INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND TECHNOLOGY (IJARET)

ISSN Print: 0976-6480   ISSN Online: 0976-6499

https://iaeme.com/Home/journal/IJARET

High Quality Peer Reviewed Referred Scientific, Engineering & Technology, Medicine and Management International Journals

PUBLISHED BY

IAEME Publication

Plot: 03, Flat- S 1, Poomalai Santosh Pearls Apartment,
Plot No. 10, Vaiko Salai 6th Street, Jai Shankar Nagar, Palavakkam,
Chennai - 600 041, Tamilnadu, India

Email : editor@iaeme.com, iaemedu@gmail.com

www.iaeme.com

International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 16, Issue 4, July-August 2025, pp. 1-9, Article ID: IJARET_16_04_001
Available online at https://iaeme.com/Home/issue/IJARET?Volume=16&Issue=4
ISSN Print: 0976-6480 and ISSN Online: 0976-6499; Journal ID: 1793-4637
Impact Factor (2025): 28.80 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJARET_16_04_001

A COMPREHENSIVE SURVEY ON MACHINE LEARNING TECHNIQUES FOR FRAUD DETECTION IN SOCIAL NETWORKS

V. Queen Jemila

Assistant Professor, Department of Computer Applications,
V. V. Vanniaperumal College for Women, Virudhunagar, India.

Dr. VidhyaSathish
Assistant Professor, School of Computing Science,
Department of Advanced Computing and Analytics, VISTAS, Pallavaram, Chennai, India.

T. Devasena
Assistant Professor, Department of Cognitive Systems,
SDNB Vaishnav college for women, Chrompet, Chennai, India.

ABSTRACT

The proliferation of social media platforms has transformed how individuals communicate, disseminate material, and consume information. Moreover, social networks have evolved into a refuge for fraudulent activities such as automated bots, phishing schemes, disinformation operations, and counterfeit profiles. Machine learning methodologies have increasingly been employed for fraud detection to mitigate these emerging concerns. This paper provides a comprehensive examination of various machine learning models utilized in social network fraud detection, including traditional methods such as supervised and unsupervised learning, as well as advanced approaches like deep learning, ensemble techniques, and graph-based models.

Furthermore, it emphasizes multimodal strategies that integrate social network frameworks, textual information, visual media, and user actions for enhanced detection accuracy. The study provides a vital evaluation of current methodologies regarding accuracy, scalability, and relevance to practical situations. The discussion encompasses essential datasets, assessment measures, and prevalent limitations within the existing research environment. The survey continues by noting existing shortcomings and emphasizing future research opportunities, such as interpretable models, resilient real-time systems, and privacy-preserving frameworks.

Keywords: Auto Encoder, Graph Cutting, GNN, GDBMS

Cite this Article: V. Queen Jemila, VidhyaSathish, T. Devasena. (2025). A Comprehensive Survey on Machine Learning Techniques for Fraud Detection in Social Networks. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 16(4), 1-9.

https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_16_ISSUE_4/IJARET_16_04_001.pdf

1. Introduction

The advent of online social networks such as Facebook, Instagram, LinkedIn, and Twitter has profoundly transformed communication, information sharing, and company operations online. These platforms, equipped with real-time communication and community-building functionalities, serve billions of individuals globally. However, this vast, public, and often anonymous environment has also become a fertile ground for diverse forms of fraud and malicious conduct.

Social network fraud can manifest through the creation of fraudulent or bot-operated accounts, identity theft, cyberbullying, phishing schemes, financial scams, click fraud, and orchestrated disinformation campaigns. Such actions entail significant consequences, including psychological distress, violations of personal information, political manipulation, and substantial financial losses. The dynamic and ever-evolving nature of these attacks renders fraud detection increasingly challenging. Assignment.

Conventional fraud detection techniques depend significantly on human developed rules and established heuristics, which tend to be inflexible, non-adaptive, and inadequate for scaling with extensive and dynamic datasets. Conversely, machine learning methodologies enable the extraction of insights from data, reveal concealed patterns, and facilitate real-time predictive decision-making, rendering them particularly effective for fraud detection within social networks. Furthermore, the variety of fraudulent behaviors across many platforms and the necessity for automated, scalable, and intelligent detection systems have resulted in an increase in machine learning-based solutions. This encompasses supervised learning for classification tasks, unsupervised anomaly detection, graph-based learning for analyzing network architecture, and deep learning for modeling intricate, non-linear relationships in extensive datasets.

