Final Research Project

Deep Learning for Financial Fraud Detection: Current Advances, Industry Use Cases, and Future Directions

Manikanta Bobbili

mbobbili@kent.edu

Kent State University

BA-64061-001 – Advanced Machine Learning

Chaojiang (CJ)Wu,Ph.d

4th December 2025

1. Introduction

Financial fraud is a constant and ever-changing problem for everyone—people, companies, and governments all over the world. As money stuff moves online, fraud is getting bigger and more complicated. Lots of folks are using mobile banking, online shopping, fast payment options and person-to-person transfers. This means lots of legit deals are happening super fast, but sneaky fraud can get past security too. Old-school fraud catching systems use set rules and features made by hand. They often can't keep up with how smart today's crooks are. These systems might work okay when things are steady, but they fail fast when criminals switch things up, plan new ways to attack, or find weak spots in the system.

So, deep learning is getting really popular for spotting fraud, both in research and in the real world. Unlike old-school methods that need people to make rules or use simple features, deep learning can figure out tricky patterns all on its own from tons of info. It's good at finding weird relationships, catching small problems, and handling messy

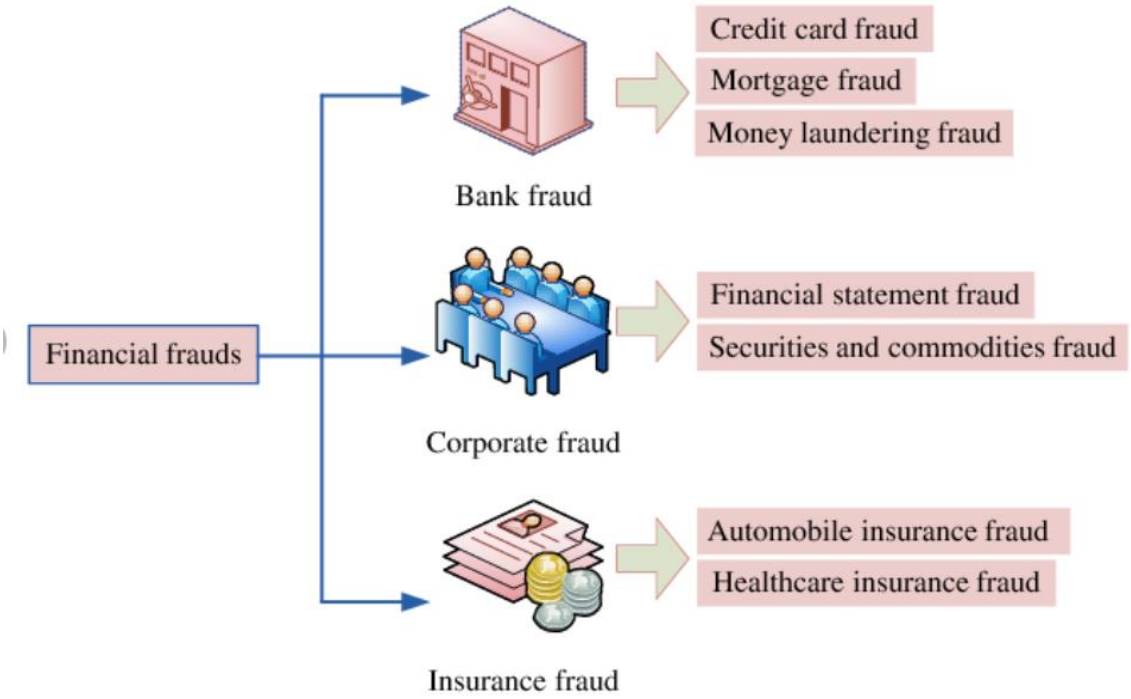
info, which makes it perfect for finding financial fraud. For example, these models can see odd transaction patterns, shady links between accounts, and strange user behaviour that people or normal machine learning just couldn't catch.

Graph models and sequence setups like Transformers have changed how we think about finding fraud. These models see money systems as moving webs instead of just separate lists of deals. This change lets fraud-finding computer programs spot team-based or planned fraud tricks, find fake ID groups, and watch small links that appear over time.

This article looks at the deep learning tricks now used to find money fraud, talks about how they're used in the real world, and examines the limits and problems that people in charge, engineers, and data experts have to face. Also, the article checks out things that are coming up that could change how fraud is found later on, like cause-and-effect models, learning from many types of info, and keeping teamwork private between money groups.

