Journal of Technology, Culture & Sustainability

EISSN: 3105-5060 | PISSN: 3105-5052 | Vol. 2, No. 1 (2026)

Review

Application Paths of Semantic Modeling in Financial Fraud Detection and Risk Identification

Victor P. Gauthier [1,*] and Daniel S. Wu [2]

[1] School of Systems and Enterprises, Stevens Institute of Technology, Hoboken, NJ, USA
[2] Department of Computer Science, Old Dominion University, Norfolk, VA, USA
* Correspondence: Victor P. Gauthier, School of Systems and Enterprises, Stevens Institute of Technology, Hoboken, NJ, USA

Abstract: Financial fraud and risk pose significant threats to economic stability and individual well-being. Traditional detection methods often struggle to keep pace with increasingly sophisticated fraudulent schemes. Semantic modeling, which focuses on understanding the meaning and relationships within data, offers a promising avenue for enhancing fraud detection and risk identification. This review paper explores the application paths of semantic modeling in this domain. We begin with a historical overview of fraud detection techniques, highlighting the limitations of traditional approaches. Subsequently, we delve into core themes, including knowledge graph-based fraud detection and semantic rule-based inference for risk assessment. We then compare and contrast different semantic modeling approaches, addressing key challenges such as data heterogeneity and scalability. Furthermore, we discuss future perspectives, focusing on the integration of semantic modeling with emerging technologies like explainable AI and federated learning. The review synthesizes findings from various studies, providing a comprehensive understanding of the current state and future directions of semantic modeling in financial fraud detection and risk identification. This review aims to guide researchers and practitioners in leveraging semantic modeling to build more robust and effective fraud detection systems. We explore current limitations and highlight opportunities for future research in this rapidly evolving field, ensuring advancements in both prevention and detection methodologies can keep pace with ever-evolving and dynamic threats.

Keywords: Semantic Modeling, Financial Fraud Detection, Risk Identification, Knowledge Graph, Semantic Rules, Artificial Intelligence, Machine Learning

Received: 12 December 2025
Revised: 01 February 2026
Accepted: 16 February 2026
Published: 23 February 2026

1. Introduction

1.1. Problem Statement and Motivation

Financial fraud poses a significant threat to global economies, eroding investor confidence and destabilizing financial institutions. Traditional fraud detection methods, relying heavily on rule-based systems and statistical analysis of structured data, often struggle to identify sophisticated schemes [1]. These methods are limited in their ability to capture complex relationships and contextual information embedded within heterogeneous data sources. The increasing volume and velocity of financial transactions necessitate more advanced and adaptable approaches for effective fraud detection and risk identification. Semantic modeling offers a promising avenue to overcome these limitations by leveraging knowledge representation and reasoning capabilities [2].

1.2. Semantic Modeling as a Solution

Semantic modeling offers a promising avenue for enhancing financial fraud detection and risk identification. By representing financial data and relationships as a graph of interconnected entities and concepts, semantic models enable sophisticated reasoning and inference. This approach facilitates the identification of subtle patterns and anomalies that might be missed by traditional methods. The ability to incorporate domain knowledge and contextual information further strengthens the detection process. This review explores various applications of semantic modeling in finance, focusing on techniques like knowledge graphs and ontologies, and their impact on improving the accuracy and efficiency of fraud detection and risk assessment, considering factors such as $precision$ and $recall$.

1.3. Review Structure

This review is structured as follows. Section 2 introduces fundamental semantic modeling techniques. Section 3 explores applications in financial fraud detection, focusing on areas like transaction analysis and anomaly detection. Section 4 discusses risk identification using semantic models, considering aspects such as credit risk and market risk, where $Risk = f$(Semantic Model). Finally, Section 5 concludes with a summary and future research directions.

2. Historical Overview of Fraud Detection Techniques

2.1. Rule-Based Systems

Early fraud detection heavily relied on rule-based systems, employing expert-defined rules to identify suspicious transactions [3]. These systems operated by flagging instances that violated pre-defined thresholds or patterns [4]. For example, a rule might flag transactions exceeding a certain dollar amount, x, or those originating from specific geographic locations known for fraudulent activity. While simple to implement and interpret, rule-based systems suffered from significant limitations. They were inflexible, requiring constant manual updates to adapt to evolving fraud schemes. Furthermore, they often generated a high number of false positives, requiring extensive manual review and potentially missing sophisticated fraudulent activities that fell outside the defined rules [5]. The lack of adaptability and the inability to detect novel fraud patterns ultimately hindered their long-term effectiveness (Table 1).

