جـامعـة الشـارقـة
UNIVERSITY OF SHARJAH

Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep Learning Algorithms

Fatima Muhair Alketbi [1], Fatih Kurugollu [2], Sebti Foufou [2], Isam Mashhour Al Jawarneh [2]

[1] *MSc in Data Science,* Department of Computer Science, University of Sharjah, UAE (U24102845@sharjah.ac.ae)

[2] Professor, Professor, & Assistant Professor @ Department of Computer Science, University of Sharjah, UAE

The 3rd International Conference on Intelligent Metaverse Technologies & Applications (iMETA2025) 2025

14-17 October 2025 | Dubrovnik, Croatia

17/10/2025

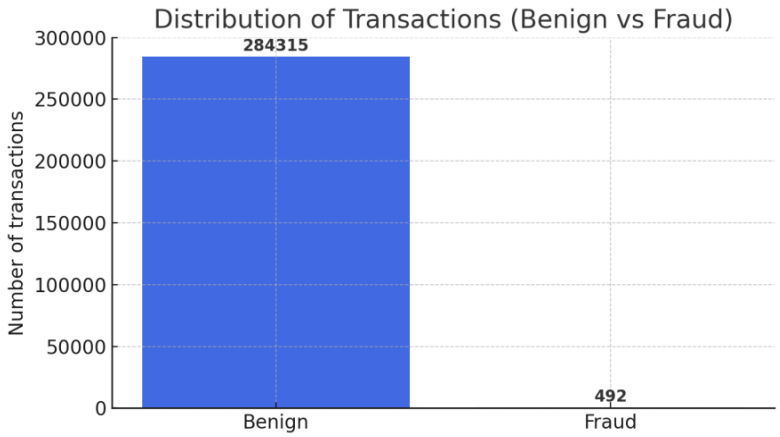
جامعة الشارقة
UNIVERSITY OF SHARJAH

Outline

- Problem & Motivation
  - Credit card fraud + privacy challenges
- Why Federated Learning?
  - Privacy-preserving collaborative training
- Dataset & Class Imbalance
  - European Credit Card Dataset (0.172% fraud)
- Methodology Overview
  - Sampling, models (CNN/MLP/LSTM), FL/SL/RL frameworks
- Key Results
  - AUC-ROC performance & robustness under noise
- Comparison with State-of-the-Art
- Discussion & Future Work
- Conclusion

Problem Statement & Motivation

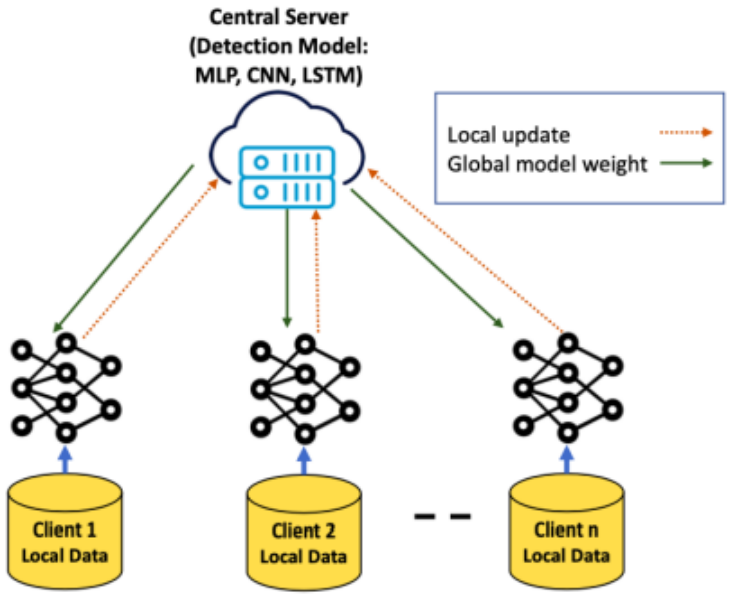
- Credit card fraud is rising → financial & reputational risks.
- Challenges:
  - Extreme class imbalance (0.172% fraud)
  - Privacy regulations (GDPR, CCPA)
  - Need for collaborative, yet privacy-preserving models
- **Goal**: Build accurate, robust, and privacy-compliant fraud detection



Only 0.172% fraud!

Why Federated Learning (FL)?