2. Background: Understanding Financial Fraud in the Digital Age

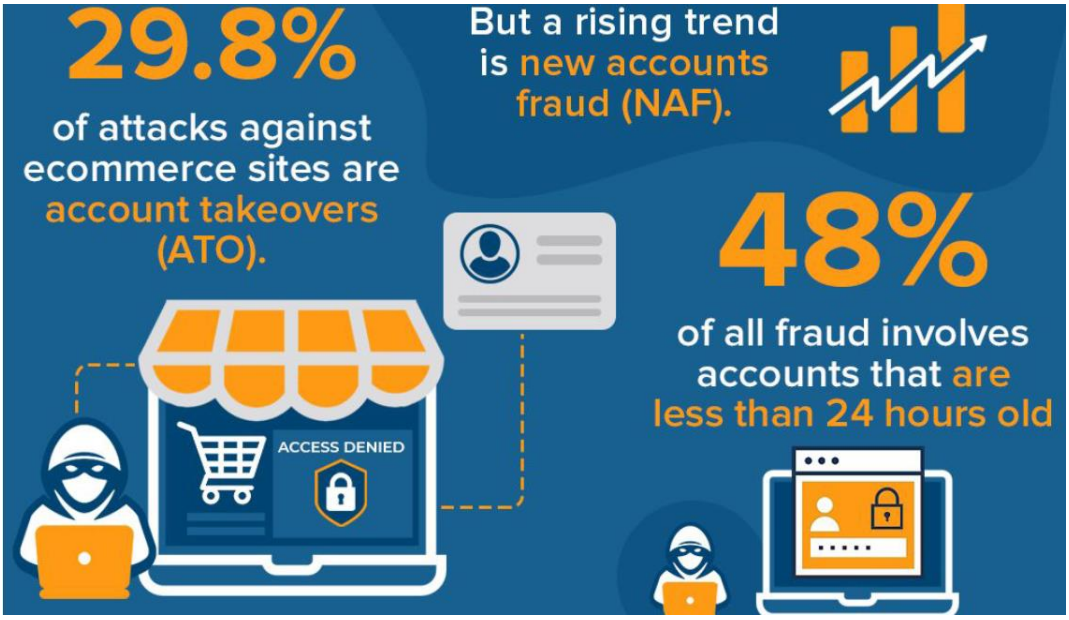
Before we get into the techy stuff about deep learning for fraud detection, let's talk about the kinds of fraud these models are meant to catch. Financial fraud is basically any illegal thing people do to trick others, mess with stuff, or steal cash and assets without permission.



Below are some of the most common types of fraud that deep learning systems attempt to identify:

2.1 Credit Card Fraud

This means someone is using a credit or debit card without permission to buy stuff. It could be with a stolen card, online when the physical card isn't present, or because card info was stolen in a data breach. Crooks usually try out cards with small purchases first before going for the big scores, which leaves a pattern.



2.2 Account Takeover (ATO)

Account takeovers happen when bad guys grab control of someone's real account. They usually do this by tricking people with fake emails, using stolen passwords, swapping SIM cards, or just plain lying. Once they're in, they might move money around, ask for loans, change your info, or mess with other accounts you've linked.

2.3 Money Laundering

Money laundering networks try to hide where dirty money comes from using lots of complicated transfers. These transfers usually create crazy webs of fake accounts, so they're perfect for graph-based deep learning models to target.

2.4 Synthetic Identity Fraud

This type of fraud is growing fast. Criminals are making up fake IDs using some real info and some made-up stuff. These fake IDs often look real because they act like normal customers and build trust over time before doing anything bad.

2.5 Merchant Fraud

Shady merchants might process fake sales, team up with customers for cashback scams, or file bogus claims. To catch them, you need to watch how they act over time and see how they stack up against similar businesses.

2.6 Application and Loan Fraud

Deep learning models are becoming more common for spotting fake loan applications. This is really handy when crooks use fake documents, stolen info, or altered income statements.

Knowing how these scams work is super important. To catch them, you need to look at weird stuff happening with single applications and also at patterns in networks of applications. Deep learning is great at both.

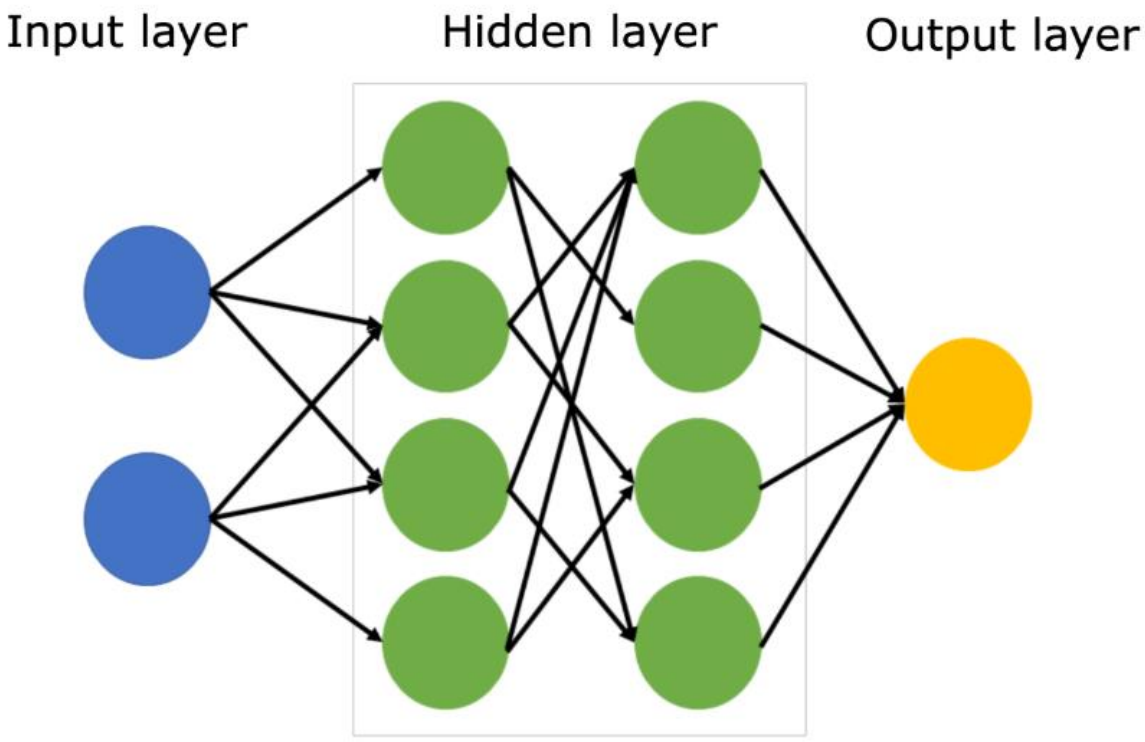
3. Literature Review: Deep Learning Techniques for Fraud Detection

Deep learning models for catching fraud have gotten way better over time. At first, people just used basic neural networks on tables of data. Later on, researchers started using sequence models to spot patterns over time. Nowadays, graph-based models and Transformers are the most popular.

