Relevance Analysis: FL in CCF Detection and Prevention

Relevance of Federated Learning (FL) for Credit Card Fraud (CCF) Detection and Prevention

1. Data Sensitivity: Credit card data is highly sensitive, and FL allows banks to train models on this data without the need to share it, maintaining confidentiality and compliance with regulations like GDPR.

2. Decentralized Learning: FL enables decentralized model training across multiple banks or financial institutions, leveraging diverse datasets to improve fraud detection models without consolidating data.

3. Real-time Updates: FL facilitates real-time model updates as new transaction data becomes available, allowing for quicker adaptation to emerging fraud patterns.

4. Collaborative Learning: It promotes collaborative learning among different entities without compromising individual data privacy, leading to more robust and comprehensive fraud detection models.

Application Examples of FL in CCF

1. Federated Averaging: Banks have used federated averaging techniques to collaboratively train models, where each institution contributes local updates to a global model, enhancing detection capabilities without data sharing.

2. Metaheuristic Optimization: As seen in the work by Mustafa Abdul Salam et al., metaheuristic algorithms like AGTO and COA have been applied to optimize the initial global model in FL, improving convergence speed and reducing communication costs.

3. Hybrid Models: The integration of FL with deep learning models, such as CNNs and LSTMs, has been successfully applied to analyze transaction patterns and detect fraudulent activities with high accuracy.

4. Blockchain Integration: FL combined with blockchain technology has been explored for secure and transparent data transactions in CCF detection systems, ensuring immutability and traceability of model updates.

Evaluate Effectiveness: FL's Impact on Data Privacy and Fraud Detection

1. Data Privacy: FL has proven effective in enhancing data privacy by allowing local model training and only sharing model updates, which are less revealing than raw data. This approach aligns with privacy regulations and builds trust among participating institutions.

2. Detection Accuracy: Studies have shown that FL models can achieve high accuracy rates in CCF detection, comparable to or exceeding traditional centralized models, by leveraging diverse and rich datasets from multiple sources.

3. Model Generalization: FL's distributed nature helps in training models that are more generalizable, as they learn from a wider range of transaction patterns across different banks.

4. Adaptability: FL models have demonstrated adaptability to new fraud tactics by continuously incorporating new data and updates from participating institutions, making the detection system more dynamic and responsive.

5. Performance Metrics: Evaluations based on metrics like accuracy, precision, recall, and F1-score have consistently shown FL's positive impact on the effectiveness of CCF detection systems.

Conclusion

In summary, FL is highly relevant for CCF detection and prevention due to its ability to maintain data privacy, improve model accuracy, and adapt to new fraud patterns in a collaborative and decentralized manner. The successful applications and positive assessments of its effectiveness underscore its potential as a leading technology in the financial sector's fight against fraud.

Reference

[1] Baabdullah, T, Alzahrani, A, Rawat, DB & Liu, C 2024, 'Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems', Future Internet, vol. 16, no. 6, p. 196, viewed 7 August 2024, <https://research.ebsco.com/linkprocessor/plink?id=bccb56af-54b4-3856-8b3c-c18c2f47527e>.

[2] Abdul Salam, M, Fouad, KM, Elbably, DL & Elsayed, SM 2024, 'Federated learning model for credit card fraud detection with data balancing techniques', Neural Computing and Applications, vol. 36, no. 11, pp. 6231–6256, viewed 7 August 2024, <https://research.ebsco.com/linkprocessor/plink?id=343034c6-6038-31b0-9701-70c15f4a3149>.

[3] Tahani Baabdullah, Amani Alzahrani, Danda B. Rawat & Chunmei Liu 2024, 'Efficienc y of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Perfor mance of Credit Card Fraud Detection (CCFD) Systems', Future Internet, vol. 16, no. 6, p. 196, viewed 7 August 2024, <https://research.ebsco.com/linkprocessor/plink?id=dc6747fd-41bb-339c-903f-43f42cf9badb>.

[4] Venkata Krishna Reddy, V, Vijaya Kumar Reddy, R, Siva Krishna Munaga, M, Karnam, B, Maddila, SK & Sekhar Kolli, C 2024, 'Deep learning-based credit card fraud detection in federated learning', Expert Systems With Applications, vol. 255, viewed 7 August 2024, <https://research.ebsco.com/linkprocessor/plink?id=9dd33e5a-5310-382f-b89c-1d97683a4688>.

[5] Salam, MA, El-Bably, DL, Fouad, KM & Elsayed, MSE 2024, 'Enhancing Fraud Detecti on in Credit Card Transactions using Optimized Federated Learning Model', Internationa l Journal of Advanced Computer Science and Applications, vol. 15, no. 5, pp. 258–263, v iewed 7 August 2024, <https://research.ebsco.com/linkprocessor/plink?id=c1d00114-2c44-378e-8172-d459746fc636>.