A comprehensive and current review of various machine learning methodologies is necessary to: Present a comprehensive overview of the current advancements. Identify the advantages and disadvantages of different methodologies. Evaluate algorithms based on performance, scalability, interpretability, and resource demands. Recognize enduring obstacles, including insufficient labeled data, large dimensionality, adversarial instances, and privacy issues. Identify nascent patterns and unresolved research challenges that forthcoming investigations may explore.

1.1 How This Survey Differs from Other Surveys

Most current surveys on fraud detection either concentrate on various domains or tackle general internet fraud. This survey focuses on fraud detection in social networks, targeting platform-specific risks such as counterfeit profiles, bots, click farms, misinformation, and Sybil assaults, so rendering it particularly pertinent in the era of social media. This assessment presents a comprehensive taxonomy that encompasses supervised, unsupervised, semi-supervised, deep learning, ensemble approaches, and graph-based models, in contrast to preceding publications that typically focus solely on supervised or unsupervised learning models. This article prioritizes multimodal approaches—integrating textual data visual content (e.g., profile images), network structure and temporal patterns—over surveys that primarily examine user behavior or metadata to enhance fraud detection efficacy.

A comparative assessment based on

- ✓ Accuracy and precision o Real-time processing capability
- ✓ Scalability to extensive networks
- ✓ Adaptability to changing fraudulent strategies

This survey uniquely explores issues like

- Adversarial assaults
- Privacy and ethical considerations
- Data imbalance and challenges in annotation

- Conceptual drift in the evolution of fraudulent patterns

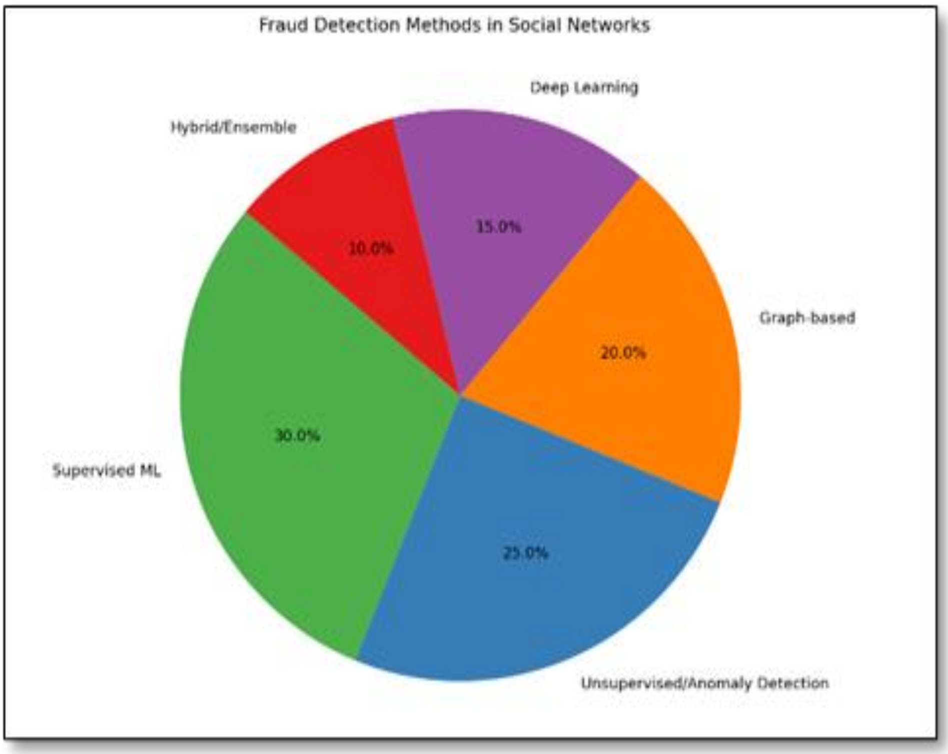

figure 1: Fraud Detection Methods in Social Networks

2. Literature Review

The advancement of fraud detection techniques in social networks has been significantly supported by several studies. The inaugural study utilizing graph-based supervised learning to identify spammers and fraudulent users was authored by Haider Ali Javaid (2024). Their research demonstrated the efficacy of predictive analysis through the application of advanced machine learning algorithms.