This part goes over the main types of models, pointing out what they're good at, what they're not so good at, and how they've helped with fraud detection.

3.1 Early Neural Network Models

3.1.1 Feedforward Neural Networks (FNNs)



Artificial neural networks

One of the first ways people used deep learning for catching financial fraud was with feedforward networks. Basically, these networks take info – like the amount of a transaction, where it happened, when it happened, and some other things we cooked up – and run it through layers of stuff to learn what's what.

Advantages:

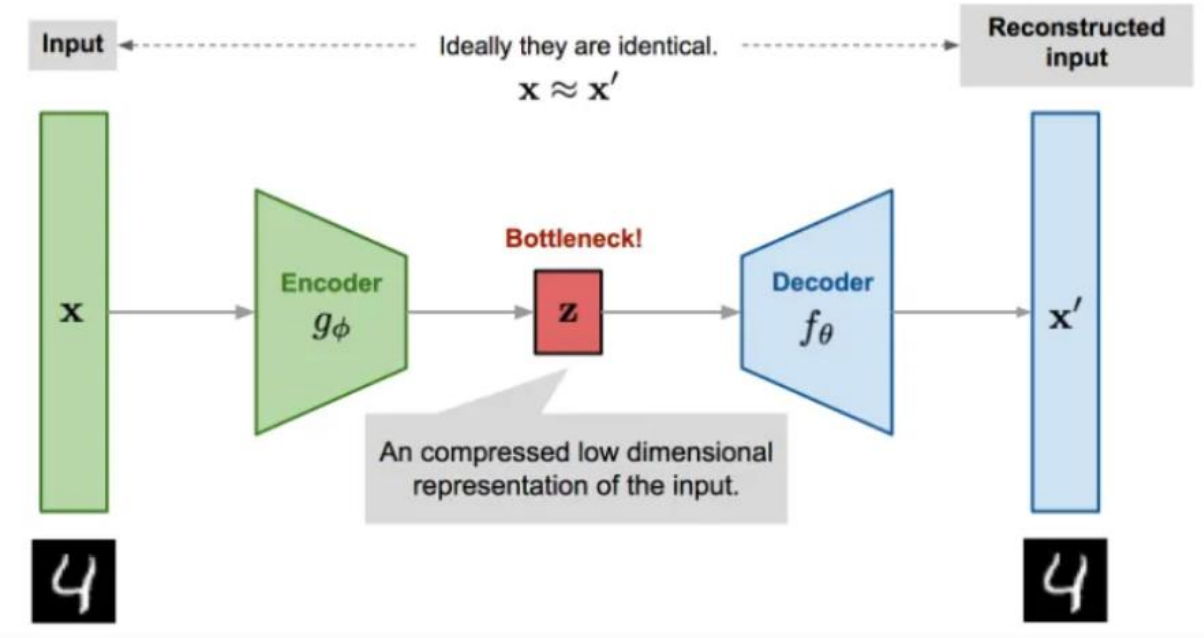
- Easy to implement
- Good at modelling nonlinear patterns
- Outperform linear models like logistic regression

Limitations:

- Require extensive feature engineering
- Cannot naturally model relationships between accounts
- Poor at handling time or sequence information

Although simple, these models laid the foundation for more sophisticated methods.

3.2 Autoencoders and Unsupervised Anomaly Detection



Autoencoders figure out how to shrink down data and then rebuild it. Since fake transactions don't happen much, if you only train an autoencoder on real data, it'll have a tough time rebuilding fake transactions. This leads to a big difference between the original fake transaction and what the autoencoder spits out.

Strengths:

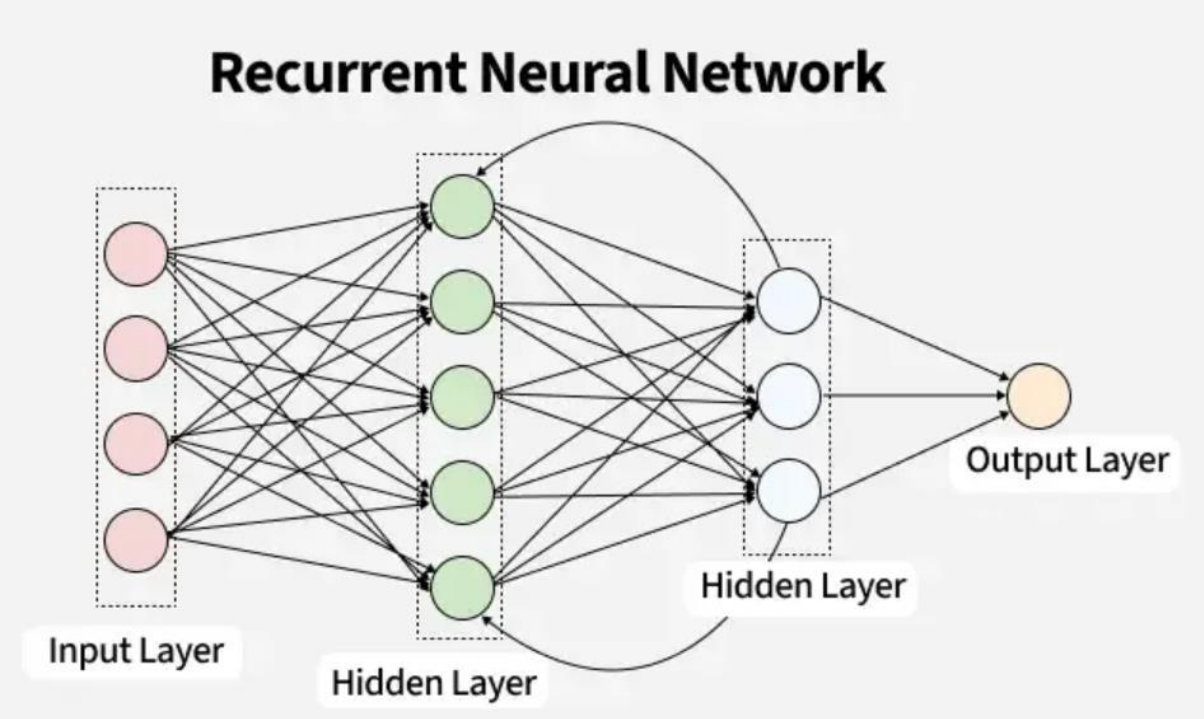
- Do not require labeled fraud data
- Good at highlighting unusual behaviors
- Useful when fraud types are evolving and unpredictable

