Differences Between 2024-25 Research and Previous Years' Papers on Credit Card Fraud Detection

Credit card fraud detection has evolved significantly in recent years due to advancements in artificial intelligence, data science, and cybersecurity. Here's how the latest research from **2024-25** differs from previous years:

---

1. Machine Learning vs. Deep Learning & AI Models

- **Previous Years (Before 2024)**
    - Research primarily focused on traditional **machine learning algorithms** like Random Forest, Decision Trees, Logistic Regression, and Support Vector Machines (SVM).
    - Feature engineering was heavily relied upon to manually select relevant features from transaction data.
    - Imbalanced data issues were addressed using oversampling techniques like **SMOTE (Synthetic Minority Oversampling Technique)**.
- **2024-25 Papers**
    - **Deep learning models** like **LSTM (Long Short-Term Memory) with Attention Mechanisms** are gaining popularity for modeling sequential transaction patterns.
    - **Transformer-based architectures (like BERT & GPT for fraud detection)** are being optimized for real-time transaction monitoring.
    - AI-driven models **automate feature extraction**, reducing the need for manual preprocessing.

---

2. Graph-Based Approaches for Complex Data Representation

- **Previous Years**
    - Fraud detection was primarily based on analyzing individual transactions.
    - Relationship-based fraud (e.g., coordinated fraud attacks) was harder to detect using traditional methods.
- **2024-25 Papers**
    - Graph-based models, such as **Graph Neural Networks (GNNs)**, are now being used to represent transactions as **networks of interactions** between customers, merchants, and banks.
    - **Heterogeneous graphs** (capturing multiple types of relationships) help detect fraud rings and synthetic identity fraud.

---

3. Self-Supervised Learning & Contrastive Learning

- **Previous Years**
    - Supervised learning methods required large amounts of labeled fraud data, which was difficult to obtain.

- Unsupervised anomaly detection methods were used, but they often resulted in a high number of false positives.

- **2024-25 Papers**
  - **Self-supervised learning** techniques like **Graph Contrastive Learning (GraphGuard)** allow models to learn fraud patterns with minimal labeled data.
  - **Autoencoders** and **generative models** help detect fraudulent transactions by reconstructing normal transaction patterns and identifying anomalies.

---

4. Real-Time Fraud Detection & Cloud Integration

- **Previous Years**
  - Most fraud detection models worked in **batch mode**, meaning fraud was detected after the transaction occurred.
  - Computational limitations restricted real-time fraud detection.
- **2024-25 Papers**
  - **Cloud-based fraud detection models** powered by **edge computing** allow for **real-time fraud prevention**.
  - Transformer-based architectures (optimized for real-time analysis) can scan millions of transactions per second, reducing the risk of fraud.

---

5. Focus on Privacy-Preserving Fraud Detection

- **Previous Years**
  - Fraud detection required access to raw transaction data, raising privacy concerns.
  - GDPR and other regulations restricted data-sharing between banks and fraud detection systems.
- **2024-25 Papers**
  - **Federated Learning (FL)** enables multiple banks to train fraud detection models **without sharing customer data**.
  - **Homomorphic encryption** ensures fraud detection can occur on encrypted transactions, preserving privacy.

Conclusion

- The research from **2024-25** represents a major shift **from traditional machine learning to deep learning, graph-based techniques, and self-supervised learning**.
- **Real-time detection, privacy-preserving methods, and cloud-based solutions** are now at the forefront of fraud prevention.
- The focus has expanded from just identifying fraudulent transactions to predicting fraud **before it happens**, making fraud detection **more proactive than reactive**.

References