Haider Ali Javaid (2024) emphasized the importance of relational learning in interconnected data and introduced the concept of collaborative categorization for fraud detection. Their technique illustrated the advantage of augmenting confidential financial institution data via network architecture.

S Amit Roy, Juan Shu, and Jia Li (2024) investigated deep autoencoder-based anomaly detection, emphasizing the identification of fraudulent profiles and atypical activity patterns. To detect anomalous nodes in a graph via Graph Anomaly Detection techniques. Their findings highlighted the advantages of employing deep representations instead of conventional feature engineering.

Qiuyang Mang, Jinseng BA, and Eth Pinjia He (2025) introduced graph-cutting algorithms to detect logical errors in Graph Database Management Systems. Graph Neural Networks (GNNs) for fraud detection demonstrated their capacity to encapsulate intricate interdependencies in user behavior across time. This signified a transition towards utilizing deep learning in dynamic settings.

Shasank Sheshar Singh, Shashank Singh, Kuldeep Singh, Vishal Srivastava, and Harish Kumar created models for opinion mining, sentiment analysis, and text mining. Moreover, hybrid models that include supervised and unsupervised methodologies, as they have indicated, exhibit enhanced robustness and adaptability in identifying developing fraud trends. These models employ Lambda architecture, Kappa architecture, and GraphX architecture. Utilizing ensemble learning and multi-view features to improve detection across varied datasets.

Collectively, these studies form the backbone of current knowledge and point toward a growing trend of integrating structural, temporal, and content-based signals to improve detection accuracy and generalizability in real-world social networks.

2.1 Comparative Analysis

S.No	**Title of the Paper**	**Authors & Year**	**Objective**	**Methodology**	**Dataset/Tools**	**Results**	**Limitations**
1.	Improving Fraud Detection and Risk Assessment in Financial Service using Predictive Analytics and Data Mining	Haider Ali Javaid, 2024	Fraud detection using data mining and predictive analytics	graph-based algorithms	Financial data	predictive analytics in risk assessment.	Dealt with general level issues

2.	Leveraging Machine Learning for Fraudulent Social Media Profile Detection	Soorya Ramdas, Agnes Neenu N. T. 2024	how data mining and predictive analytics methods make use of vast amounts of financial data to find trends, connections, and insights.	Graph based social network analysis algorithms	Customer data	Financial institutions may preserve client confidence, secure their assets, and remain in compliance with regulations	It suggests the solution for generic data only
3.	GAD-NR: Graph Anomaly Detection via Neighborhood Reconstruction	Amit Roy, Juan Shu, Jia Li 2024	To identify the abnormal nodes in Graph using Graph Anomaly Detection	Auto Encoder	real-world datasets (Cora, Weibo, Reddit, Disney, Books, and Enron)	detection of various anomalies including con-textual, structural, and joint-type anomalies.	With a higher latent dimension size, the model becomes too much expressive and it can overfit the anomalies.
4.	Finding Logic Bugs in Graph-processing Systems via Graph-cutting	Qiuyang Mang, Jinseng BA, and Eth Pinjia He 2025	To detect logic bugs in Graph Database Management System	Graph Cutting	NetworkX, Neo4j, and Kùzu.	Find the bugs in Graph Dtatabase Management System	It may try to find the bugs in Cypher based GDBMS

5.	Big Data Meets Social Networks: A Survey of Analytical Strategies and Research Challenges	Shasank Sheshar Singh, Shashank Singh, Kuldeep Singh, Vishal Srivastava, and Harish Kumar 2025	opinion mining, sentiment analysis, text mining, and natural language processing in Social Networks data	Lambda architecture, Kappa architecture, and GraphX architecture.	Social Network Analysing Techniques	Provide generic solutions without any implementation	No datasets are analyzed

3. Conclusion

This survey reviewed the progression of machine learning techniques used in fraud detection within social networks, covering classical supervised methods, unsupervised and anomaly detection approaches, graph-based models, and deep learning architectures. While traditional methods offer transparency and simplicity, modern techniques like GNNs deliver improved performance in capturing sophisticated fraud patterns. However, challenges persist, such as limited labeled datasets, evolving attacker strategies, and the demand for real-time, scalable, and interpretable solutions. Future research should emphasize creating adaptable, explainable models that combine multiple data sources and collaborate with industry to develop resilient, ethical fraud detection systems that enhance the safety of social network environments.

