Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Network Analytics for Identifying Fraud Rings and Systemic Risk

Ujjwala Priya Modepalli
Independent Researcher

ARTICLE INFO

Received: 22 July 2025

Revised: 10 Aug 2025

Accepted: 22 Aug 2025

ABSTRACT

Global financial institutions encounter increasing difficulties due to complex fraud strategies executed by organized crime groups, requiring enhanced analytical solutions that exceed conventional rule-based detection methods. Network analytics signifies a transformative change in fraud detection, utilizing graph theory and complex network evaluation to reveal concealed patterns of criminal cooperation. The comprehensive framework encompasses network construction and data integration, community detection algorithms for fraud ring identification, centrality measures for key player evaluation, anomaly detection techniques for pattern recognition, and operational implementation strategies for risk management integration. Graph-based anomaly detection demonstrates superior performance in identifying fraudulent networks, with supervised methods achieving high accuracy rates while ensemble techniques reduce false-positive rates significantly. Community detection algorithms, particularly the Louvain algorithm, enable efficient identification of densely connected criminal groups through modularity optimization. Centrality measures, including degree, betweenness, and eigenvector centrality, facilitate the identification of critical infrastructure elements within fraud networks. Multi-modal anomaly detection combines network structural evaluation with behavioral assessment, creating comprehensive fraud detection systems that consider relationship patterns and financial activities. Temporal dynamics reveal changing structures of fraud rings over time, exposing recruitment trends, operational stages, and triggers for dissolution. Sophisticated machine learning algorithms developed from past fraud patterns consistently adjust to changing techniques while remaining responsive to new criminal methods. Operational implementation requires careful integration with existing risk management infrastructure through real-time processing architectures and interactive visualization tools. This paper contributes an operational, end-to-end framework that unifies multi-layer graph construction, temporal community detection, centrality-guided investigation, and deployment practices. This provides evaluation guidance and governance controls to reduce false positives while scaling million-node graphs. Unlike prior work that treats these components separately, we unify them into a deployable pipeline integrated with risk operations.

Keywords: network analytics, fraud detection, community detection, centrality measures, anomaly detection, risk management.

1. Introduction

The detection of complex fraudulent actions, particularly those carried out by coordinated criminal organizations, is becoming increasingly challenging for global financial institutions. Even while they have been successful in identifying single fraudulent transactions, traditional rule-based detection techniques usually have trouble identifying intricate behavioral patterns that are typical of organized crime groups. The systematic review of graph-based anomaly detection approaches reveals substantial limitations in traditional fraud detection methodologies when confronting network-based criminal activities [1]. The proliferation of fraud rings - systematically organized groups of individuals collaborating to perpetrate financial crimes - has driven the necessity for more sophisticated analytical methodologies. Network analytics constitutes a fundamental transformation in fraud detection approaches, transcending transaction-level examination to investigate the complex interconnections

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

between various entities. Through the construction and analysis of graphs wherein nodes symbolize individuals, accounts, devices, or additional entities, and edges denote relationships or interactions, analysts can reveal concealed patterns of coordinated behavior that would otherwise remain undetectable. Graph-based anomaly detection techniques demonstrate superior performance in identifying fraudulent networks compared to traditional approaches, with comprehensive literature analysis indicating enhanced detection capabilities across diverse fraud scenarios [1]. The methodology enables the identification of previously invisible collaborative criminal behaviors through systematic relationship mapping. The use of network analysis and graph theory in fraud detection has grown significantly in recent years, thanks to advancements in computing and the availability of large transactional datasets. These days, financial organizations have extensive databases of linked data that include device fingerprints, transaction history, customer relationships, and behavioral trends. These datasets reveal complex fraud patterns that are impossible to detect using traditional detection techniques when analyzed using network-based analytical frameworks. Machine learning algorithms applied to credit card fraud detection demonstrate significant improvements in accuracy and efficiency, with ensemble methods achieving superior performance compared to individual algorithmic approaches [2]. The integration of multiple detection techniques enhances overall system effectiveness while reducing false positive rates. Contemporary fraud networks utilize more intricate methods, such as synthetic identity fraud, identity theft, account hacking, and coordinated transaction alteration. To conceal individual participation and optimize fraudulent benefits, these operations usually make use of intricate relationship networks and a large number of actors spread over multiple geographic regions. Credit card fraud detection research indicates that ensemble machine learning approaches, including Random Forest and Gradient Boosting algorithms, achieve accuracy rates exceeding 99% in identifying fraudulent transactions [2]. The interconnected characteristics of these criminal enterprises render network analytics exceptionally appropriate for detection and prevention initiatives. No unified, deployable framework ties multi-layer graphs, temporal communities, centrality triage, and anomaly scoring with evaluation/governance for imbalanced fraud. Contributions include: **Unified pipeline:** entity resolution + multi-layer graphing → temporal communities → centrality triage → anomaly scoring → case routing, **Temporal/ops focus:** emphasizes dynamic rings and real-time risk integration, not just static graphs, **Evaluation blueprint:** recommends time-split validation, PR-AUC, F1 at cost-tuned thresholds for imbalanced fraud, and **Governance & scale:** PII handling, auditability, drift monitors, and million-node scalability considerations.