- FL enables collaborative training without sharing raw data.
- Preserves data privacy and ensures regulatory compliance.
- Ideal for banks/financial institutions that cannot share transaction data.
- Compared with Regular Learning (RL) and Split Learning (SL)



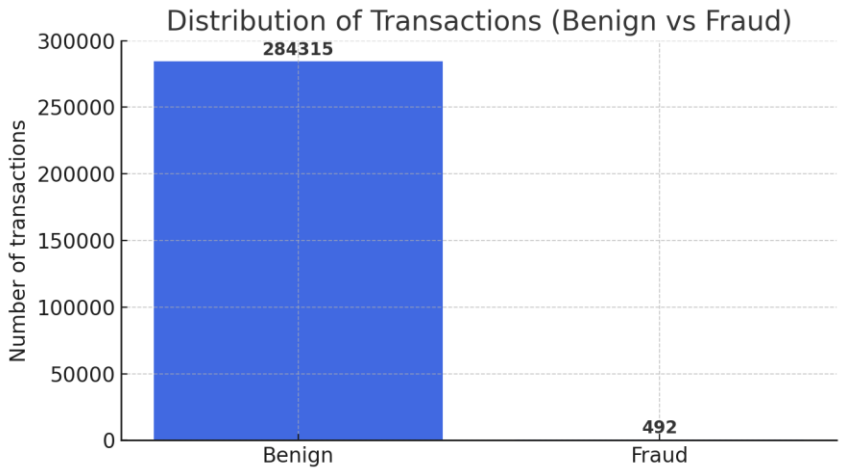
Typical Federated Learning architecture: ***privacy-preserving collaboration***

Related Work

- Prior FL fraud detection studies use:
  - SMOTE/Approx-SMOTE for imbalance.
  - CNN/MLP/LSTM architectures.
  - FedAvg aggregation.
- Gaps addressed in this work:
  - AUC-ROC as primary metric (not just accuracy/F1).
  - Robustness under noisy/malicious clients.

Dataset Overview

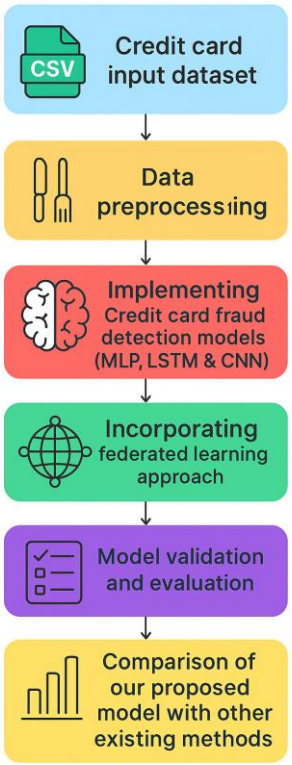
- European Credit Card Dataset (Kaggle)
  - 284,807 transactions
  - Only 492 fraudulent (0.172%)
- Features: Time, Amount, V1–V28 (PCA-transformed)
- Highly imbalanced → requires resampling



284,807 transactions | 492 fraud (0.172%)

Methodology Overview

- 5-Step Pipeline:
  - Data preprocessing (resampling + normalization)
  - Model design (CNN, MLP, LSTM)
  - Integration with FL, SL, RL frameworks
  - Evaluation using AUC-ROC + robustness tests
  - Comparison with state-of-the-art