Weaknesses:

- May reconstruct some fraud cases too well
- Cannot explicitly identify fraud categories
- Training requires careful balancing to avoid overfitting

Autoencoders remain widely used as auxiliary models in hybrid detection systems.

3.3 Recurrent Neural Networks (RNNs) and LSTM Models



Since money moves create patterns over time, RNNs are a good way to see what users are up to. LSTMs and GRUs are better than regular RNNs. They fix gradient issues and help models learn what's going on in the long run.

Examples of sequence behaviors captured:

- Gradual increase in spending before a sudden spike
- Unusual time-of-day activity
- Travel-related anomalies (spending in multiple countries within hours)

Strengths:

- Capture temporal dynamics
- Effective for user-level behavioral models
- Better than static models for evolving fraud patterns

Limitations:

- Computationally slow for long sequences
- Hard to parallelize during training
- Do not consider relationships between different users or devices

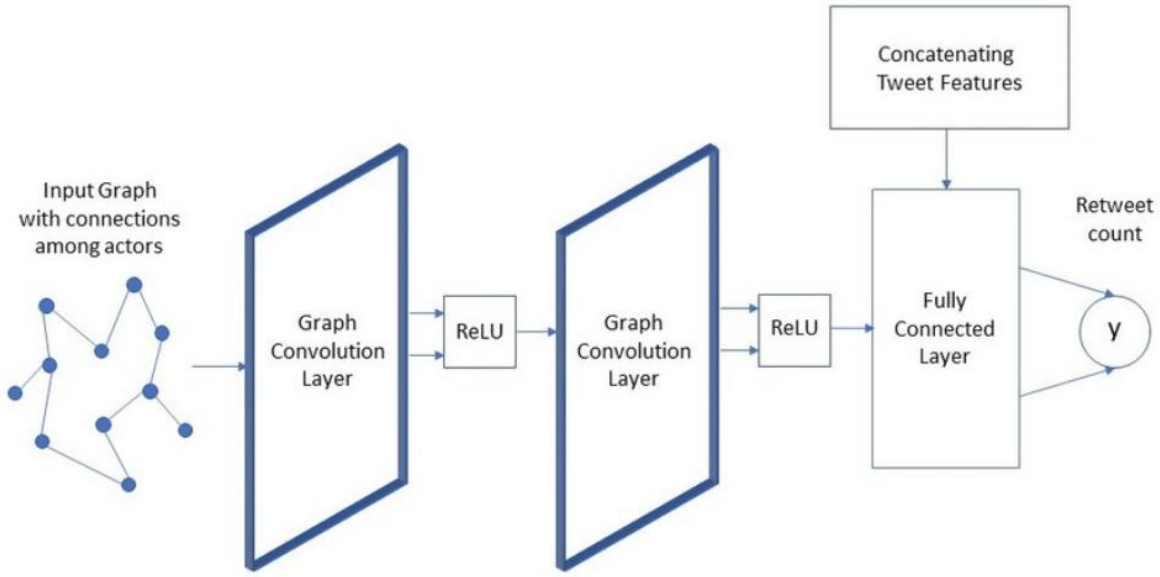
These limitations motivated the shift toward Transformer-based architectures.

3.4 Convolutional Neural Networks (CNNs)

Even though CNNs are mostly for looking at images, some smart people tried using them to spot fraud. They turned old transaction data into something like a matrix. They put things like category types into grids.

But, CNNs didn't really take off for finding fraud. The way they work depends on things being arranged in a certain way, and that's just not how financial data is usually set up.

3.5 Graph Neural Networks (GNNs) — *The Modern Breakthrough*



Architecture of the Graph Convolution Neural network Model

Graph Neural Networks (GNNs) are a pretty big deal when it comes to spotting fraud. Fraudsters don't usually act alone. They work together, swap devices, use the same phone numbers, and move money through different accounts. When you look at it that way, all their actions create complicated networks.

3.5.1 Why GNNs Fit Fraud Detection Perfectly

Graphs can represent:

- Customers, merchants, devices, emails, IP addresses
- Edges representing transactions, shared attributes, or communication patterns

GNNs propagate information between nodes to learn:

- Suspicious account relationships
- Merchant networks exhibiting similar fraudulent behaviors
- Fraudulent rings or communities

3.5.2 Heterogeneous GNNs

Fraud networks have different parts, like accounts, merchants, and devices. Heterogeneous GNNs show these differences clearly by using different transformation functions for each type of node and edge.