Table 1. Evolution of Fraud Detection Techniques.

Technique	Description	Advantages	Limitations
Rule-Based Systems	Employs expert-defined rules to identify suspicious transactions based on pre-defined thresholds or patterns (e.g., transactions exceeding a certain dollar amount, x).	Simple to implement and interpret.	Inflexible; requires constant manual updates; high number of false positives; inability to detect novel fraud patterns; misses sophisticated fraud outside defined rules.

2.2. Statistical Methods

Statistical methods have historically played a crucial role in fraud detection. Regression analysis, for instance, can identify relationships between variables and flag anomalies [6]. A model might predict expected transaction amounts based on customer history; deviations exceeding a threshold, defined by parameters like standard deviation σ, could indicate fraudulent activity. Time series analysis is also valuable, particularly for detecting anomalies in sequential data. Techniques like ARIMA (Autoregressive Integrated Moving Average) model temporal dependencies and forecast future values. Unexpected spikes or drops in a time series, exceeding a defined range R, may signal fraudulent transactions or manipulated financial data. These methods offer a quantitative approach to identifying suspicious patterns [7].

2.3. Machine Learning Approaches

Machine learning has significantly impacted fraud detection, offering sophisticated methods to identify complex patterns indicative of fraudulent activities. Supervised learning algorithms, such as logistic regression, support vector machines (SVM), and decision trees, are widely used, trained on labeled datasets of fraudulent and legitimate transactions to predict the likelihood of fraud [8]. The performance of these models often depends on feature engineering and the quality of the labeled data. Unsupervised learning techniques, including clustering algorithms like k-means and anomaly detection methods, are employed to identify unusual behaviors without prior knowledge of fraudulent patterns. These methods are particularly useful when labeled data is scarce or when detecting novel fraud schemes. The choice of algorithm depends on the specific characteristics of the financial data and the nature of the fraud being investigated [9].

3. Knowledge Graph-Based Fraud Detection

3.1. Knowledge Graph Construction

Knowledge graph construction is the foundational step for knowledge graph-based fraud detection. This process involves extracting relevant entities and relationships from diverse financial data sources, including transaction records, customer profiles, news articles, and regulatory filings [10]. Entity extraction identifies key actors such as individuals, merchants, banks, and accounts. Techniques like Named Entity Recognition (NER) and rule-based systems are commonly employed for this purpose. NER models, often trained on financial corpora, can automatically identify and classify entities. Rule-based systems, on the other hand, rely on predefined patterns and dictionaries to extract entities based on specific keywords or formats [11].

Relationship identification focuses on uncovering the connections between these entities. This can be achieved through techniques like relation extraction, co-occurrence analysis, and rule-based reasoning [12]. Relation extraction models, similar to NER, are trained to identify and classify relationships based on contextual information. Co-occurrence analysis identifies relationships based on the frequency with which entities appear together in the same document or transaction [13]. For instance, if account A frequently transfers money to account B, a “transaction” relationship can be inferred. The extracted entities and relationships are then used to populate the knowledge graph, forming the basis for subsequent fraud detection analysis (Table 2).

Table 2. Knowledge Graph Components.

Component	Description	Techniques
Entities	Key actors involved in financial activities (e.g., individuals, merchants, banks, accounts).	Named Entity Recognition (NER), Rule-based systems
Relationships	Connections between entities, illustrating interactions and dependencies (e.g., transaction, ownership, association).	Relation extraction, Co-occurrence analysis, Rule-based reasoning

3.2. Graph-Based Feature Engineering

Graph-based feature engineering leverages the structural information encoded within knowledge graphs to create informative features for fraud detection models. These features capture the relationships and characteristics of entities (nodes) and their connections (edges), providing valuable insights beyond traditional attribute-based features [14].

One common approach involves calculating node centrality measures. Centrality metrics quantify the importance of a node within the graph. Examples include degree centrality, which measures the number of connections a node has; betweenness centrality, which identifies nodes that lie on many shortest paths between other nodes; and eigenvector centrality, which assigns scores to nodes based on the centrality of their neighbors. Higher centrality scores for a suspicious account, for instance, might indicate its involvement in a larger fraudulent network [15].