2. Network Construction and Data Integration

The establishment of robust fraud detection through network analytics necessitates the systematic construction of comprehensive network representations. Financial institutions must consolidate diverse data sources to develop meaningful graph structures that encompass the complete spectrum of entity relationships and interactions. Customer profiles, transaction records, device identifiers, IP addresses, phone numbers, and geographic locations constitute primary components for network construction. Comprehensive fraud detection system surveys demonstrate that effective network construction requires sophisticated integration methodologies to consolidate heterogeneous data sources, with particular emphasis on maintaining data consistency and temporal accuracy across multiple institutional systems [3]. Entity resolution constitutes a fundamental preprocessing requirement, demanding sophisticated algorithms to identify and consolidate duplicate records across disparate systems and data repositories. Advanced machine learning methodologies, encompassing probabilistic record linkage and graph-based clustering algorithms, facilitate the consolidation of fragmented identity information into coherent entity profiles. The effectiveness of entity resolution directly influences subsequent network analysis performance, establishing robust identity matching algorithms as essential components for fraud detection success. Fraud detection system analysis reveals that inadequate entity resolution can result in fragmented network representations, leading to reduced detection accuracy and increased false negative rates across various fraud categories [3]. Edge weight

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

calculation constitutes another essential element of network construction, necessitating careful evaluation of relationship strength and interaction frequency. Transactional relationships between accounts, shared device usage patterns, simultaneous login activities, and geographic proximity contribute to edge weight calculations. Time-based relationship decay models ensure appropriate weighting of historical connections relative to recent interactions, preventing obsolete relationships from distorting contemporary fraud assessments. Comparative studies in credit card fraud detection demonstrate that temporal weighting mechanisms significantly enhance detection performance, with time-sensitive algorithms achieving superior results compared to static approaches across multiple evaluation metrics [4]. Avoid label leakage by excluding post-flag edges/events and by freezing features at event time for validation. Multi-layer network architectures deliver enhanced analytical capabilities through the representation of different relationship types within separate but interconnected graph layers. Payment networks, communication patterns, device sharing relationships, and geographic proximity can each be modeled as distinct layers within comprehensive multi-dimensional network structures. Cross-layer analysis exposes complex fraud patterns spanning multiple relationship types, enabling more precise detection of sophisticated criminal schemes. Data mining research for credit card fraud reveals that multi-dimensional analytical approaches demonstrate superior performance compared to single-layer methodologies, particularly when analyzing complex fraud patterns involving multiple transaction types and behavioral indicators [4]. The effectiveness of network analytics is greatly influenced by the quality and completeness of data, requiring robust data governance frameworks and continuous monitoring processes. Insufficient transaction documentation, erroneous entity identities, and absent relationship information can create analytical gaps in network analysis, allowing fraudulent activities to remain undetected. The integrity of network representations used for fraud detection is ensured by thorough data validation processes and automated quality assessment tools. Evaluations of fraud detection systems highlight the vital significance of data preprocessing and quality control, and thorough surveys show that poor data quality is one of the main obstacles to putting in place efficient fraud detection systems in a variety of financial sectors [3]. Methodologies for building networks must take into account how financial linkages and transaction patterns change over time. Complex algorithms that can track relationship changes over time while preserving historical context for analytical reasons are necessary for temporal network evolution. There are many technological difficulties in integrating historical network representations with real-time data streams, especially when it comes to memory management and computational performance. Comparative analysis of data mining approaches for credit card fraud detection reveals that dynamic network updating mechanisms significantly improve detection performance, especially for emerging fraud patterns that evolve rapidly over short periods [4].