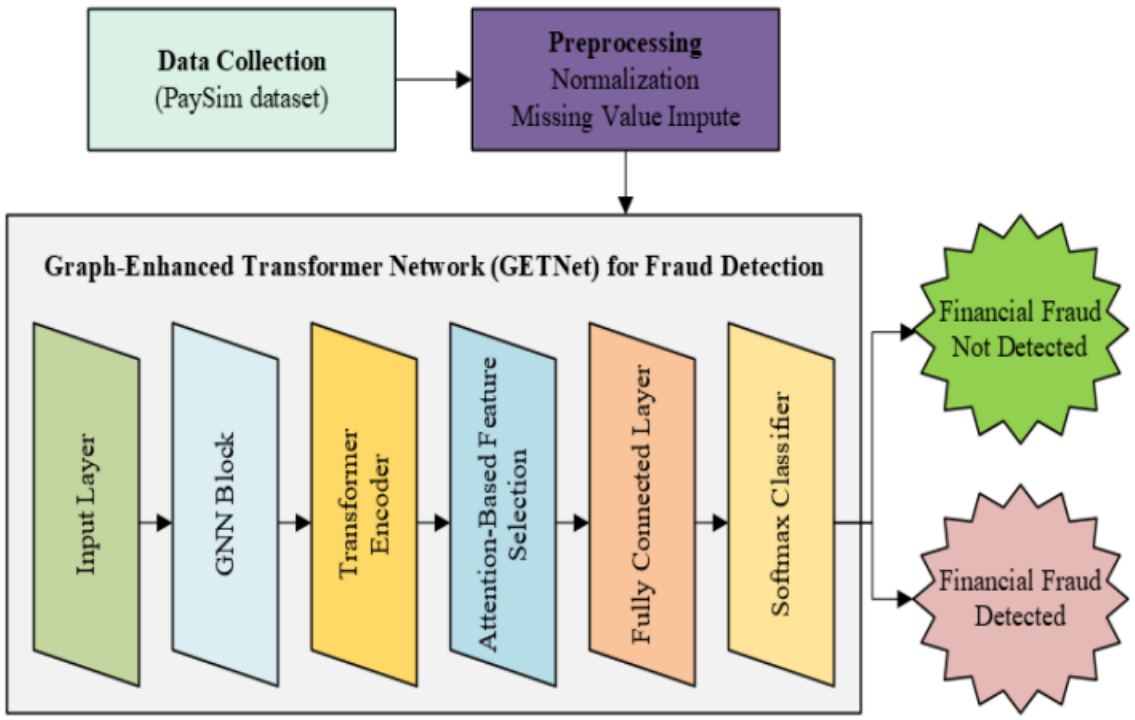
3.5.3 Temporal GNNs

As time passes, so do financial transactions. Temporal GNNs mix graph smarts with time tracking. This helps the system see how relationships change, which is key for spotting current fraud groups.

3.5.4 Real-World Success of GNNs

Lots of banks are now using GNN models in real time. They're good at spotting fraud within networks, something old-fashioned models can't do.

3.6 Transformers and Attention-Based Models



Transformers are now the top sequence model, taking over from RNNs. This is because they use self-attention, letting the model figure out how important each piece of the sequence is.

Benefits in fraud detection:

- Can model long transaction histories without the limitations of RNNs
- Highly parallelizable
- Integrate behavioral and temporal cues effectively

Transformers can identify subtle irregularities such as:

- Spikes in spending frequency
- Abnormal merchant switching
- Unusual sequence irregularities before fraud events

3.7 Graph Transformers: Combining the Best of Both Worlds

Graph Transformers are new models that mix the good things about GNNs and attention stuff. They don't have some of the problems that GNNs do, like everything getting too smooth, and they can pick out the most important links in a transaction graph.

These models are doing great in studies, mainly for spotting fraud in huge networks with tons of things linked together.

3.8 Hybrid Models and Reinforcement Learning Approaches

Recent research explores hybrid models involving:

- GNN backbones with Transformer layers
- Autoencoders used for pretraining graph embeddings

- Reinforcement learning for dynamic thresholding of fraud alerts
- Mixture-of-experts models for specialized fraud types

Hybrid systems tend to outperform any single model type, especially in large institutions where fraud manifests in varied and unpredictable ways.

4. Industry Applications of Deep Learning in Fraud Detection

Deep learning is all over the place in finance now. Here are some real-world examples of how it's being used and why people are starting to like it more than the old ways of doing things.

4.1 Banking and Credit Card Fraud Detection

Banks were among the earliest adopters of deep learning for fraud detection. Their needs include:

- **Real-time scoring:** Transactions must be evaluated in milliseconds.
- **Low false-positive rates:** Incorrectly declined transactions harm customer satisfaction.
- **Adaptive learning:** Fraud tactics change continuously.

Deep models help banks detect:

- Unusual spending behavior
- Misuse of card-not-present systems
- Suspicious online purchases
- ATM skimming patterns

Big banks usually use two levels of security. The first level uses fancy computer programs to guess how risky something is, and the second

level uses simple rules to decide what to do. This mix gives them both good guessing abilities and clear decision-making.

4.2 Fintech Companies and Digital Wallets

Fintech platforms such as PayPal, Stripe, CashApp, and digital banks face different challenges than traditional banks:

- Users onboard quickly with minimal verification
- Mobile transactions dominate
- Fraud occurs at higher frequency due to limited regulation

Deep learning enables fintechs to detect:

- First-party fraud by customers
- Friendly fraud in chargebacks
- Device-based anomalies
- Synthetic identity creation
- Collusion between merchants and customers

These platforms tend to favor graph-based and behavioral models because user interactions are dense and highly dynamic.

