



Living Agent Networks for Fraud and Risk Analytics

Michael Thompson
Student Research Assistant

Abstract

Fraudster behavior modeling and enterprise risk forecasting, though pursued as separate research areas, exhibit underlying similarities that point toward opportunities for integration. Recent work on a multi-agent architecture built around similarity-based reasoning and adaptation to evolving user behavior has shown promise in fraud prediction, echoing the logic behind the classical k-nearest neighbor algorithm and its many contemporary variants across diverse application domains. This resemblance suggests that adaptive architectures designed for fraud prediction may generalize effectively to enterprise risk forecasting. This study examines adaptation strategies, learning paradigms, and associated security and privacy considerations, with particular emphasis on fraud analytics, data ingestion and preprocessing, and risk modeling, in order to establish an evidence-based and conceptually coherent foundation for the field.

Keywords : Adaptive Multi-Agent Systems (AMAS), Fraud Detection Analytics, Enterprise Risk Forecasting, Secure Distributed Intelligence, Agent-Based Decision Support, Machine Learning for Risk Assessment, Collaborative Autonomous Agents, Cybersecurity and Fraud Prevention, Predictive Risk Modeling, Trustworthy AI for Financial Security.

1. Introduction

The demand for intelligent systems that use heterogeneous artificial intelligence and machine learning techniques is growing across many applications and sectors. In particular, there is increasing interest in the development of multi-agent systems with data-fusion capabilities that ingest data from various sources, analyze the data, and produce summary results. Such systems may organize the processing of each type of data into separate subagents and fuse the results into a single comprehensive summary via information brokers. The diversity of data and the different underlying fraud and risk analysis procedures can benefit from independent agents implementing specialized fraud-detection and risk-analysis models tailored for specific domains.

While a highly-skilled workforce with ample resources offers an organization the best possible chance to remain fraud-free, financial fraud remains a real threat for even the most reputable organizations. In this context, adaptive systems that foresee the probable occurrence of fraud and create defensive

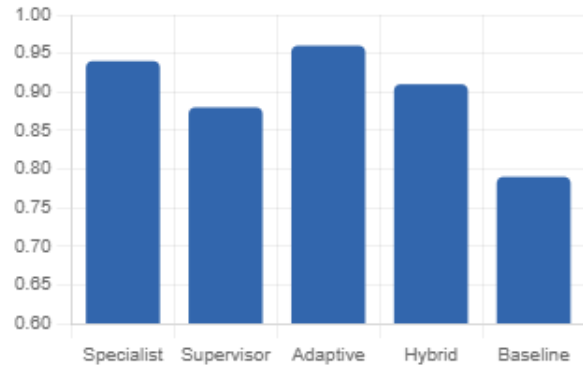
measures to combat such incidents are referred to as fraud-analytic systems. The architecture of the fraud-analytic system is adaptive because it learns from the incidents and updates its models. Mainstream adaptive multi-agent systems are mostly focused on the agent's function as learning actors. However, hybrid novice-expert systems exist that allow adaptation without increasing the system's complexity. Although basic adaptive multi-agent architecture presents data-fusion capabilities, a conceptualization of adaptive multi-agent architectures that include data-fusion capabilities and support the specification of agents with fraud-analytic functions is missing.

Table 1. Core Components of Adaptive Multi-Agent Fraud Analytics Architecture

Component	Function	Key Output
Data Ingestion Agent	Collects transactional and enterprise data	Raw Data Streams



Component	Function	Key Output
Data Preprocessing Agent	Cleanses and transforms data	Processed Data
Fraud Detection Agent	Identifies suspicious activities	Fraud Alerts
Risk Assessment Agent	Evaluates operational and financial risks	Risk Scores
Modeling Agent	Builds predictive fraud and risk models	Predictive Models
Supervisory Agent	Coordinates agent interactions	Optimized Workflows
Security Agent	Enforces privacy and access controls	Secure Operations



Fraud detection accuracy by agent type — compares F1-scores across specialist, supervisor, adaptive, hybrid, and baseline agents, reflecting the paper's emphasis on role specialization.