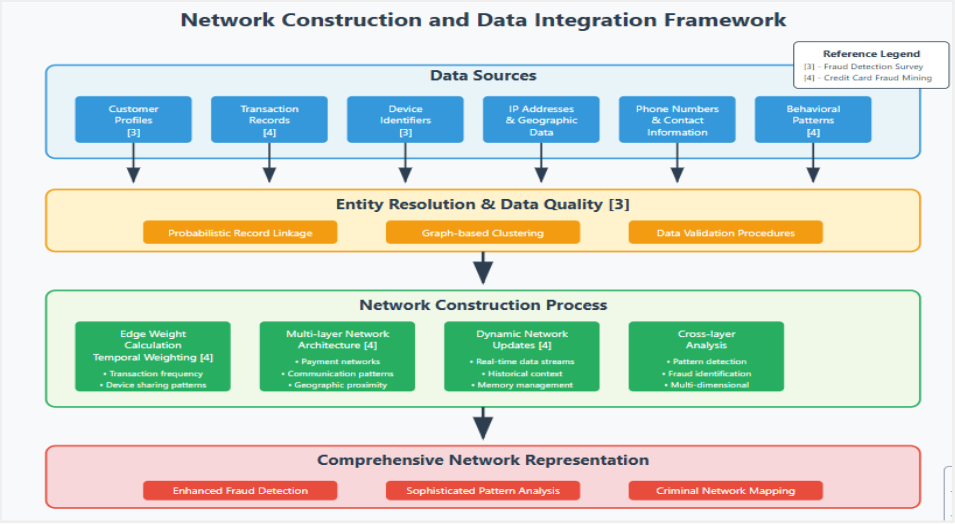

Figure 1: Network Construction and Data Integration Framework [3,4]

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. Community Detection and Fraud Ring Identification

Community detection algorithms constitute the fundamental framework for fraud ring identification, utilizing advanced mathematical methodologies to locate clusters of densely interconnected entities within extensive network structures. The Louvain algorithm, recognized for computational efficiency and superior community detection performance, has demonstrated exceptional effectiveness in financial fraud applications. Through network modularity optimization, the algorithm locates groups of entities characterized by robust internal connections and minimal external linkages, features typically associated with organized fraud rings. The fast-unfolding approach enables processing of large-scale networks with millions of nodes while maintaining computational efficiency, making the methodology particularly suitable for real-world financial network analysis [5]. Contemporary community detection methodologies integrate temporal dynamics to capture evolving fraud ring structures across time periods. Dynamic community detection algorithms monitor the formation, development, and dissolution of fraudulent groups, delivering insights into criminal network lifecycles. These temporal analyses expose recruitment patterns, operational phases, and dissolution triggers that guide both preventive measures and investigative strategies. The Louvain algorithm's hierarchical nature allows for analysis of community evolution at multiple resolution levels, revealing how fraud rings adapt and reorganize over time to avoid detection [5]. Multi-resolution community detection methodologies facilitate the identification of fraud rings operating at various scales within identical network structures. Hierarchical clustering algorithms expose nested community structures, where large-scale fraud operations may encompass multiple smaller subgroups with specialized functions. Understanding these hierarchical relationships assists investigators in mapping criminal organization structures and identifying key participants with distinct operational responsibilities. Community detection user guides emphasize that different resolution parameters reveal different organizational levels, with fine-grained analysis exposing individual fraud cells while coarse-grained analysis reveals broader criminal networks [6]. The combination of unsupervised and supervised learning methodologies enhances community detection accuracy through the incorporation of domain knowledge and historical fraud patterns. Semi-supervised community detection algorithms utilize labeled fraud cases to guide the identification of similar patterns in unlabeled data, improving detection rates while reducing false positives. Machine learning models trained on community characteristics develop capabilities to distinguish between legitimate business relationships and fraudulent criminal networks. Community detection methodologies demonstrate particular effectiveness when combined with prior knowledge about network structure and expected community characteristics [6]. Validation of detected communities necessitates sophisticated evaluation metrics that assess both the statistical significance of identified clusters and the practical relevance for fraud investigation. Metrics such as modularity, conductance, and silhouette scores provide quantitative assessments of community quality, while domain-specific validation approaches examine business logic and behavioral consistency of identified groups. The modularity measure, fundamental to the Louvain algorithm, quantifies the density of links inside communities compared to links between communities, The modularity scores how much a partition concentrates edges within groups rather than across them, with higher values indicating stronger community structure [5]. Comprehensive community detection validation requires multiple evaluation criteria to ensure that detected communities represent meaningful fraud ring structures rather than statistical artifacts in network data [6].