Another powerful technique is extracting path-based features. These features analyze the paths connecting different entities in the graph [16]. Simple path counts, representing the number of paths between two nodes satisfying certain criteria, can be used. More sophisticated approaches involve extracting meta-paths, which are predefined sequences of node and edge types representing specific relationships. For example, a meta-path like "Account - TransfersTo - Account - Reports - FraudulentAccount" could indicate a suspicious transfer pattern. Path ranking algorithms can further refine these features by assigning scores to paths based on their relevance to fraud. The length of a path, denoted as l, can also be a useful feature, with shorter paths often indicating stronger relationships. These extracted features, combined with node attributes, significantly enhance the performance of fraud detection models.

3.3. Fraud Detection Algorithms on Knowledge Graphs

Fraud detection on knowledge graphs leverages the relational structure to identify anomalous patterns indicative of fraudulent activities. Graph Neural Networks (GNNs) have emerged as powerful tools, enabling node classification based on aggregated information from their neighbors. For instance, algorithms like Graph Convolutional Networks (GCNs) learn node embeddings by iteratively aggregating feature information from neighboring nodes, effectively capturing complex relationships. The embedding of node i, denoted as h_i, is updated based on the embeddings of its neighbors $N(i)$.

Community detection methods also play a crucial role. Fraudulent actors often form tightly knit communities to coordinate their activities. Algorithms like the Louvain method or label propagation can identify these suspicious clusters within the knowledge graph. Anomalous subgraphs, characterized by unusual connectivity patterns or attribute distributions, can be flagged as potential fraud indicators. Furthermore, path-based approaches analyze the relationships between entities, identifying suspicious paths that deviate from normal transaction patterns. The length of a path between two nodes u and v can be represented as $L(u,v)$. These algorithms exploit the inherent interconnectedness of knowledge graphs to enhance fraud detection accuracy.

4. Semantic Rule-Based Inference for Risk Assessment

4.1. Semantic Rule Definition and Representation

Semantic rule definition is crucial for translating domain expertise into machine-understandable logic for risk assessment. These rules capture relationships between financial entities, transactions, and contextual factors, enabling the system to infer potential risks. A semantic rule typically consists of an antecedent (IF part) and a consequent (THEN part), representing conditions and their corresponding risk implications.

Several rule languages and formalisms can be employed. Production rules, often expressed in languages like Jess or Drools, offer a straightforward way to represent IF-THEN logic. For instance: IF $transaction.amount > threshold$ AND $customer.creditScore < minScore$ THEN $flagAsHighRisk = true$. Semantic Web Rule Language (SWRL) provides a more expressive formalism, allowing integration with ontologies and leveraging semantic relationships. SWRL rules can reason over individuals, classes, and properties defined in ontologies, enabling more sophisticated risk assessments. For example, Customer(?c) ^ hasTransaction(?c, ?t) ^ Transaction(?t) ^

hasAmount(?t, ?a) ^ swrlb:greaterThan(?a, 10000) -> HighRiskCustomer(?c). First-order logic provides an even more general framework, but its complexity can make rule definition and reasoning more challenging. The choice of formalism depends on the complexity of the risk assessment task and the desired level of expressiveness (Table 3).

Table 3. Example Semantic Rules for Fraud Detection.

Rule Type	Example Rule	Description
Production Rule (Jess/Drools)	IF $transaction.amount > 5000$ AND $customer.location != transaction.location$ THEN $flagAsSuspicious = true$	Flags transactions exceeding $5000 where the customer's location differs from the transaction location.
SWRL Rule	Customer(?c) ^ hasTransaction(?c, ?t) ^ Transaction(?t) ^ hasAmount(?t, ?a) ^ swrlb:greaterThan(?a, 10000) ^ hasCurrency(?t, "USD") -> HighRiskCustomer(?c)	Identifies customers as high risk if they have a transaction with an amount greater than $10,000 USD. Uses ontology elements like Customer, hasTransaction, Transaction, hasAmount, and hasCurrency.
Production Rule (Simple)	IF $transaction.type == "wire_transfer"$ AND $new_beneficiary == true$ THEN $flagForReview = true$	Flags wire transfer transactions to new, previously unseen beneficiaries for manual review.
SWRL Rule	Account(?a) ^ hasTransaction(?a, ?t) ^ Transaction(?t) ^ swrlb:date(?d, ?t)^ swrlb:month(?m, ?d)^ swrlb:day(?dy, ?d)^ swrlb:hour(?h, ?d) ^ swrlb:greaterThan(?h, 22) ^ swrlb:lessThan(?h, 6) -> FlagForNightTransaction(?t)	Flags a transaction ?t for review, occurring between 10 PM and 6 AM based on the temporal properties
First-Order Logic (Simplified)	$\forall t\ (\text{Transaction}(t) \wedge \text{Amount}(t, a) \wedge a > 100000 \wedge \text{InvolvedIn}(c, t) \wedge \text{Customer}(c) \wedge \text{Country}(c, x) \wedge \text{Country}(t, y) \wedge x \neq y) \Rightarrow \text{FlagHighRisk}(t)$	For all transactions, if the amount exceeds $100,000, a customer is involved, and the customer's country differs from the transaction's country, flag the transaction as high risk.