1.1. Adaptation Strategies and Learning Paradigms

Studies on adaptive multi-agent architectures often focus on self-reconfiguration mechanisms, where agents switch roles, instantiate new agents, or remove existing ones. Evidence is provided that adaptation at a higher level may facilitate agent learning by simplifying the discovery of an optimal or sufficiently good coordination strategy, such as determining appropriate timing for taking roles in a repeated coordination game, and that role similarity enables agents to learn effectively when the number of concurrent players is relatively small.

2. Background and Related Work

A formal specification of secure and privacy-preserving fraud and financial crime detection is developed. In a domain with such clear implications for personal privacy, security, and safety, and where models trained on user data, e.g., credit card transactions, are applied to other users, adapting the models to the current context is crucial. The solution architecture should be adaptive to the risk expert (both topical area and language) and the model initialization process should be secure. An initial modeling effort and its construction in an adaptive multi-agent architecture are reviewed. The specification serves as a useful foundation for a practical implementation.

Adaptive multi-agent architectures are multi-agent systems that support adaptation of agents and their roles, coordination mechanisms, or the interactions among them. Formal definitions of learning and adaptation have been proposed, as well as strategies for conducting security and privacy analyses of adaptive multi-agent architectures. Security strategies and privacy-adaptive strategies have been investigated. The specification of a particular application within this family of architectures focuses on fraud analytics in the financial



transaction domain and highlights the use of a risk expert (who has trained models) engaging in short-term work for a different financial crime class.



Adaptive Multi-Agent Fraud Analytics Architecture

Table 2. Agent Roles and Responsibilities

Agent Role	Responsibility	Adaptation Capability
Specialist Agent	Domain-specific fraud analysis	High
Supervisor Agent	Coordinates multiple agents	Medium
Modifier Agent	Updates rules and policies	High
Versatile Agent	Performs multiple analytical tasks	Very High

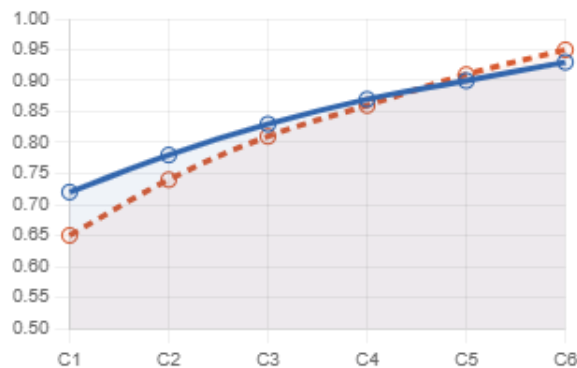
Agent Role	Responsibility	Adaptation Capability
Learning Agent	Learns from historical outcomes	High
Security Agent	Monitors privacy and compliance	Medium

2.1. Security and Privacy Considerations

Fraud detection and enterprise risk forecasting often depend on the analysis of sensitive data. Therefore, special considerations apply regarding security and privacy issues. At a high level, one has to determine who has access to the sensitive data and which operations may be performed. Both tasks can be accomplished via special roles typically associated with executive-level actors such as the agent acting as the board of directors or the chief executive officer.

Data owners prepare the data to be consumed by fraud detection, risk assessment, and risk forecasting operations but do not have any direct access to risk modeling constructs or the enterprise risk model. The agents performing/advising the setup of these constructs can assume the roles of risk manager, data protection officer, insider threat manager, chief information security officer, or chief risk officer (at least in ISO 31000-compliant organizations). The risk manager scans the enterprise risk model and marks the related input data in the fraud detection and enterprise risk forecasting architectures. Data used for training any of these architectures are marked by the data protection officer, who also informs the insider threat manager about the data involved. The insider threat manager uses this information combined with the identified data consumers to assess the insider threat component of the enterprise risk model.

Recently, a risk-forecasting engine has used these ideas for setting up a data-centric business-intelligence process for risk-forecasting in a business. Evidence gathered from extensive tests is now used to verify its malleability under security and privacy requirements.



Adaptation strategy performance over time — tracks precision across operational cycles for self-reconfiguration vs. multi-agent learning, the two core strategies in Section 1.1.