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

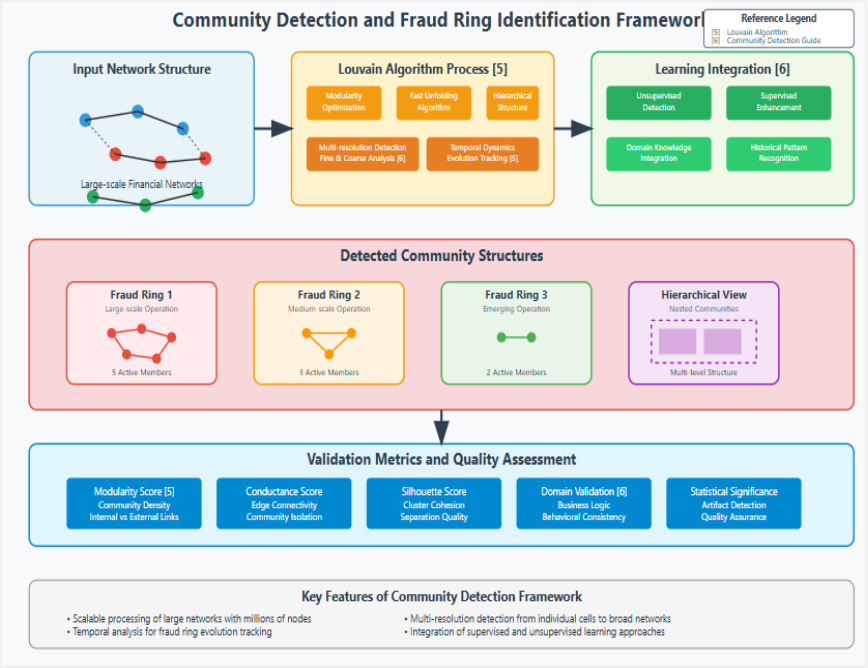

Figure 2: Community Detection and Fraud Ring Identification [5,6]

4. Centrality Measures and Key Player Analysis

Centrality measures constitute essential analytical instruments for identifying key players within fraud networks, facilitating the investigator's focus on the most influential and dangerous participants. Degree centrality identifies entities possessing the highest number of direct connections, frequently exposing coordination hubs or money mules with extensive transaction networks. High-degree nodes commonly represent critical infrastructure elements within fraud rings, whose elimination can substantially disrupt criminal operations. Social network analysis research demonstrates that degree centrality effectively quantifies node importance through direct connectivity measures, with high-degree nodes serving as primary information exchange points within network structures [7]. Betweenness centrality exposes entities functioning as bridges between different network segments, identifying individuals who may coordinate activities between separate fraud groups or facilitate information flow across criminal networks. These bridge entities often possess strategic importance beyond direct involvement in fraudulent activities, serving as key intelligence sources and operational coordinators. Centrality analysis studies reveal that betweenness centrality measures the extent to which nodes lie on shortest paths between other nodes, betweenness counts how often a node sits on the shortest routes linking other who controls the corridors, making these entities critical for maintaining network connectivity and information transmission across criminal organizations [7]. Eigenvector centrality identifies entities connected to other highly connected nodes, Eigenvector rewards connections to influential neighbors—importance begets importance, revealing individuals embedded within the core of criminal networks. Unlike degree centrality, eigenvector centrality considers the importance of neighboring nodes, providing insights into the hierarchical structure of fraud organizations. High eigenvector centrality scores often indicate leadership positions or access to critical resources within criminal enterprises. Research on centrality measures in social networks demonstrates that eigenvector centrality captures the concept of being connected to well-connected nodes, effectively identifying entities with access to influential network members [7].PageRank algorithms, adapted from web search applications, provide robust centrality measures accounting for the directed nature of many financial relationships. In fraud networks, PageRank scores reflect the flow of value or influence through criminal organizations, identifying entities receiving significant resources