4.2. Inference Engines and Reasoning Techniques

Inference engines form the core of semantic rule-based systems, driving the reasoning process to derive new knowledge and assess risk. These engines apply predefined semantic rules to financial data represented in a knowledge graph or similar semantic model. Several reasoning techniques are employed, including forward chaining (data-driven) and backward chaining (goal-driven) inference. Forward chaining starts with known facts and applies rules to infer new facts until a desired conclusion or risk score is reached. Backward chaining, conversely, begins with a hypothesis about potential fraud or risk and attempts to find supporting evidence by tracing back through the rules and data.

Production rule systems, often implemented using the Rete algorithm, are commonly used for their efficiency in handling large rule sets and frequent data updates. These systems excel at identifying patterns and anomalies indicative of fraudulent activities. Description Logic (DL) reasoners, such as Pellet or HermiT, provide more expressive reasoning capabilities, enabling complex inferences based on ontologies and semantic relationships. These are particularly useful for identifying subtle connections between seemingly disparate entities that might indicate collusion or sophisticated fraud schemes. The choice of inference engine and reasoning technique depends on the complexity of the rules, the size of the dataset, and the desired level of accuracy and explainability. The risk score, S, can be calculated based on the inferred facts and the weights assigned to each rule, w_i, such that $S = \sum_{i=1}^{n} w_i * f_i$, where f_i represents the inferred facts.

4.3. Applications in Anti-Money Laundering (AML) and Compliance

Semantic rule-based inference offers a powerful approach to enhance Anti-Money Laundering (AML) and compliance efforts by codifying regulatory requirements and suspicious activity patterns into machine-readable rules. These rules, expressed using semantic technologies like ontologies and rule languages (e.g., SWRL), enable automated reasoning over transactional data to identify potential money laundering activities. For instance, a rule might state: "IF TransactionAmount > Threshold AND TransactionType = 'InternationalWireTransfer' AND SenderCountry = 'HighRiskCountry' THEN FlagAsSuspicious".

This approach allows for the detection of complex money laundering schemes that might be missed by traditional threshold-based systems. Semantic reasoning can connect seemingly disparate transactions based on shared entities, relationships, or contextual information, revealing hidden patterns of illicit activity. Furthermore, the transparency of rule-based systems facilitates auditability and explainability, crucial for regulatory compliance. The ability to easily modify and update rules in response to evolving regulations and emerging typologies provides a significant advantage over static, hard-coded systems. By leveraging semantic technologies, financial institutions can improve the effectiveness and efficiency of their AML programs, reducing the risk of financial crime and ensuring regulatory adherence (Table 4).

Table 4. Comparative Analysis of Rule-Based Systems in AML.

Feature	Traditional Threshold-Based Systems	Semantic Rule-Based Systems
Rule Representation	Simple thresholds (e.g., Amount > x)	Complex rules using ontologies and rule languages (e.g., SWRL) reflecting regulatory requirements and suspicious activity patterns. Includes semantic relationships.
Pattern Detection	Limited to predefined single-transaction thresholds. Difficulty in detecting complex or hidden patterns.	Capable of detecting complex, multi-transaction money laundering schemes by connecting disparate transactions based on shared entities, relationships, and contextual information.
Scalability	May struggle to scale effectively with increasing data volume and complexity without significant performance degradation.	Designed to potentially scale well with efficient reasoning algorithms and data structures using optimized database performance.
Adaptability	Difficult and time-consuming to update rules in response to new regulations or typologies. Requires code changes which are slow and costly.	Rules can be easily modified and updated in response to evolving regulations and emerging typologies through ontology and rule language updates. Quick to adapt.

Feature	Traditional Threshold-Based Systems	Semantic Rule-Based Systems
Explainability & Auditability	Limited explainability; often a "black box" lacking transparency.	High transparency and auditability due to clearly defined and documented rules (easy to debug). Facilitates compliance efforts.
Effectiveness	Lower effectiveness in detecting sophisticated money laundering techniques. Prone to both false positives and false negatives.	Higher effectiveness in identifying complex schemes and potentially reducing false positives and negatives through contextual understanding.
Contextual Awareness	Limited ability to incorporate contextual information.	Strong integration of contextual awareness through semantic technologies and knowledge representation.