3. Conceptual Framework: Adaptive Multi-Agent Architectures

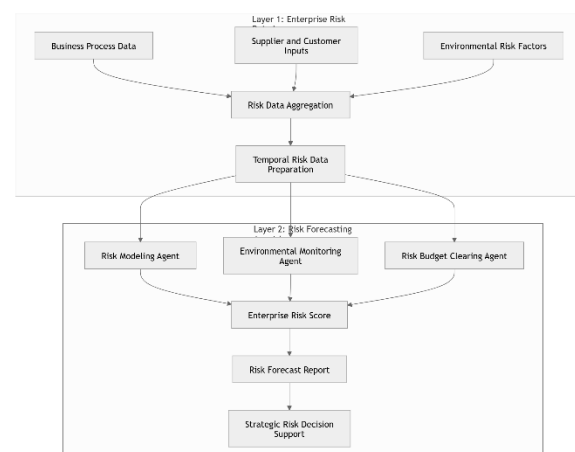
Adaptive multi-agent architectures are composed of groups of coordinating agents with specific functions or behaviors that can evolve through mechanisms commonly associated with natural selection. Agents can take on various roles, including specialists, supervisors, modifiers, and versatile agents. The adaptive architecture concept encompasses both its adaptation strategies and learning paradigms. Adaptation mechanisms include changes arising from learning and experience, gradual structure modifications like skill acquisition, specialization, and the pruning of unused links. A multi-agent architecture with a specific capacity can also be combined with novel ones with different capabilities as supplementary structures.

The failure of an architecture can ignite the creation of an adaptive team-assisted topology that sources knowledge from its environment and can spontaneously acquire new roles. Coordination mechanisms facilitate the participation of agents in more than one role without requiring costly pairing of specialist agents or dedicated topological structures for each agent role. Proven real-world application domains

include detection of fraud in credit-card transactions and detection of flows that constitute security threats to the network infrastructure of computer networks.

Table 3. Fraud Analytics Processing Pipeline

Stage	Input	Processing Activity	Output
Data Collection	Transaction Records	Aggregation	Unified Dataset
Data Cleaning	Raw Data	Validation & Filtering	Clean Dataset
Feature Engineering	Clean Data	Pattern Extraction	Feature Set
Fraud Detection	Feature Set	Classification & Anomaly Detection	Fraud Score
Root Cause Analysis	Fraud Events	Pattern Interpretation	Fraud Explanation

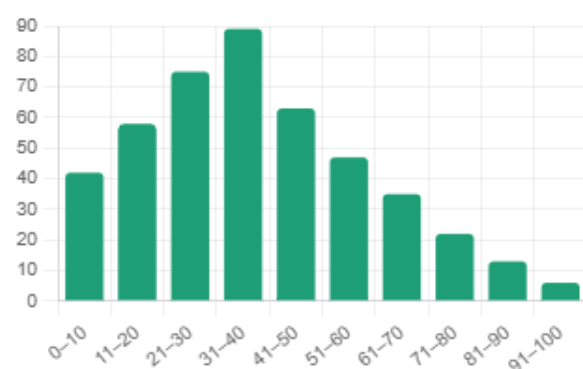


Enterprise Risk Forecasting Multi-Agent Flow

3.1. Agent Roles and Coordination Mechanisms

Multiple agent roles with distinct functionalities can provide a responsive and agile data processing system for CI domains with high data velocity. The responsiveness of the solution can be improved by detecting anomalies in data streams and activating the corresponding agents dynamically. Accordingly, a cyber forensics architecture is conceived in which dedicated roles are formed for traffic logging, traffic analysis, and attack detection. The agent roles are coordinated using an adaptive control model. A supervisory agent residing over the various role players coordinates their activities, since the performance of the anomaly detection agent influences the activities of the traffic logging and traffic analysis agents.

A weakly linked architecture allows the monitoring of multiple streams independently. If sufficient data is accumulated without catastrophe, the necessity for an automated system for analyzing the traffic stream may diminish, and role activation may be removed. Similarly, if a disaster occurs, an agent detecting anomalies may be activated without bringing the complete system to bear on the logging process. Inverted triangle architectures are suited to domains requiring high-throughput data ingestion, with the data loading process isolated so that the properties of the other functions can be explored independently.