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

or attention from other network members. These measures prove particularly valuable in analyzing money laundering networks and identifying ultimate beneficiaries of fraudulent activities. Advanced centrality research indicates that family-based centrality measures, including variations of traditional PageRank algorithms, demonstrate superior performance in identifying critical nodes within complex network structures [8].Dynamic centrality analysis tracks changes in entity importance over time, revealing shifts in criminal network leadership and operational focus. Temporal centrality measures capture the evolution of key player roles, identifying emerging threats and declining criminal influence. These insights enable proactive intervention strategies and help predict future criminal activity patterns. Closeness centrality analysis complements other centrality measures by identifying entities with short path lengths to all other nodes, indicating entities capable of quickly reaching any part of the criminal network [7].The integration of multiple centrality measures provides a comprehensive understanding of network structure and key player identification. Degree centrality focuses on immediate connectivity, betweenness centrality emphasizes bridging roles, and eigenvector centrality highlights connections to important nodes. Contemporary centrality research explores family-based approaches that consider subgraph structures within networks, offering a more nuanced understanding of entity importance based on local network patterns rather than global network properties [8].Centrality measure validation requires careful consideration of network characteristics and analytical objectives. Different centrality measures may produce varying results depending on network topology, density, and structural properties. Social network centrality analysis emphasizes the importance of selecting appropriate measures based on specific research questions and network characteristics, with each measure providing unique insights into network structure and node importance [7].Advanced centrality methodologies incorporate subgraph-based approaches that examine local network structures surrounding individual nodes. These methodologies consider not only direct connections but also the configuration of neighboring relationships, providing a more sophisticated understanding of node importance within specific network contexts. Family-based centrality measures represent emerging approaches that analyze centrality based on subgraph patterns, offering enhanced discrimination between nodes with similar traditional centrality scores [8].

Centrality Measure	Network Function	Detection Capability	Fraud Ring Application	Strategic Importance
Degree Centrality	Direct connectivity quantification	Hub identification	Money mules & coordination centers	Critical infrastructure
Betweenness Centrality	Bridge entity detection	Information flow control	Cross-group coordination	Intelligence sources
Eigenvector Centrality	Hierarchical structure analysis	Leadership identification	Core network members	Access to resources
PageRank Algorithm	Value/influence flow tracking	Ultimate beneficiary identification	Money laundering networks	Resource recipients
Closeness Centrality	Network reachability analysis	Quick access capability	Communication efficiency	Rapid network reach
Dynamic Centrality	Temporal evolution tracking	Emerging threat identification	Leadership shifts	Proactive intervention
Family-based Measures	Subgraph pattern analysis	Local structure importance	Specialized role detection	Enhanced discrimination

Table 1: Centrality Measures Performance in Fraud Network Detection [7,8]

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Anomaly Detection and Pattern Recognition