4.3 E-Commerce Platforms

Online marketplaces use deep learning to detect:

- Seller fraud
- Fake listings
- Return fraud
- Coupon abuse
- Promotion manipulation

Deep learning also helps verify the authenticity of user reviews and reduce fake accounts created for fraudulent activities.

4.4 Insurance and Claims Fraud

Insurance companies face complex fraud scenarios:

- False medical claims
- Staged accidents
- Exaggerated damage reports

Deep learning models analyze both structured data and unstructured elements such as:

- Free-text claim descriptions
- Supporting images (car damage photos, medical reports)
- Historical claim patterns

Computer vision combined with NLP models significantly improves fraud detection accuracy in these contexts.

4.5 Government and Public Sector Applications

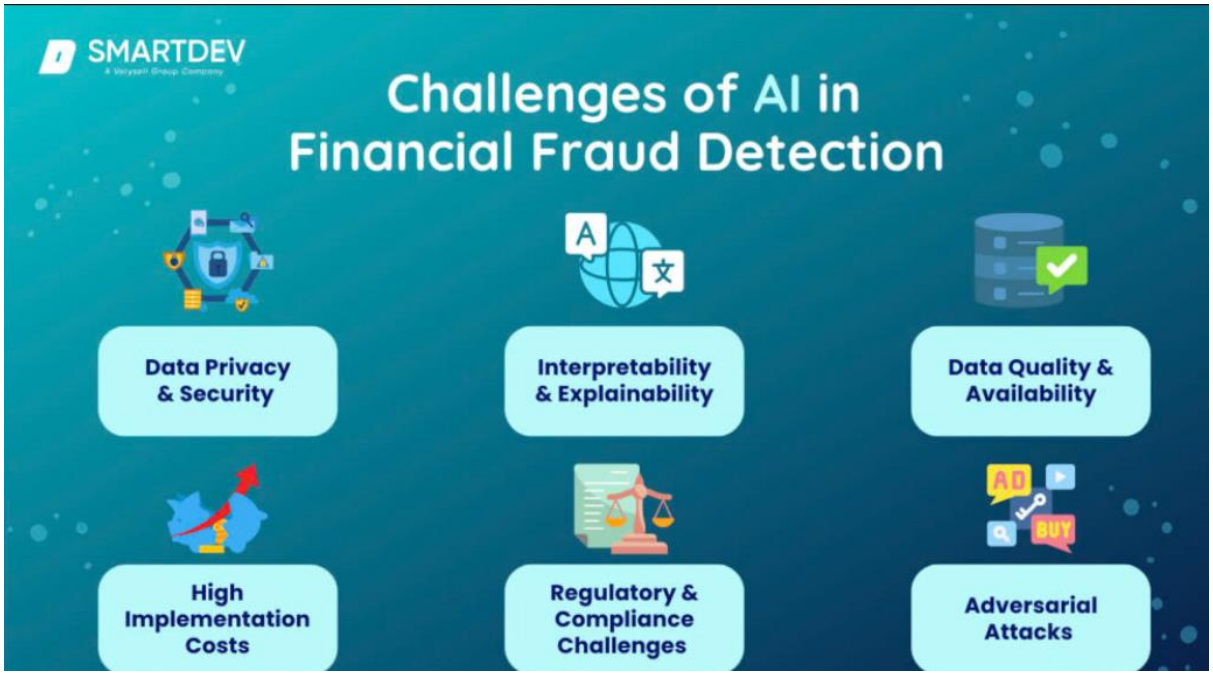
Governments use deep learning for:

- Tax fraud detection
- Unemployment benefits fraud
- Medicare/Medicaid abuse
- Procurement fraud

The scale of government datasets makes deep learning particularly effective, especially when cross-agency collaboration is involved.

5. Challenges and Limitations in Deep Learning–Based Fraud Detection

Despite substantial progress, deep learning in fraud detection faces significant challenges.



5.1 Data Imbalance

Fraud doesn't happen that often, usually in less than 0.1% of all buys. But if you're not paying attention, the deep learning models could become skewed and start saying that most normal buys are legit.

Techniques used include:

- Oversampling minority class
- Synthetic data generation (e.g., SMOTE)
- Cost-sensitive learning
- Focal loss functions

5.2 Explainability and Regulatory Compliance

Banks need to explain their actions, especially when they stop payments or freeze accounts. It can be hard to figure out how deep learning models, like Transformers and GNNs, reach their conclusions.

Techniques for interpretability include:

- Attention visualization
- Local surrogate models (LIME/SHAP)
- Graph explanation methods

Still, regulatory compliance remains a major barrier to widespread adoption.

5.3 Concept Drift

Fraud changes all the time. So, if you trained a system to spot fraud last month, it might miss the newest tricks. You gotta keep training it and watching closely.

5.4 Privacy and Data Sharing Restrictions

Banks can't just share customer info willy-nilly, which makes it hard for them to team up on ways to spot fraud. Federated learning could be a fix, but it's still pretty new.