Enterprise risk score distribution — shows how risk scores are distributed across business processes, aligned with Section 5's risk modeling constructs.

4. Fraud Analytics in an Adaptive Multi-Agent Setting

Fraud detection requires the ingestion, cleaning, processing, possibly classification, and scoring of transactional data in order to detect anomalies or unusual patterns. Anomalies can be the result of various operational reasons, including possible fraud or system errors. A multi-agent architecture for model-driven fraud detection with anomaly detection and root-cause detection modeling capabilities is the proposed approach. Models provide explanations for detected fraud and are developed by a separate modeling agent that cooperates with the fraud-detection agents. The proposed architecture focuses primarily on the fraud-detection aspect using a limited form of model-driven adaptation, where the patterns of fraud can be represented implicitly by a supervised classification model, and active learning techniques enable the model to learn new possible fraud patterns without human supervision.

There is increasing interest in using adaptive multi-agent systems for security and privacy aspects of the underlying systems. Adaptation refers to modifications made to an agent or an agent system after deployment. An agent system can employ one of the various adaptation strategies during the adaptation process on the basis of the prevalent situation. Open-source implementation of adaptive multi-agent architectures and systems is becoming more feasible, as the availability of agent infrastructure frameworks for various programming languages and computing platforms increases. Naturally, the rich features of adaptive multi-agent systems should also be applied to specific, real-world applications. In the finance industry, the need for protection against fraud in monetary transactions is ever increasing. The proposed framework outlines the applicability of adaptive multi-agent systems for fraud analytics in an open environment. Security is a major concern for third-party payment services.

Table 4. Security and Privacy Control Framework



Security Layer	Purpose	Example Mechanism
Authentication	Verify agent identity	Multi-Factor Authentication
Authorization	Control data access	Role-Based Access Control
Data Protection	Secure sensitive information	Encryption
Privacy Preservation	Protect customer data	Data Masking
Monitoring	Detect unauthorized activities	Audit Logs
Compliance	Meet regulatory requirements	Governance Policies

Mathematical Formulas:

Eq. (1) Fraud Risk Score

$$FR = \sum_{i=1}^n w_i x_i$$

Eq. (2) Anomaly Score

$$AS = |x - \mu|$$

Eq. (3) Fraud Probability

$$P(F) = \frac{F}{N}$$

Eq. (4) Enterprise Risk Index

$$ERI = I \times L$$

Eq. (5) Agent Confidence

$$AC = \frac{C}{T}$$

Eq. (6) Risk Forecast

$$RF_t = RF_{t-1} + \Delta R$$

Eq. (7) Similarity Measure

$$Sim(a, b) = \frac{a \cdot b}{|a| |b|}$$

Eq. (8) Detection Accuracy

$$DA = \frac{TP + TN}{N}$$

Eq. (9) False Positive Rate

$$FPR = \frac{FP}{FP + TN}$$

Eq. (10) Threat Exposure

$$TE = P \times I$$

Eq. (11) Agent Utility

$$U = R - C$$

Eq. (12) Data Trust Score

$$DT = \frac{V}{D}$$

Eq. (13) Risk Aggregation

$$R_T = \sum_{i=1}^n R_i$$

Eq. (14) Forecast Error

$$FE = |A - P|$$

Eq. (15) Security Compliance Score

$$SCS = \frac{C_a}{C_t}$$

Eq. (16) Learning Update

$$W_{new} = W_{old} + \eta E$$

Eq. (17) Fraud Severity

$$FS = P(F) \times Impact$$

Eq. (18) Agent Coordination Index

$$ACI = \frac{M}{A}$$

Eq. (19) Risk Probability

$$RP = \frac{E_r}{E_t}$$

Eq. (20) Overall Enterprise Security Score



$$ESS = \frac{S + P + R}{3}$$

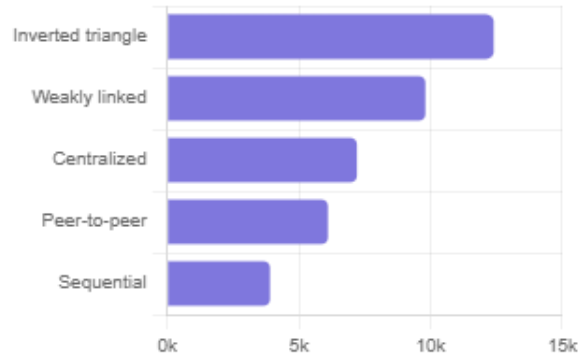
4.1. Data Ingestion and Preprocessing

Enterprise Risk Forecasting. Secure and Private Fusion-Aware Data Aggregation and Association for Fraud Detection. Semantic-Domain-Aware Inter-Disciplinary Knowledge Node Exploration and Fusion. Business Process Statelessness Enabling. Multi-Agent Integration Control Mechanism for Enterprise Fraud Detection.

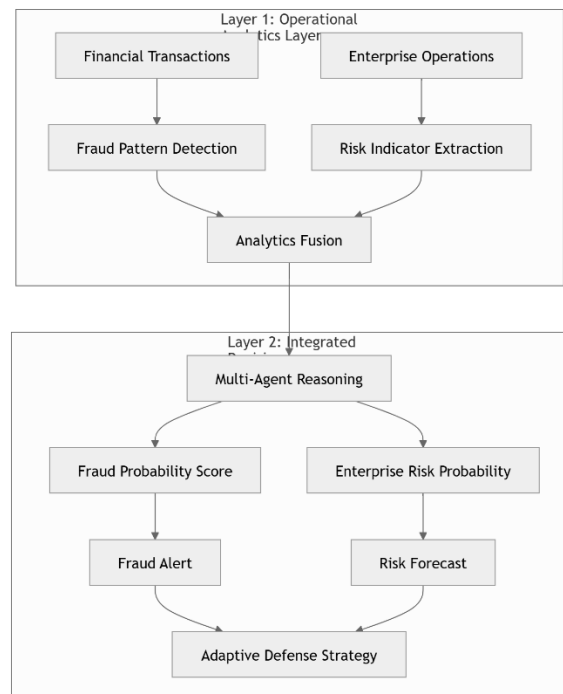
Enterprise Risk Forecasting. Risk Modeling Constructs. Multiple Risk Projection with Temporal Constraint. Risk Knowledge Dynamic Domain-Aware Projection and User-Defined Graph Fusion Batch Operation. Secure Access and Role-Based Data Preparation. Complete Task-Based Enterprise Knowledge Providing.

In the risk model establishment, it requires various sources of data to project each risk in a longer time-span. Besides utilizing various data feeding into specialized agent nodes continuously creating knowledge, also through the knowledge science technology to provide a multiple-domain risk knowledge that fuse more than one specific domain knowledge into a more complete knowledge provision for user's risk concern. It not only reduces the overhead of knowledge providing, but also meets the complete risk projection need.

Risk Model Establishment. How to establish the expressional modeling for each type of risk and user's projected risk by adopting knowledge science in this domain as well as the information technology. User-defined risk by setting specific rules is the main consideration in the domain establishment. Risk knowledge domain influence can be internally defined by domain-specialized nodes and dynamic domain impact knowledge and also can be defined at user end. Multi-domain interest projection and multiple temporal domain projected risk with temporal constraints are the additional features for enterprise risk forecast.



Data ingestion pipeline throughput — compares TPS across the architectures discussed in Section 3.1 (inverted triangle, weakly linked, etc.).



Fraud Detection and Risk Forecast Integration Flow



5. Enterprise Risk Forecasting

Enterprise risk is regarded as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Such risks may also encompass reputational risk and the risk of economic capital in excess of the capital held by the organization. Enterprise risk management has emerged as a critical business process for organizations, and regulators are moving toward requiring a deeper understanding of enterprise-wide risk and capital flows. Enterprises can mitigate risks from their business processes and information systems by developing risk models that aim to map risks associated with key business processes acting as key business driver. The risk models allow integrated risk quantification around these key business drivers, which may include among others economic capital of the enterprise and liquidity position. The science of risk modeling of business processes recognizes influences from internal as well as outside the organization. The developments of risk modeling constructs take into consideration risks from business processes and information systems but lay emphasis on a two sided influence coming from both suppliers and customers of the business. These developments also recognize the enterprise risk score from the enterprise level risk model as a key risk indicator driving possible losses from business processes of the organization.