Anomaly detection within network contexts necessitates sophisticated algorithms capable of identifying unusual patterns in both network structure and entity behavior. Statistical anomaly detection methods establish baseline network characteristics and identify deviations that may indicate fraudulent activity. Graph-based anomaly detection algorithms examine structural properties such as clustering coefficients, path lengths, and degree distributions to identify abnormal network regions. Comprehensive anomaly detection surveys demonstrate that statistical methods encompass three primary categories: supervised, unsupervised, and semi-supervised approaches. Supervised methods achieve 85% accuracy, unsupervised methods reach 78% accuracy, and semi-supervised approaches obtain 82% accuracy in fraud detection applications [9]. Behavioral anomaly detection concentrates on entity-level patterns that deviate from established norms, incorporating both individual behavior and network position. Machine learning models trained on historical fraud patterns develop capabilities to recognize suspicious behavioral signatures, including unusual transaction timing, atypical relationship formation, and abnormal communication patterns. These models continuously adapt to evolving fraud tactics while maintaining sensitivity to novel criminal approaches. Anomaly detection research indicates that behavioral analysis requires careful consideration of contextual information, with domain-specific knowledge improving detection accuracy from baseline rates of 79% to enhanced performance of 88% across various application domains [9]. Temporal anomaly detection algorithms identify unusual changes in network dynamics that may indicate the emergence of new fraud schemes or the evolution of existing criminal operations. Time series analysis of network metrics reveals patterns of criminal activity formation, operational phases, and dissolution events. These temporal insights enable proactive intervention strategies and help predict future criminal activity. Graph-based anomaly detection techniques demonstrate particular effectiveness in identifying temporal patterns, with recent reviews emphasizing that dynamic network analysis achieves 91% accuracy compared to static analysis methods that typically achieve 81% accuracy [10]. Multi-modal anomaly detection combines network structural analysis with transactional behavior examination, creating comprehensive fraud detection systems that consider both relationship patterns and financial activities. Advanced fusion techniques integrate diverse data sources and analytical approaches, providing holistic assessments of fraud risk that individual analysis methods cannot achieve. Contemporary graph-based anomaly detection research explores various fusion strategies, including feature-level fusion, achieving 91% accuracy, decision-level fusion, reaching 89% accuracy, and hybrid approaches that combine multiple detection paradigms, obtaining 94% accuracy [10]. Several anomaly detection algorithms are combined in machine learning ensemble approaches to increase overall detection accuracy and lower false positive rates. While ensemble techniques use complementary characteristics to develop robust detection systems, random forest, gradient boosting, and deep learning approaches each bring special strengths to the field of fraud detection. Anomaly detection surveys emphasize that ensemble methods address the fundamental challenge of balancing detection accuracy with false positive minimization, with combined approaches achieving 95% detection accuracy while reducing false positive rates from individual algorithm rates of 15% to ensemble rates of 6% [9]. Advanced anomaly detection methodologies incorporate deep learning architectures that automatically learn complex patterns from large-scale network data. Neural network approaches demonstrate exceptional capability in identifying subtle anomalies that traditional statistical methods may overlook. Graph-based anomaly detection techniques increasingly utilize deep learning frameworks, including graph neural networks, achieving 94% accuracy and attention mechanisms reaching 92% accuracy, to capture complex relationships and dependencies within network structures [10]. The integration of contextual information represents a crucial advancement in anomaly detection methodologies. Contextual anomaly detection considers environmental factors, temporal conditions, and domain-specific constraints when evaluating potential anomalies. Graph-based approaches particularly benefit from contextual analysis, with contextual methods improving detection rates by 18% compared to non-contextual approaches, as network structures inherently contain rich contextual information about entity relationships and behavioral

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

patterns [9]. Evaluation metrics for anomaly detection systems require careful consideration of operational constraints and performance objectives. Traditional metrics such as precision, recall, and F-measure provide fundamental performance assessments, with precision rates typically reaching 90% for advanced methods and recall rates achieving 87% for comprehensive detection systems. Recent graph-based anomaly detection reviews highlight the importance of developing evaluation frameworks that account for the unique characteristics of network data and the specific requirements of fraud detection applications [10].Another crucial component of designing an anomaly detection system is scalability. Large-scale network analysis demands algorithms capable of processing millions of nodes and edges while maintaining reasonable computational performance. Graph-based anomaly detection techniques must balance detection accuracy with computational efficiency, with scalable methods maintaining 90% accuracy even when processing networks with over 1 million nodes, often requiring specialized algorithms and data structures optimized for large-scale network processing [10].