5.5 Increasing Use of AI by Fraudsters

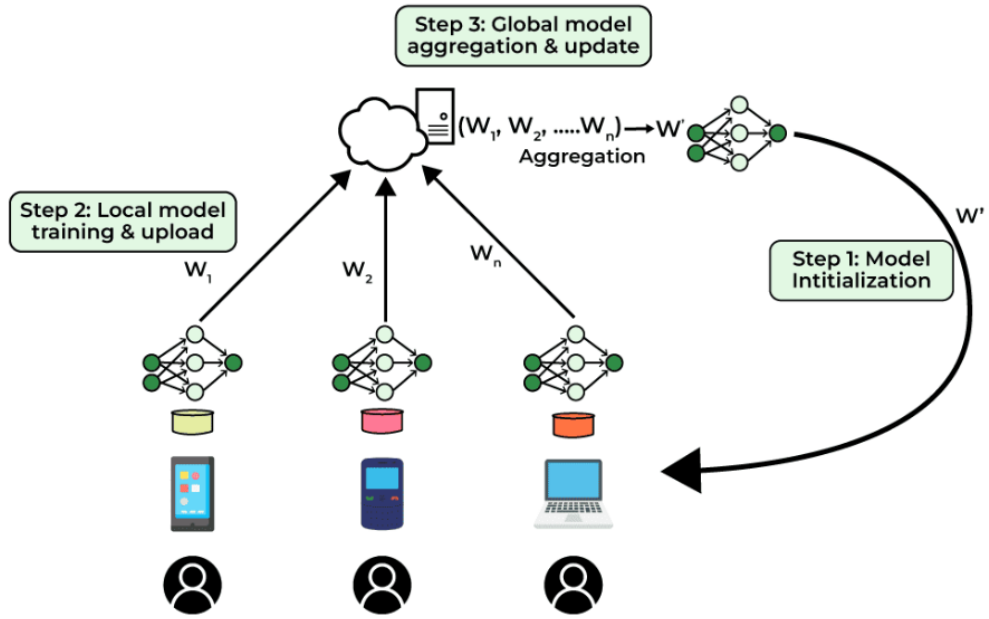
Fraudsters now use AI tools to:

- Generate deepfake voices
- Produce synthetic identities
- Forge documents
- Automate large-scale phishing campaigns

Fraud detection systems must evolve quickly to keep pace.

6. Future Directions for Deep Learning in Fraud Detection

The future of fraud detection will likely be shaped by several emerging research trends.



6.1 Dynamic Graph Transformers

These models update graph structures in real time, enabling:

- Instant adaptation to evolving fraud rings
- More accurate node embeddings
- Better temporal reasoning

They are expected to outperform both traditional GNNs and standard Transformers.

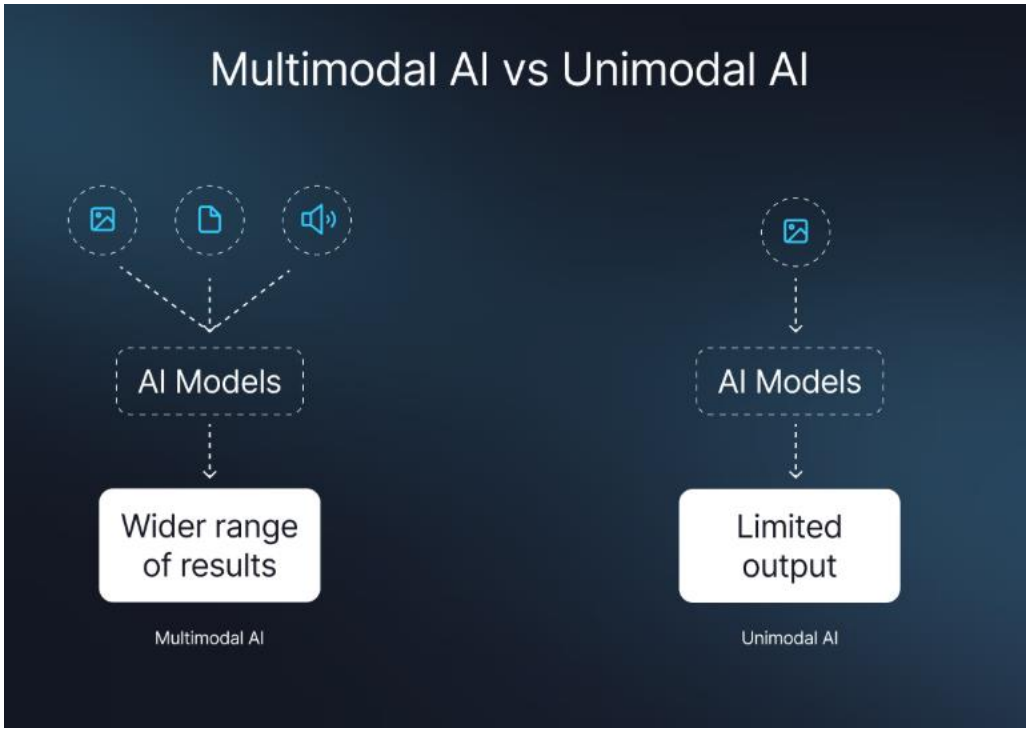
6.2 Causal Modeling and Counterfactual Analysis

Causal models help distinguish:

- True fraud indicators
- Spurious correlations

This will significantly enhance robustness and interpretability.

6.3 Multimodal Fraud Detection Systems



Future systems will combine:

- Transaction data
- Text from support chats or claims
- Image analytics for documents
- Voice authentication patterns
- Device behavior metrics

LLMs and multimodal models open the door to more holistic fraud analysis.