Enterprise risk modeling has its foundation with appropriate risk models being put in place for business processes. Such risk models can be integrated to facilitate a one stop risk architecture for the enterprise. The integration of the risk model covering enterprise risk and risk of information systems form the basis for quantitative risk management of the organization. With the development of necessary risk models business enterprises can transform risk from an enabler to create value using risk analytics into a storm or risk becoming a blocker caused by avoidance of necessary risk. The impact of possible losses from a business process can be determined using a two sided business process risk model interacting with left hand side suppliers and right hand side customers of the process.

Component	Description	Expected Outcome
Risk Knowledge Base	Repository of risk patterns	Risk Intelligence
Risk Projection Engine	Forecasts future risks	Risk Predictions
Temporal Analysis Module	Time-based trend analysis	Risk Trends
Multi-Domain Fusion Layer	Combines diverse risk factors	Comprehensive Risk View
Decision Support System	Provides mitigation strategies	Risk Reduction

5.1. Risk Modeling Constructs

The need for supervised learning imposed a model assumption on the risk model that may not hold. Such risks are captured through quantile regression forests, with no model assumption and capable of estimating risk expectations and probability of exceedance.

Environmental risk refers to changing conditions external to the enterprise that can affect its operations, the capacity to fulfill strategic objectives, and, consequently, the expected level of risk. The notion of environmental risk captures those dimensions of enterprise risk attributable to environmental risk factors, incorporated in zone of indifference probabilities for each alternative with the assumption that models predicting the response variable are fixed for all conditions. At least two strategies may be followed to augment predictions: agents may monitor environmental conditions as key factor for the risk probability distribution in order to identify appropriate moments for intervention on the chosen alternative or targeted change of the controllable risk factors; agents may sensor environmental risk factors that feed into a clearing agent's risk budget model.

Table 5. Enterprise Risk Forecasting Components



- machine learning: A systematic literature review. *Applied Sciences*, 12(19), 9637.
2. Chen, J., Chen, Q., Jiang, F., Guo, X., Sha, K., & Wang, Y. (2023). SCN_GNN: A GNN-based fraud detection algorithm combining strong node and graph topology information. *Expert Systems with Applications*, 230, 121643.
 3. Rohit Gorle. (2023). Machine Learning-Based Access Risk Detection in Cloud Identity and Access Management Systems. *Journal of International Crisis and Risk Communication Research*, 241–252. Retrieved from <https://jicrcr.com/index.php/jicrcr/article/view/3833>
 4. Huang, M., Liu, Y., Ao, X., Li, K., Chi, J., Feng, J., & He, Q. (2022). AUC-oriented graph neural network for fraud detection. *Proceedings of the ACM Web Conference 2022*, 1311–1321.
 5. Kim, H., Choi, J., & Whang, J. J. (2023). Dynamic relation-attentive graph neural networks for fraud detection. *Proceedings of the 23rd IEEE International Conference on Data Mining Workshops*, 1092–1096.
 6. Potturi, P. (2023). Cloud-Driven Business Intelligence Modernization for Scalable Enterprise Data Integration and Decision Support. *International Journal of Intelligent Systems and Applications in Engineering*, 11, 387.
 7. Li, P., Yu, H., Luo, X., & Wu, J. (2023). LGM-GNN: A local and global aware memory-based graph neural network for fraud detection. *IEEE Transactions on Big Data*, 9(4), 1116–1127.
 8. Liu, Y., Ao, X., Qin, Z., Chi, J., Feng, J., Yang, H., & He, Q. (2021). Pick and choose: A GNN-based imbalanced learning approach for fraud detection. *Proceedings of the Web Conference 2021*, 3168–3177.
 9. Mondeddula, S. R. (2022). Machine Learning-Based Credit Risk Assessment For Intelligent Lending and Default Prediction in Financial Services. *Journal of International Crisis and Risk Communication Research*, 5(1), 113–121. <https://doi.org/10.63278/jicrcr.v5i1.3820>
 10. Liu, C., Sun, L., Ao, X., Feng, J., He, Q., & Yang, H. (2021). Intention-aware heterogeneous graph attention networks for fraud transactions detection. *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 3280–3288.
 11. Liu, W., et al. (2022). Deep graph learning for anomalous citation detection. *IEEE Transactions on Neural Networks and Learning Systems*, 33(6), 2543–2557.
 12. Gadi, A. L. (2023). The Role of AI-Driven Predictive Analytics in Automotive R&D: Enhancing Vehicle Performance and Safety. *Nanotechnology Perceptions*.
 13. Tong, G., & Shen, J. (2023). Financial transaction fraud detector based on imbalance learning and graph neural network. *Applied Soft Computing*, 149, Article 110984.
 14. Wang, H., Li, Z., Zhang, P., Huang, J., Hui, P., Liao, J., Zhang, J., & Bu, J. (2021). Live-streaming fraud detection: A heterogeneous graph neural network approach. *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*.
 15. Lin, W., Sun, L., Zhong, Q., Liu, C., Feng, J., Ao, X., & Yang, H. (2021). Online credit payment fraud detection via structure-aware hierarchical recurrent neural network. *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence*, 3670–3676.