5. Comparison of Semantic Modeling Approaches and Challenges

5.1. Comparison of Knowledge Graph and Semantic Rule Approaches

Knowledge graph and semantic rule approaches offer distinct advantages in fraud detection. Knowledge graphs excel at capturing complex relationships between entities (e.g., individuals, accounts, transactions) and uncovering hidden connections indicative of fraudulent activity. Their strength lies in handling large, heterogeneous datasets and enabling reasoning across multiple hops. However, constructing and maintaining knowledge graphs can be resource-intensive. Semantic rules, conversely, provide explicit, interpretable logic for identifying fraud patterns. They are effective when fraud schemes are well-defined and readily expressible as rules. A weakness is their inflexibility in adapting to novel or evolving fraud tactics. The choice depends on the specific scenario: knowledge graphs are better suited for exploratory analysis and detecting sophisticated, interconnected fraud, while semantic rules are appropriate for enforcing compliance and identifying known fraud patterns [17].

5.2. Challenges in Data Heterogeneity and Integration

Data heterogeneity presents a significant hurdle in applying semantic modeling to financial fraud detection. Financial institutions amass data from diverse sources, including transaction records, customer profiles, news articles, and social media feeds. These sources exhibit variations in data formats, semantics, and quality. Integrating such disparate data into a unified semantic model requires substantial effort in data cleaning, transformation, and reconciliation. Furthermore, mapping different data elements to a common ontology can be complex, especially when dealing with ambiguous or context-dependent financial terms. The sheer volume and velocity (v) of data, compounded by its variety (v), exacerbate these integration challenges, demanding scalable and efficient semantic modeling techniques.

5.3. Scalability and Performance Issues

Semantic modeling faces significant scalability challenges when applied to massive financial datasets. The computational complexity of reasoning and inference over large knowledge graphs, often $O(n^3)$ or higher where n represents the number of entities and relationships, can lead to unacceptable processing times. Materialization of inferred knowledge further exacerbates storage requirements. Performance bottlenecks arise from query execution against these large graphs, requiring optimized indexing strategies and distributed processing frameworks to achieve acceptable latency for real-time fraud detection. Efficient management of evolving data and schema changes is also crucial for maintaining performance over time.

6. Future Perspectives

6.1. Integration with Explainable AI (XAI)

The integration of semantic modeling with Explainable AI (XAI) holds significant promise for enhancing the transparency and interpretability of financial fraud detection systems. Semantic models, by capturing the underlying meaning and relationships within financial data, can provide valuable context for XAI techniques. This allows for a deeper understanding of why a particular transaction or entity is flagged as potentially fraudulent. For instance, semantic relationships can highlight unusual connections between seemingly unrelated accounts, providing XAI algorithms with crucial features. Furthermore, XAI methods can then elucidate how these semantically-enriched features contribute to the model's final decision, offering insights into the model's reasoning process. This synergy between semantic modeling and XAI can lead to more trustworthy and reliable fraud detection models, fostering greater confidence among stakeholders and facilitating effective risk mitigation strategies. The use of metrics like $interpretability$, $transparency$, and $confidence$ can be used to quantify the benefits.

6.2. Federated Learning for Privacy-Preserving Fraud Detection

Federated learning (FL) presents a promising avenue for privacy-preserving fraud detection using semantic modeling. By enabling collaborative model training without direct data sharing, FL addresses the critical concern of data privacy across financial institutions. Each institution trains a local semantic model on its private data, sharing only model updates (e.g., gradients, weights) with a central server. These updates are aggregated to create a global model, which is then redistributed to the institutions. This iterative process allows for the development of a robust fraud detection system that leverages the collective knowledge of multiple institutions while safeguarding sensitive customer data. The privacy gain can be further enhanced by employing techniques like differential privacy, adding noise to the model updates before sharing, controlled by a privacy parameter ϵ.

7. Conclusion

This review highlights semantic modeling's significant potential in financial fraud detection and risk identification. Key findings reveal its effectiveness in uncovering complex relationships and patterns often missed by traditional methods. Semantic approaches, leveraging knowledge graphs and ontologies, enhance the accuracy and interpretability of fraud detection systems. Furthermore, the ability to integrate diverse data sources and reason about risk factors makes semantic modeling a promising avenue for future research and practical applications in finance.

