UNIVERSITY OF INFORMATION TECHNOLOGY, VNU-HCM
FACULTY OF COMPUTER NETWORKS AND COMMUNICATION

FRAUDGNN–RL: A GRAPH NEURAL NETWORK WITH REINFORCEMENT LEARNING FOR ADAPTIVE FINANCIAL FRAUD DETECTION

GVHD: THS. PHAN THẾ DUY

GROUP MEMBERS

Hoàng Bảo Phước - Thành viên
MSSV: 23521231

Đỗ Quang Trung - Trưởng nhóm
MSSV: 23521673

Nguyễn Đình Khang - Thành viên
MSSV: 23520694

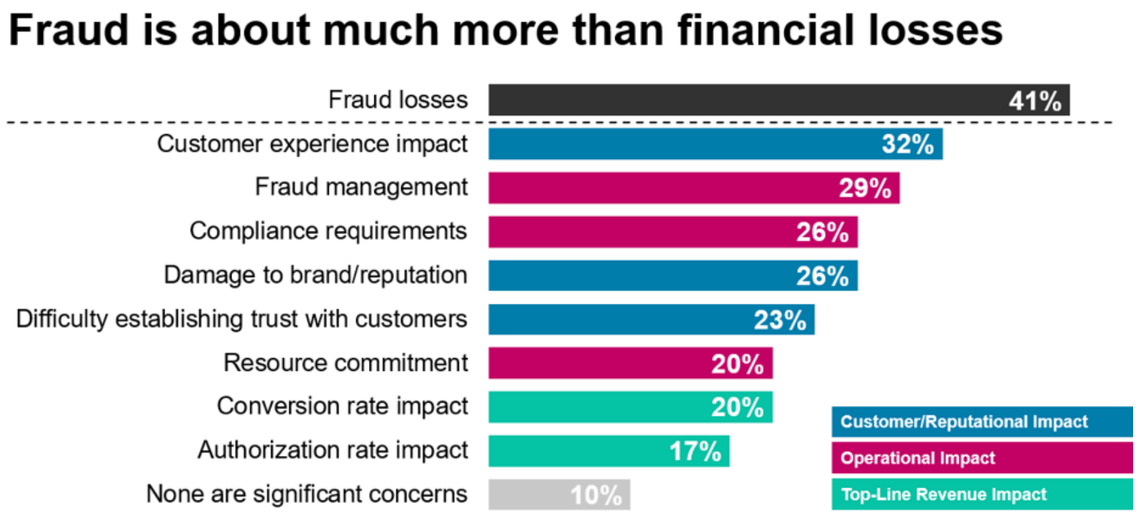
REFERENCES

CUI, Yiwen, et al. ***FraudGNN-RL: A Graph Neural Network With Reinforcement Learning for Adaptive Financial Fraud Detection.*** IEEE Open Journal of the Computer Society, 2025.

TABLE OF CONTENTS

THE CHALLENGE OF FINANCIAL FRAUD

Problem Statement: Financial fraud causes $5.127 trillion in global losses annually; sophisticated, evolving patterns challenge digital systems.



Significance: Critical need for advanced detection in digital financial services.

WHY FRAUDGNN-RL?

Limitations of Current Methods: Rule-based and static ML fail to capture complex relationships, adapt to changes, or ensure privacy.

Objective: FraudGNN-RL addresses temporal-spatial-semantic modeling, adaptability, and privacy.

TABLE OF CONTENTS

PRIOR WORK AND RESEARCH GAPS

Key Studies: Dal Pozzolo et al. (2018) – limited adaptability; Lebichot et al. (2019) – no RL; Liu et al. (2021) – lacks privacy/adaptivity.

Gaps: Inability to model complex transactions, adapt dynamically, or preserve privacy.

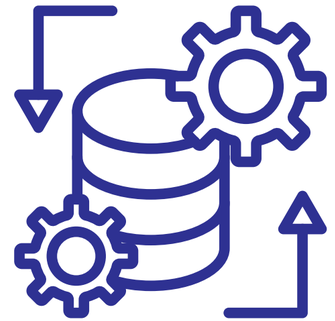
FraudGNN-RL Contribution: Integrates GNN, RL, and FL to address these gaps.