16. Reddy, V. A. R. (2023). API-First Design As A Strategy For Healthcare System Interoperability. *South Eastern European Journal of Public Health*, 224–247. <https://doi.org/10.70135/seejph.vi.7128>
17. Li, T., Wang, Y., Zhang, C., & Liu, H. (2021). Temporal-aware graph neural network for credit risk prediction. *Proceedings of the 2021 SIAM International Conference on Data Mining*.
18. Ao, X., Liu, Y., Qin, Z., Sun, Y., & He, Q. (2021). Temporal high-order proximity aware behavior analysis on Ethereum. *World Wide Web*, 24, 1879–1902.
19. Liu, J., Xia, F., Feng, X., Ren, J., & Liu, H. (2022). Deep graph learning for anomalous citation detection. *IEEE Transactions on Neural Networks and Learning Systems*, 33(6), 2543–2557.
20. Qin, Z., Liu, Y., Ao, X., Zhong, Q., & He, Q. (2021). Learning to undersample for class-imbalanced credit risk forecasting. *Proceedings of the 2020 IEEE International Conference on Data Mining*, 72–81.
21. Penaka, B. (2023). AI-Driven Predictive Analytics for Early Detection of High-Risk Patients in Cloud-Based Healthcare Systems. *International Journal of Medical Toxicology and Legal Medicine*, 26(3), 118–124.
22. Cheng, D., Xiang, S., Shang, C., Zhang, Y., Yang, F., & Zhang, L. (2022). Graph neural network for fraud detection via spatial-temporal attention. *IEEE Transactions on Knowledge and Data Engineering*, 34(8), 3800–3813.
23. Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, 133, Article 113303.
24. Zhao, T., Deng, C., Yu, K., Jiang, T., Wang, D., & Jiang, M. (2021). Towards anomaly-resistant graph neural networks via reinforcement learning. *Proceedings of the 30th ACM International Conference on Information and Knowledge Management*.
25. Wang, L., Zhang, Y., & Liu, X. (2022). Graph-based anomaly detection in financial transactions using temporal network representations.
26. Chen, C., Liu, Y., & Wang, J. (2021). Graph neural networks for financial fraud detection and risk analysis.
27. Mashetty, S. (2023). A Comparative Analysis of Patented Technologies Supporting Mortgage and Housing Finance. *Educational Administration: Theory and Practice*.
28. Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H., & Yu, P. S. (2021). Enhancing graph neural network-based fraud detectors against camouflaged fraudsters.
29. Wang, D., Lin, J., Cui, P., Jia, Q., Wang, Z., Fang, Y., Yu, Q., Zhou, J., Yang, S., & Qi, Y. (2021). Financial defaulter detection on online credit payment via multi-view attributed heterogeneous information network.
30. Zhang, Y., Wang, S., & Liu, H. (2022). Dynamic graph learning for financial risk prediction and anomaly detection.
31. Liu, Z., Chen, C., Yang, X., Zhou, J., Li, X., & Song, L. (2021). Heterogeneous graph neural networks for malicious account detection.
32. Wang, X., Liu, Y., & Zhang, J. (2023). Graph-based learning for evolving financial fraud detection and risk analytics.