Semantic modeling offers promising avenues for financial fraud detection and risk identification. Future research should explore advanced techniques like graph neural networks and knowledge graph embedding to enhance model accuracy and scalability, particularly with high-dimensional financial data where $n > p$.

References

1. C. Wu, J. Chen, Z. Wang, R. Liang, and R. Du, "Semantic sleuth: Identifying ponzi contracts via large language models," in *Proc. 39th IEEE/ACM Int. Conf. Automated Software Engineering*, 2024, pp. 582-593.
2. C. L. Cheong, "Research on AI Security Strategies and Practical Approaches for Risk Management", Journal of Computer, Signal, and System Research, vol. 2, no. 7, pp. 98–115, Dec. 2025, doi: 10.71222/17gqja14.
3. J. Gong, Y. Wang, W. Xu, and Y. Zhang, "A deep fusion framework for financial fraud detection and early warning based on large language models," *J. Computer Science and Software Applications*, vol. 4, no. 8, pp. 19-29, 2024.
4. M. An, Y. Gao, J. Li, X. Wang, and X. He, "FRAUDLLM: Zero-Shot Fraud Detection with Large Language Models," in *China Conference on Information Retrieval*, Singapore: Springer Nature Singapore, 2025, pp. 76-89.
5. S. Yuan, "Conceptual Modeling and Semantic Relations in the Construction of Financial Knowledge Graphs", Econ. Manag. Innov., vol. 3, no. 1, pp. 64–70, Feb. 2026, doi: 10.71222/evj1tt66.

6. S. Goel and O. Uzuner, "Do sentiments matter in fraud detection? Estimating semantic orientation of annual reports," *Intelligent Systems in Accounting, Finance and Management*, vol. 23, no. 3, pp. 215-239, 2016.
7. J. L. Zhao, "Graph-based deep dive on AI startup revenue composition and venture capital network effect," Economics and Management Innovation, vol. 3, no. 1, pp. 27–36, 2026
8. W. Liu, Z. Wang, and X. Zhang, "Research on financial fraud detection by integrating latent semantic features of annual report text with accounting indicators," *J. Accounting & Organizational Change*, vol. 21, no. 5, pp. 841-866, 2025.
9. C. Song, M. Liu, C. Dong, L. Zhang, and C. Fang, "Leveraging Large Language Models in Financial Statement Fraud Detection of Listed Companies," in *2025 Thirteenth Int. Conf. Advanced Cloud and Big Data (CBD)*, 2025, pp. 389-394.
10. S. Bhatt and G. Garg, "NLP for Fraud Detection and Security in Financial Documents," in *Transformative Natural Language Processing: Bridging Ambiguity in Healthcare, Legal, and Financial Applications*, Cham: Springer Nature Switzerland, 2025, pp. 131-155.
11. Y. Yu, Z. Wu, Y. Han, Y. Ding, and W. Wei, "Improving Financial Statement Fraud Detection: A Large Language Model Processing Approach," *ACM Transactions on Internet Technology*.
12. J. Wang, "A Literature Review of Enterprise Strategic Management in the Context of Digital Transformation", Economics and Management Innovation, vol. 3, no. 1, pp. 71–78, Feb. 2026, doi: 10.71222/5wmnnj82.
13. C. Wei and X. Qian, "Bridging the Semantic Gap: An Ensemble Learning Framework With Textual Topic-Raw Financial Feature Fusion to Enhance Fraud Detection in Chinese Markets," *J. of Mathematics*, vol. 2025, no. 1, 6643152, 2025.
14. Z. Erva Ergun and E. Sefer, "Financial Statement Fraud Detection via Large Language Models," *Intelligent Systems in Accounting, Finance and Management*, vol. 32, no. 4, e70021, 2025.
15. S. Yuan, "Mechanisms of High-Frequency Financial Data on Market Microstructure," Modern Economics & Management Forum, vol. 6, no. 4, pp. 569–572, 2025.
16. N. Neha and V. Prabhu, "Language Models in Financial Fraud Detection: A Comparative Study," in *Int. Conf. on Artificial Intelligence on Textile and Apparel*, Singapore: Springer Nature Singapore, 2024, pp. 45-60.
17. C. L. Cheong, "Study on Risk Assessment Methods and Multi-Dimensional Control Mechanisms in AI Systems", European Journal of AI, Computing & Informatics, vol. 2, no. 1, pp. 31–46, Jan. 2026, doi: 10.71222/58dr7v22.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the publisher and/or the editor(s). The publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.