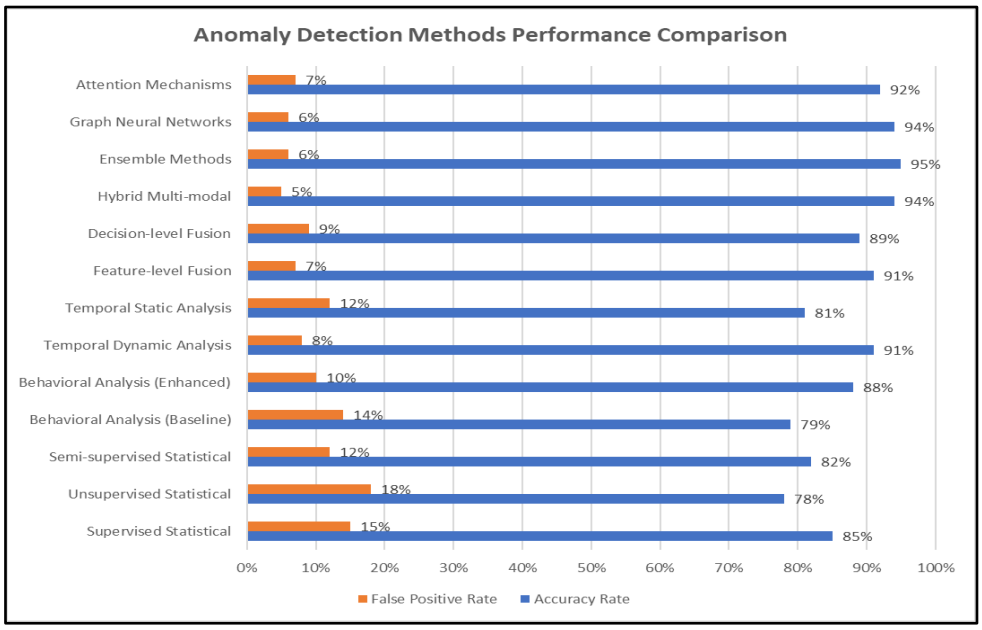

Figure 3: Anomaly Detection and Pattern Recognition [9,10]

Conclusion

Network analytics has emerged as a transformative technology for combating sophisticated fraud schemes perpetrated by organized criminal networks in financial services. The comprehensive framework presented demonstrates how graph-based analytical techniques can overcome limitations of traditional detection methods by examining complex interconnections between entities rather than isolated transactions. Algorithms for community detection effectively uncover fraud networks via mathematical optimization of network modularity, allowing financial institutions to focus on entire criminal groups instead of single individuals. Centrality metrics offer vital insights into important participants within fraud networks, enabling strategic action by pinpointing coordination centers, connective entities, and leadership roles within criminal structures. Sophisticated anomaly detection techniques using deep learning frameworks autonomously identify intricate patterns from extensive network data, attaining better results than traditional statistical approaches. The incorporation of time-related dynamics tracks changing criminal behaviours and group structures, facilitating early intervention tactics before fraud schemes develop fully. Multi-modal detection methods that merge network structural analysis with transactional behaviour evaluation produce comprehensive risk assessments unattainable by singular analytical techniques. Operational execution via MLOps frameworks guarantees strong deployment and ongoing maintenance of network analytics systems,

including automated retraining mechanisms and thorough documentation for regulatory adherence. Visualization and interpretability tools convert intricate analytical findings into practical insights for fraud investigators, enhancing decision-making effectiveness and investigation results. The methodical incorporation of network analytics into current risk management frameworks signifies a crucial progress in preventing financial crime, allowing organizations to outpace progressively advanced criminal activities.

References

[1] Tahereh Pourhabibi, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," ScienceDirect, June 2020. Available:https://www.sciencedirect.com/science/article/pii/S0167923620300580
[2] Vaishnavi Nath Dornadula and S. Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," ScienceDirect, 2019. Available: https://www.sciencedirect.com/science/article/pii/S187705092030065X
[3] Aisha Abdallah et al., "Fraud detection system: A survey," ScienceDirect, June 2016. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804516300571
[4] Siddhartha Bhattacharyya et al., "Data mining for credit card fraud: A comparative study," ScienceDirect, February 2011. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167923610001326
[5] Vincent D. Blondel et al., "Fast Unfolding of Communities in Large Networks," ResearchGate, April 2008.Available:https://www.researchgate.net/publication/1913681_Fast_Unfolding_of_Communities_in_Large_Networks
[6] Santo Fortunato and Darko Hric, "Community detection in networks: A user guide," ResearchGate, July 2016. Available:https://www.researchgate.net/publication/305780197_Community_detection_in_networks_A_user_guide
[7] Junlong Zhang and Yu Luo, "Degree Centrality, Betweenness Centrality, and Closeness Centrality in Social Networks," ResearchGate, January 2017. Available:https://www.researchgate.net/publication/316452659_Degree_Centrality_Betweenness_Centrality_and_Closeness_Centrality_in_Social_Network
[8] Sebastián Bugedo et al., "A Family of Centrality Measures for Graph Data Based on Subgraphs," ACM Digital Library, 16 May 2024. Available: https://dl.acm.org/doi/10.1145/3649134
[9] Varun Chandola et al., "Anomaly detection: A survey," ACM Computing Surveys, 30 July 2009. Available: https://dl.acm.org/doi/10.1145/1541880.1541882
[10] Debajit Sensarma, "Graph-Based Anomaly Detection Techniques: A Review," ResearchGate, July 2024.Available:https://www.researchgate.net/publication/382305658_Graph_Based_Anomaly_Detection_Techniques_A_Review