TABLE OF CONTENTS

DATA PREPROCESSING

- Missing value imputation using mean values for numerical features and mode for categorical features
- Feature scaling using min-max normalization for numerical features

- One-hot encoding for categorical variables
- Temporal feature extraction including hour of day transactions Reinforcement Learning (RL), and Federated Learning (FL).



FRAUDGNN-RL FRAMEWORK OVERVIEW

Overview: Combines Temporal-Spatial-Semantic Graph Convolution (TSSGC), Reinforcement Learning (RL), and Federated Learning (FL).

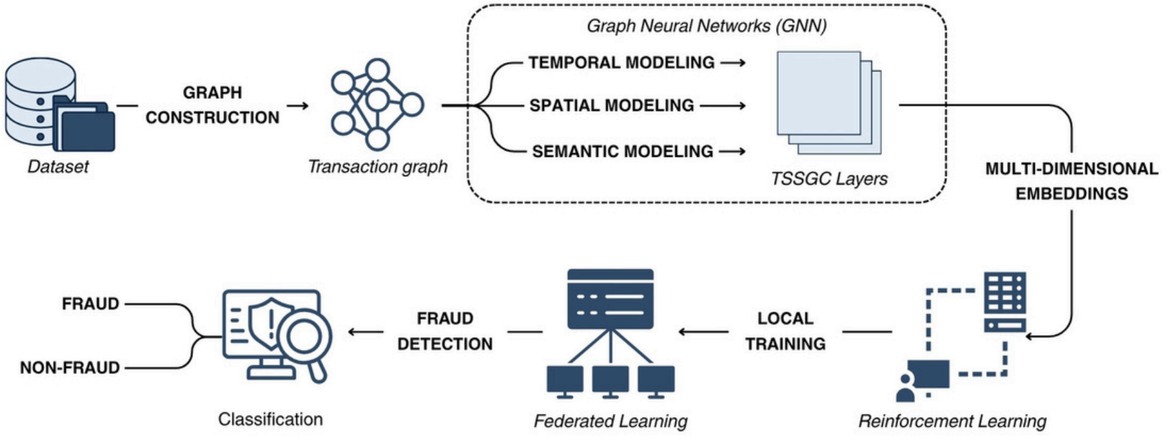


Figure: *Federated GNN-Based Fraud Detection Pipeline with RL-Driven Adaptation*

Purpose: Capture complex transaction patterns, adapt to evolving fraud, ensure privacy.

TSSGC: MODELING TRANSACTION GRAPHS

TSSGC (GNN-based): Captures temporal dynamics (GRU with attention), spatial relationships, semantic information (embeddings).

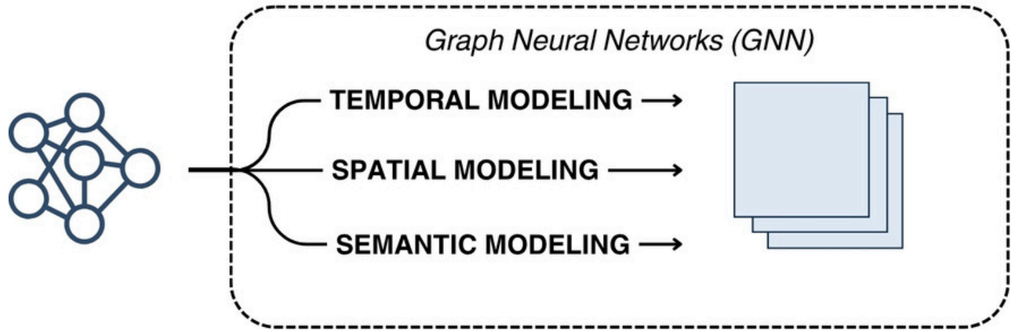
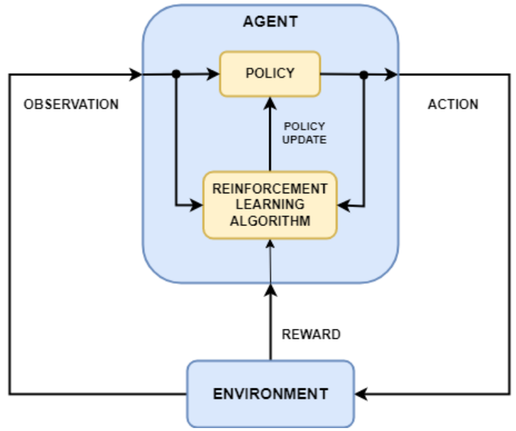