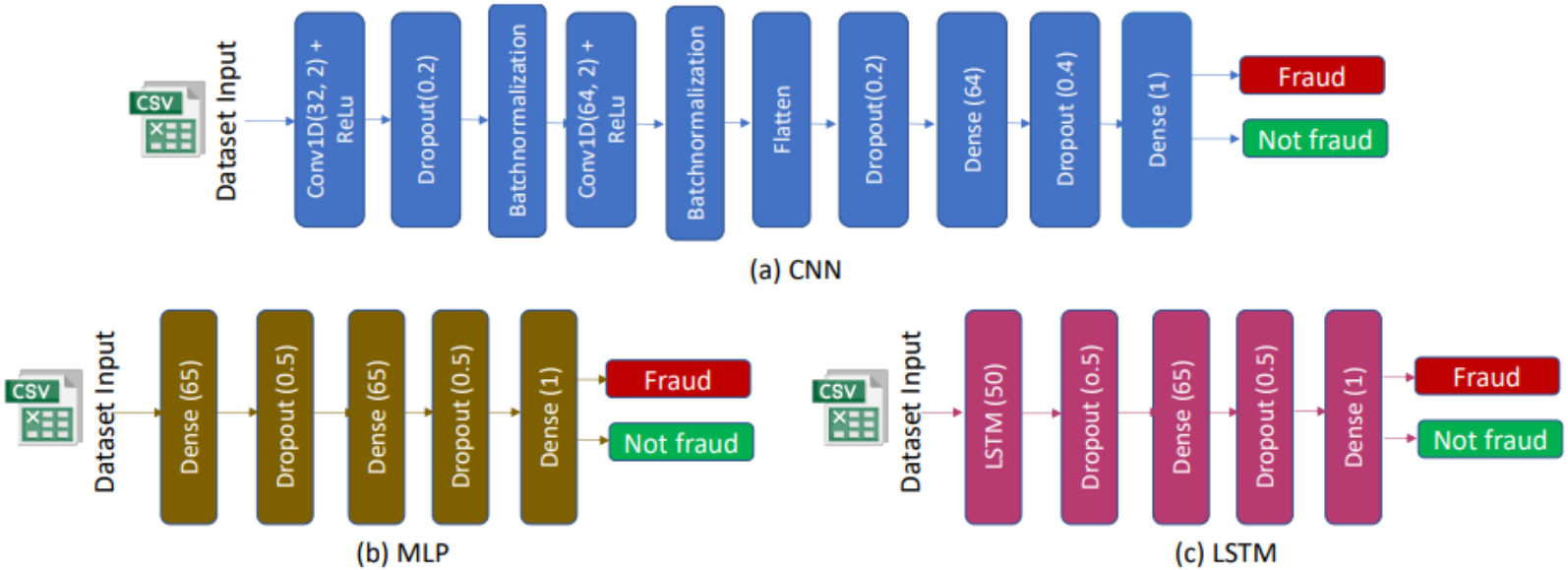


5-step pipeline: Preprocessing → Model → FL → Validation → Comparison

Sampling Techniques for Imbalance

- Four methods applied only on training data:
  - SMOTE (synthetic minority oversampling)
  - Random Oversampling (ROS)
  - Random Undersampling (RUS)
  - NearMiss Undersampling (NMU)
- Prevents data leakage; maintains test set realism

Model Architectures



- CNN: 2 conv layers, batch norm, dropout, dense layers.
- MLP: 3 dense layers + dropout.
- LSTM: 1 LSTM layer + dense + dropout
- All use ReLU (hidden), Sigmoid (output), Adam optimizer.
- Hyperparameters tuned via Keras Tuner

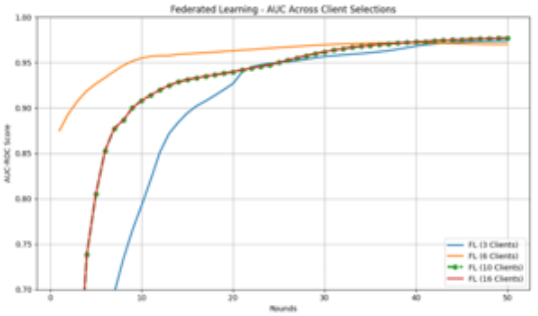
جامعة الشارقة
UNIVERSITY OF SHARJAH

Federated Learning Setup

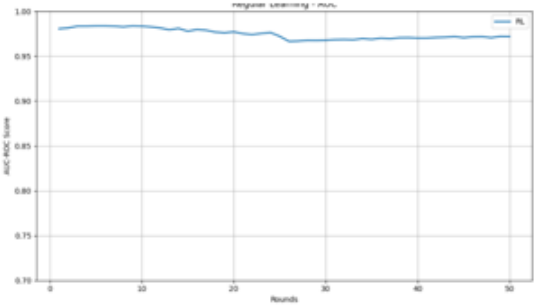
- FedAvg aggregation.
- IID data partitioning (balanced fraud ratio per client).
- Clients: 3 (CNN/MLP), 2 (LSTM) → later tested up to 16.
- 50 communication rounds, full client participation.
- Local training: 1 epoch/round, batch size = 64.

Key Results – AUC-ROC Comparison

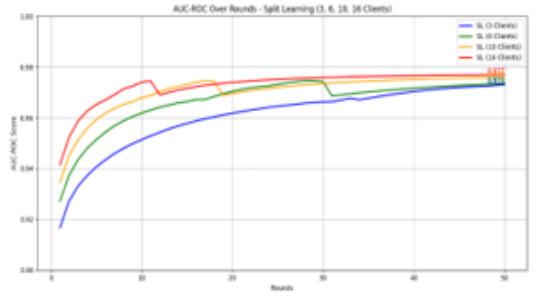
- FL outperforms RL (0.977 vs. 0.972)
- Best performance: FL with 10–16 clients
- SL matches FL at 16 clients
- CNN + SMOTE: best model (AUC-ROC = 0.9951)



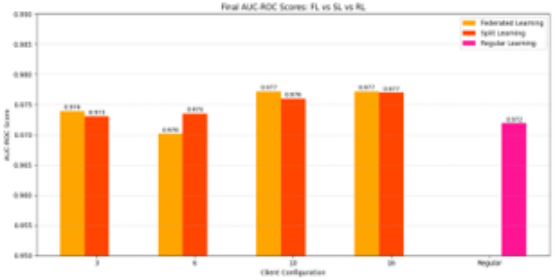
(a) Federated Learning– AUC Across Client Selections.



