team structure and assign initial roles.

Work Breakdown & Task Allocation

GITAM
SCHOOL OF COMPUTER
SCIENCE AND ENGINEERING

Thota Dakshyani Sanjana-VU22CSEN0101682

Project Planning

- **Responsibilities:**
  - Develop a detailed project proposal.
  - Define technical requirements (frameworks like TensorFlow Federated, PySyft, Flower, datasets, tools).
  - Prepare a Gantt chart with milestones and deadlines.
  - Identify risks (e.g., dataset limitations, accuracy-privacy trade-off) and create mitigation strategies.
  - Plan resources (computing environment, libraries, budget if applicable).
  - Define evaluation metrics (accuracy, precision, recall, F1-score, privacy guarantees).

Outcome: A comprehensive project plan with schedules, risk management, and success criteria.

Work Breakdown & Task Allocation

N.G.M.S.PARIKSHIT-VU22CSEN0100286

Project Design & Development

- **Responsibilities:**
    - Create conceptual, architectural, and detailed designs (e.g., system architecture diagram, UML, workflow).
    - Set up the development environment with federated learning libraries.
    - Develop core modules (collaborative filtering models, federated training setup, secure aggregation, differential privacy).
    - Integrate all modules into a working prototype.
    - Demonstrate a prototype for review and feedback.

Outcome: A functional federated recommendation system prototype

Work Breakdown & Task Allocation

GITAM
SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

G.SN MURTHY-VU22CSEN0100802

Testing & Validation

- **Responsibilities:**
  - Develop a detailed test plan covering unit, integration, and system-level testing.
  - Conduct unit testing of modules and integration testing across components.
  - Perform system testing with sample datasets.
  - Carry out user acceptance testing (UAT) with simulated real-world data scenarios.
  - Record and analyze test results, refining models where necessary.

Outcome: Verified and validated system performance with documented results.

Work Breakdown & Task Allocation

V Bala vardhan-VU22CSEN0100805

Project Closure

- Submit all deliverables (code, datasets, final report).
- Archive project files for future reference.
- Reflect as a team on challenges faced and lessons learned.

Work Breakdown & Task Allocation

Shared Responsibilities (All Members)

5. Documentation

- Draft report sections (each member contributes to Introduction, Methodology, Results, Discussion).
- Prepare technical documentation (installation guide, usage manual).
- Review and finalize the project report before submission.

6. Presentation & Evaluation

- Collaboratively prepare slides.
- Rehearse and split sections for final presentation.
- Address evaluator Q&A confidently.
- Incorporate feedback for improvements.

Conclusion

InvestSafe demonstrates how federated learning can be leveraged to provide secure, personalized stock and investment recommendations. By keeping user data local and sharing only model updates, the system ensures privacy while benefiting from collective insights across users. Integrating historical prices, market fundamentals, and sentiment analysis enhances recommendation accuracy and reliability. The cloud-based aggregation enables scalable deployment and continuous model improvement.

References

[1] J. Kumarappan, R. Thangavelu, and S. Kumar, “Federated Learning Enhanced MLP–LSTM Modeling in an Integrated Deep Learning Pipeline for Stock Market Prediction,” *Int. J. Comput. Intell. Syst.*, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s44196-024-00680-9

[2] Y. Zhang, Y. Wang, and H. Li, “Federated Meta Embedding Concept Stock Recommendation,” *IEEE Trans. Big Data*, 2024. [Online]. Available: https://www.computer.org/csdl/journal/bd/2024/06/09919348/1HsTwBOPy4o

[3] X. Li, J. Chen, and K. Xu, “Leveraging Federated Learning and Edge Computing for Recommendation Systems within Cloud Computing Networks,” *arXiv preprint arXiv:2403.03165*, 2024. [Online]. Available: https://arxiv.org/pdf/2403.03165

[4] Y. Zhang, H. Zhou, and J. Xu, “Federated Learning on Recommender Systems,” *ResearchGate Preprint*, 2025. [Online]. Available: https://www.researchgate.net/publication/388088244_Federated_Learning_on_Recommender_Systems

References

[5] S. S. Tiwari, R. Gupta, and A. Singh, “Federated Deep Reinforcement Learning for Privacy-Preserving Sentiment-Driven Stock Market Forecasting,” *ResearchGate Preprint*, 2025. [Online]. Available: https://www.researchgate.net/publication/394875275_Federated_Deep_Reinforcement_Learning_For_Privacy-Preserving_Sentiment-Driven_Stock_Market_Forecasting

[6] J. Kumarappan, R. Thangavelu, and S. Kumar, “Federated Learning for Financial Forecasting,” *arXiv preprint arXiv:2509.16393*, 2025. [Online]. Available: https://arxiv.org/pdf/2509.16393

[7] T. H. Rafi, M. Khan, and M. Rahman, “Fairness and Privacy Preserving in Federated Learning,” *J. Netw. Comput. Appl.*, vol. 220, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1566253523005146

[8] L. Qu, Y. Xu, and H. Zhou, “Federated Graph Neural Network-based Recommender Systems,” PhD Thesis, Univ. of Queensland, 2024. [Online]. Available: https://espace.library.uq.edu.au/view/UQ%3A90adad5/s4643591_phd_thesis.pdf

References

[9] M. Imran, S. Ullah, and F. Ali, “ReFRS: Resource-efficient Federated Recommender System for Dynamic and Diversified User Preferences,” *arXiv preprint arXiv:2207.13897*, 2022. [Online]. Available: https://arxiv.org/abs/2207.13897

[10] C. Wu, M. Chen, and X. Li, “FedCL: Federated Contrastive Learning for Privacy-Preserving Recommendation,” *arXiv preprint arXiv:2204.09850*, 2022. [Online]. Available: https://arxiv.org/abs/2204.09850

[11] M. A. Khan, M. R. Shaikh, and M. N. Bajwa, “Federated Learning for Healthcare Recommendation Systems,” *J. Inf. Syst. Eng. Manag.*, vol. 6, no. 2, pp. 1–8, 2021. [Online]. Available: https://jisem-journal.com/index.php/journal/article/download/567/188/

[12] H. Wang, Y. Song, and Z. Yang, “A Survey on Privacy-Preserving Federated Learning for Recommendation,” *ACM Comput. Surv.*, 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3582270

[13] M. Chen, Y. Wang, and C. Wu, “Federated Learning Meets Recommender Systems: Applications and Challenges,” *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3024–3037, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9865432

References

[14] R. Shokri and V. Shmatikov, “Privacy-Preserving Deep Learning,” in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 1310–1321. [Online]. Available: https://dl.acm.org/doi/10.1145/2810103.2813687

[15] P. Kairouz, H. B. McMahan, B. Avent, et al., “Advances and Open Problems in Federated Learning,” *Found. Trends® Mach. Learn.*, vol. 14, no. 1–2, pp. 1–210, 2021. [Online]. Available: https://arxiv.org/abs/1912.04977

Thank You