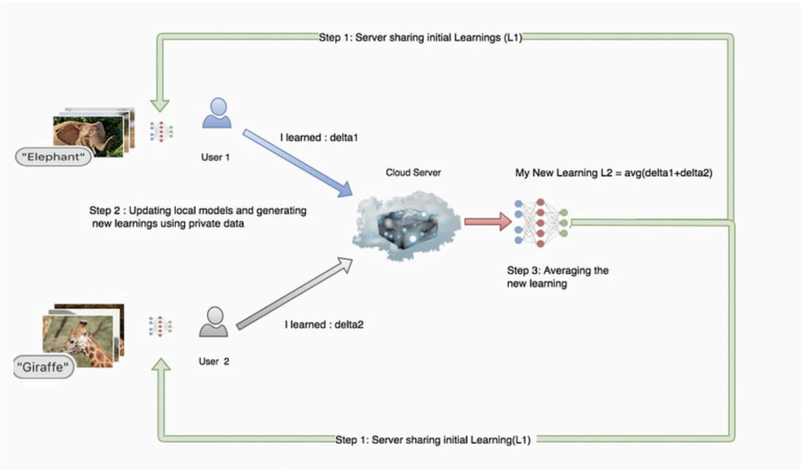
Figure: *Graph Neural Network Architecture Overview*

Uses GCN for stability, efficiency, and robustness.

RL AND FL FOR ADAPTIVITY AND PRIVACY

RL (DQN with NAF): State (TSSGC embeddings), Action (threshold/feature adjustments), Reward (accuracy vs. false positive rate).





FL (FedAvg): Privacy-preserving training via local parameter updates and global aggregation.

TABLE OF CONTENTS

EXPERIMENTAL SETUP AND DATASETS

The proposed model is **FraudGNN-RL**, combining:

- Graph Neural Networks **(GNN)** for capturing transaction relationships.
- Reinforcement Learning **(RL)** for dynamic threshold adjustment.
- Federated Learning **(FL)** for privacy-preserving (100 rounds total).

Credit Card Fraud 2023 Dataset:

Dataset	Transactions	Features	Fraud Rate	Time Span	Key Characteristics
Credit Card 2023	> 550,000	31	Imbalanced	2023	Anonymized features, temporal patterns

SCENARIO 1:

Method	AUC-ROC	AUC-PR	F1	Recal@5%
XGBoost	0.9570	0.4380	0.7830	72.10
Isolation Forest	0.9350	0.3920	0.7450	67.20
LOF	0.9220	0.3750	0.7120	64.80
DeepAE	0.9720	0.5380	0.8520	81.50
Our Methods	**0.9774**	**0.8752**	**0.8957**	**91.51**

Table. *Overall Performance Comparision of Fraud Detection Methods on Credit Card 2023 Dataset*

SCENARIO 2:

Method	Credit Card 2023			
	F1	AUC-ROC	AUC-PR	Recal@5%
GAT	0.8805	0.9701	0.8621	0.8948
GCN	0.8957	0.9744	0.8720	0.9151

GCN is more accurate and stable:

- **F1-Score** (GCN and GAT): **0.8957** and 0.8805 respectively.
- GAT is slightly more stable (lower F1 standard deviation), but the difference is very small.

TABLE OF CONTENTS

KEY ACHIEVEMENTS AND LIMITATIONS

The proposed FraudGNN-RL framework aims to simultaneously address three significant challenges in financial fraud detection: capturing **temporal-spatial-semantic** aspects, adapting to evolving fraud patterns **(concept drift)**, and maintaining **data privacy**.

F1-score and **AUC-ROC** are still lower than the original paper (0.928 and 0.996). Significant F1-score fluctuations (0.0034 to 0.7941), likely due to **non-IID client data**.

TABLE OF CONTENTS

FUTURE DIRECTIONS

Continue developing the model for the **IEEE-CIS dataset** while fine-tuning model parameters and validating data preprocessing on the **Credit Card Fraud 2023 dataset** to match the paper's results.

If the results are promising, apply **XAI methods** to analyze feature importance and enhance model performance.

THANK YOU

NT522.P21.ANTT - GROUP12