References

[1] Leman Akoglu, Hanghang Tong, and Danai Koutra. Graph-based anomaly detection and description: a survey. Data mining and knowledge discovery, 2015.

[2] Leman Akoglu, Hanghang Tong, Jilles Vreeken, and Christos Faloutsos. Fast and reliable anomaly detection in categorical data. In CIKM, 2012.

[3] Sambaran Bandyopadhyay, N Lokesh, and M Narasimha Murty. Outlier aware network embedding for attributed networks. In AAAI, 2019.zv

[4] Sambaran Bandyopadhyay, N Lokesh, and M Narasimha Murty. Outlier aware network embedding for attributed networks. In AAAI, 2019.

[5] Sambaran Bandyopadhyay, Saley Vishal Vivek, and MN Murty. Outlier resistant unsupervised deep architectures for attributed network embedding. In WSDM,2020.

[6] Sambaran Bandyopadhyay, Saley Vishal Vivek, and MN Murty. Outlier resistant unsupervised deep architectures for attributed network embedding. In WSDM,2020. Aleksandar Bojchevski and Stephan Günnemann. Bayesian robust attributed graph clustering: Joint learning of partial anomalies and group structure. AAAI, 2018.

[7] Tianyi Chen and Charalampos Tsourakakis. Antibenford subgraphs: Unsuper-vised anomaly detection in financial networks. In KDD, 2022.

[8] Zhenxing Chen, Bo Liu, Meiqing Wang, Peng Dai, Jun Lv, and Liefeng Bo. Gen-erative adversarial attributed network anomaly detection. In CIKM, 2020.

[9] Javier E Contreras-Reyes and Reinaldo B Arellano-Valle. Kullback–leibler diver-gence measure for multivariate skew-normal distributions. Entropy, 2012.

[10] Benoıt Corsini, Pierre-André Noël, David Vázquez, and Perouz Taslakian. Self-supervised anomaly detection in static attributed graphs. arxiv, 2021.

[11] Gabriele Corso, Luca Cavalleri, Dominique Beaini, Pietro Liò, and Petar eličković. Principal neighbourhood aggregation for graph nets. NeurIPS, 2020.Gh

[12] C. Fernandez-Basso, A. J. Francisco-Agra, M. J. Martin-Bautista, and M. Dolores Ruiz, ‘‘Finding tendencies in streaming data using big datafrequent itemset mining,’’ Knowl.-Based Syst., vol. 163, pp. 666–674,Jan. 2019.

[13] V. Persico, A. Pescapé, A. Picariello, and G. Sperlí, ‘‘Benchmarking big data architectures for social networks data processing using public cloud platforms,’’ Future Gener. Comput. Syst., vol. 89, pp. 98–109, Dec. 2018.

[14] S. Sagiroglu and D. Sinanc, ‘‘Big data: A review,’’ in Proc. Int. Conf. Collaboration Technol. Syst. (CTS), May 2013, pp. 42–47.

[15] N. A. Ghani, S. Hamid, I. A. T. Hashem, and E. Ahmed, ''Social media big data analytics: A survey,'' Comput. Hum. Behav., vol. 101, pp. 417–428, Aug. 2018.

Citation: V. Queen Jemila, VidhyaSathish, T. Devasena. (2025). A Comprehensive Survey on Machine Learning Techniques for Fraud Detection in Social Networks. International Journal of Advanced Research in Engineering and Technology (IJARET), 16(4), 1-9.

Abstract Link: https://iaeme.com/Home/article_id/IJARET_16_04_001

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_16_ISSUE_4/IJARET_16_04_001.pdf

✉ **editor@iaeme.com**