(b) Regular Learning– AUC Across Client Selections.



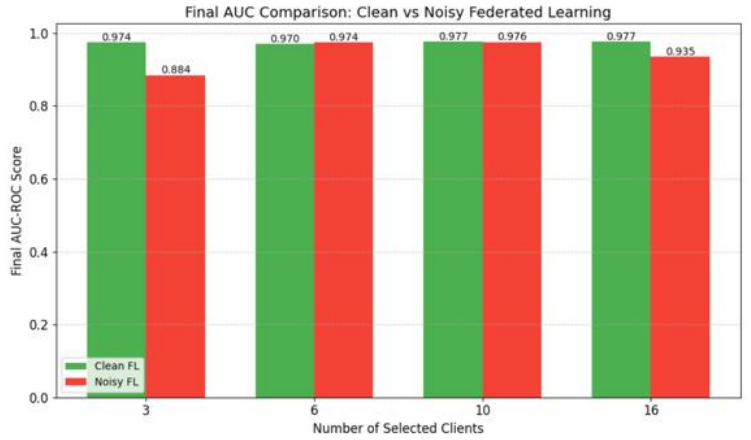
(c) Split Learning– AUC Across Client Selections



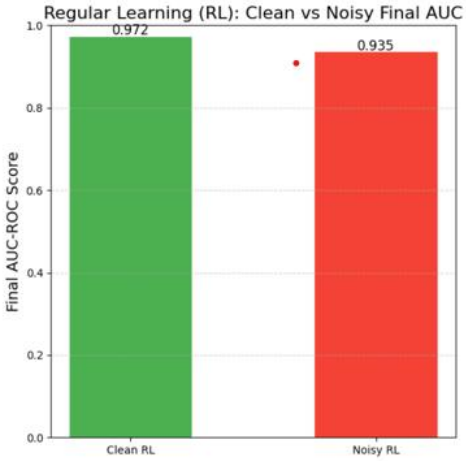
(d) Final AUC ROC Scores: FL vs RL vs SL

Robustness to Noisy Clients

- Simulated adversarial/malicious clients
- FL degrades less than RL under noise
  - FL (10 clients): −0.44% AUC drop
  - RL: −3.81% drop (0.972 → 0.935)
- FL shows strong resilience with balanced client diversity



(a) Clean vs noisy AUC-ROC scores for Federated Learning under varying client configurations.



(b) Clean vs noisy AUC-ROC scores for Regular Learning (centralized setup).

Comparison with State-of-the-Art

- Proposed FL model: AUC-ROC = 0.977
- Federated SDT [14]: AUC-ROC = 0.963
- Our model is more robust, especially under noise.
- Demonstrates practical reliability for real-world deployment.

MODEL	AUC-ROC
Proposed FL (Ours)	**0.977**
Federated SDT [14]	0.963

جامعة الشارقة
UNIVERSITY OF SHARJAH

Discussion & Insights

- CNN + SMOTE is most effective for this task.
- FL maintains privacy without sacrificing performance.
- Client count matters: too few or too many → instability under noise.
- AUC-ROC is essential for imbalanced fraud detection.

جامعة الشارقة
UNIVERSITY OF SHARJAH

Limitations & Future Work

- Limitation: Single dataset (European cards).
- Future directions:
  - Multi-institutional real-world data
  - Non-IID/heterogeneous client data
  - Concept drift adaptation
  - Explainable AI (XAI) + secure aggregation
  - Communication efficiency in FL/SL

جامعة الشارقة
UNIVERSITY OF SHARJAH

Conclusion

- FL enables accurate, private, and robust fraud detection.
- Outperforms centralized learning in adversarial settings.
- Validates deep learning + resampling in decentralized frameworks.

جامعة الشارقة
UNIVERSITY OF SHARJAH

Q&A

Thanks for your attention!

Question's time...

Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep Learning Algorithms

Fatima Muhair Alketbi [1], Fatih Kurugollu [2], Sebti Foufou [2], Isam Mashhour Al Jawarneh [2]

[1] *MSc in Data Science,* Department of Computer Science, University of Sharjah, UAE (U24102845@sharjah.ac.ae)

[2] Professor, Professor, & Assistant Professor @ Department of Computer Science, University of Sharjah, UAE

The 3rd International Conference on Intelligent Metaverse Technologies & Applications (iMETA2025) 2025

14-17 October 2025 | Dubrovnik, Croatia 17/10/2025