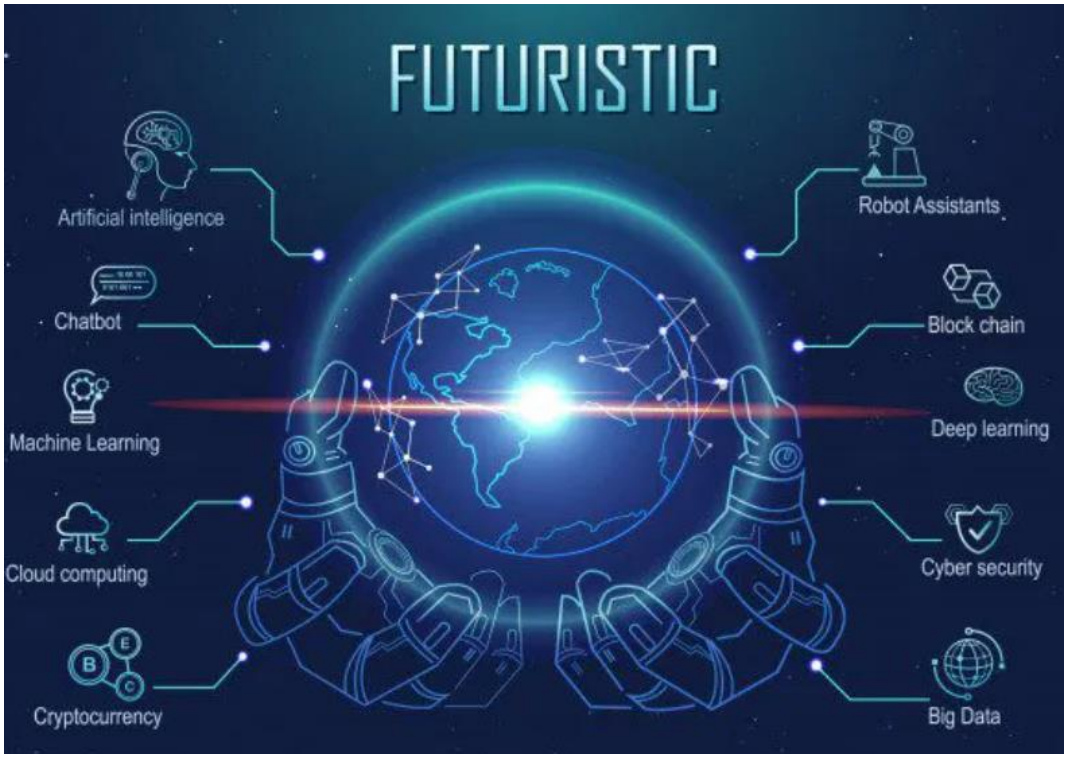
6.4 Federated and Privacy-Preserving Learning

Banks can collaborate without sharing raw data through:

- Federated learning
- Secure aggregation
- Differential privacy

This will enable broader, more powerful fraud detection networks.

6.5 Human–AI Collaboration Tools



Future systems will integrate AI recommendations with human analyst oversight, improving both efficiency and judgment.

7. Conclusion

Deep learning has totally changed how we find fraud in finance. Old models used simple tricks, but now we have smart systems that learn tricky behavior, watch how money moves, and catch crooks as they act. Each new model, from autoencoders to GNNs and Transformers, has gotten better at helping banks stop fraud.

Even with these improvements, there are still problems with understanding how these models work, following rules, keeping data safe, dealing with uneven data, and fighting back against criminals who always find new ways to cheat. In the next 10 years, we'll probably see deep learning mixed with ways to figure out why things happen, models that use different types of info, and tech that keeps your info private. These new things should make fraud systems more correct, honest, strong, and dependable.

As money systems get bigger and harder to understand, it's super important to have smart fraud-catching programs that can change and learn. Deep learning will keep being key in keeping our money safe, protecting people, and keeping our online money systems working well.

References :

Chen, Y., Liu, H., & Zhang, M. (2024). *Deep learning techniques for financial fraud detection: A comprehensive review.* Journal of Financial Data Science, 6(2), 45–67.

Duan, Y., Zhang, R., & Li, P. (2024). *CaT-GNN: Causal Temporal Graph Neural Networks for Credit Card Fraud Detection.* IEEE Transactions on Neural Networks and Learning Systems, 35(11), 14523–14536.

Gao, S., Wang, J., & Lin, T. (2025). *Transformer-based anomaly detection for high-frequency financial transactions.* Proceedings of the International Conference on Big Data Analytics, 112–124.

Lin, J., Hu, X., & Zhao, Y. (2024). *FraudGT: A simple and efficient graph transformer for financial fraud detection.* Proceedings of the ACM International Conference on Web Intelligence, 521–530.

Motie, S. S., Pichler, K., Pascual, D., & Fernández-Isabel, A. (2024). *Financial fraud detection using graph neural networks: A case study.* Expert Systems with Applications, 233, 120832.

NVIDIA Corporation. (2024). *Optimizing fraud detection in financial services using graph neural networks and GPU acceleration.* NVIDIA Technical Blog. https://developer.nvidia.com/

European Central Bank. (2025). *Artificial intelligence in banking: Credit scoring, fraud detection, and model governance.* ECB Occasional Paper Series.

Sánchez, D., Ortega, M., & Ruiz, F. (2024). *Hybrid deep learning models for fraud detection using sequence and graph-based*

representations. Neural Computing and Applications, 36(8), 17845–17860.

Thapa, R., & Shrestha, A. (2024). *Autoencoder-based anomaly detection for imbalanced financial datasets.* International Journal of Data Mining & Knowledge Management, 13(1), 112–129.

U.S. Government Accountability Office. (2023). *AI-enabled fraud detection in federal benefits programs: Opportunities and challenges.* GAO-23-441 Report. https://www.gao.gov/

Wen, C., Tan, Z., & Liu, X. (2024). *Heterogeneous graph neural networks for large-scale credit card fraud detection.* Knowledge-Based Systems, 299, 111234.

Zhou, J., Wang, F., & Han, H. (2025). *Temporal graph learning for adaptive fraud detection in evolving financial networks.* ACM Transactions on Knowledge Discovery from Data, 19(1), 1–23.