International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 6, June 2026)

Review on AI Approach for Financial Fraud Detection

Deepak Kuma[1], Dr. Chinmay Bhatt[2],
[1]M.Tech Scholar, Department of CSE, SRK University, Bhopal, India
[2]Professor, Department of CSE, SRK University, Bhopal, India

Abstract **Financial fraud has become a significant challenge in modern digital financial systems due to the increasing volume and complexity of online transactions. Artificial Intelligence (AI) has emerged as a powerful approach for detecting fraudulent activities by analyzing large datasets, identifying hidden patterns, and recognizing suspicious behavior in real time. This review examines various AI-based techniques used for financial fraud detection, including Machine Learning, Deep Learning, Neural Networks, Decision Trees, Random Forests, Support Vector Machines, and Hybrid AI models. The study highlights the effectiveness of these approaches in improving detection accuracy, reducing false alarms, and adapting to evolving fraud strategies. Furthermore, the review discusses commonly used datasets, evaluation metrics, challenges, and recent advancements in AI-driven fraud detection systems. The findings indicate that AI-based solutions provide a more efficient and scalable framework for identifying fraudulent transactions compared to traditional rule-based methods, making them essential for enhancing security and trust in financial services.**

Keywords—DL, IOT, Botnet, CNN, RNN, LSTM.

I. INTRODUCTION

Financial fraud detection refers to the process of identifying, preventing, and investigating illegal financial activities performed with the intention of obtaining unauthorized monetary benefits [1]. In recent decades, the financial sector has undergone significant digital transformation through the adoption of online banking, mobile payment systems, digital wallets, and electronic commerce platforms. These technological developments have increased the speed, accessibility, and convenience of financial transactions while simultaneously creating new opportunities for fraudulent activities. Consequently, financial fraud has emerged as a major concern for financial institutions, regulatory authorities, businesses, and consumers across the world. Effective fraud detection mechanisms are therefore essential to ensure the security and reliability of financial systems.

The increasing adoption of digital financial services has resulted in an unprecedented growth in transaction volumes and data generation [2]. Every day, banks and financial organizations process millions of transactions involving customers from diverse geographical locations and economic backgrounds. The vast amount of transaction data generated through these activities provides valuable information for detecting suspicious behavior. However, the sheer scale and complexity of financial datasets make manual monitoring extremely difficult and time-consuming. As a result, organizations require automated detection systems capable of analyzing large volumes of data efficiently and accurately.

The emergence of sophisticated cyber threats has further complicated the challenge of fraud detection in modern financial environments [3]. Fraudsters continuously develop innovative methods to bypass security measures, exploit system vulnerabilities, and conceal fraudulent activities. Advanced attack techniques such as phishing, account takeover, synthetic identity fraud, and online payment manipulation have become increasingly common. These evolving threats require organizations to adopt intelligent and adaptive detection approaches that can identify abnormal patterns and respond to new fraud strategies in real time.

Financial fraud has become a critical issue for the global financial industry due to its significant economic and social consequences [4]. Fraudulent activities can lead to substantial financial losses, legal liabilities, operational disruptions, and reputational damage for affected institutions. In addition, customers who become victims of fraud may lose confidence in digital financial services, reducing trust in financial organizations. Therefore, the implementation of reliable fraud detection systems plays an important role in maintaining customer satisfaction, regulatory compliance, and overall financial stability.

Financial fraud encompasses a wide range of illegal activities designed to obtain financial benefits through deception or misrepresentation [5]. Common forms of fraud include credit card fraud, identity theft, insurance fraud, tax fraud, loan fraud, money laundering, and fraudulent financial reporting. Each type of fraud presents unique characteristics and challenges, requiring specialized

detection techniques and analytical methods. Understanding the nature and patterns of different fraud categories is essential for designing effective prevention and detection strategies.

The diversity of fraud types in financial systems has increased considerably with the expansion of digital technologies and online services [6]. Fraudsters exploit multiple channels, including internet banking platforms, mobile applications, payment gateways, and electronic commerce systems. Because fraudulent transactions often resemble legitimate activities, distinguishing between genuine and malicious behavior remains a challenging task. Consequently, fraud detection systems must analyze multiple transaction attributes and behavioral indicators to accurately identify suspicious activities while minimizing incorrect classifications.

Financial fraud not only causes direct economic losses but also has broader implications for organizations and society [7]. Large-scale fraud incidents can affect market confidence, disrupt business operations, and increase regulatory scrutiny. Financial institutions often invest significant resources in fraud prevention, investigation, and recovery efforts. Additionally, customers impacted by fraudulent activities may experience financial hardship and reduced trust in financial services. These consequences highlight the importance of developing robust and proactive fraud management frameworks.

Modern financial organizations recognize fraud detection as a crucial component of risk management and security operations [8]. Effective fraud detection systems enable organizations to monitor transactions continuously, identify unusual behavior, and generate timely alerts for further investigation. Such systems help reduce financial losses, improve operational efficiency, and support compliance with regulatory requirements. Furthermore, early detection of fraudulent activities allows institutions to take corrective actions before significant damage occurs.

Traditional fraud detection methods were primarily based on statistical analysis, manual auditing, and expert-defined rules [9]. These approaches relied on predefined thresholds and transaction characteristics to identify suspicious activities. Although they provided a foundation for fraud prevention, traditional methods often struggled to handle complex and rapidly changing fraud patterns. Their dependence on static rules limited their ability to detect previously unseen fraudulent behaviors, resulting in reduced effectiveness in dynamic financial environments[10].

To address the limitations of conventional approaches, researchers explored data mining and analytical techniques for fraud detection [11]. Data mining methods enable the extraction of hidden patterns, relationships, and anomalies from large financial datasets. By analyzing historical transaction records, these techniques can identify characteristics associated with fraudulent behavior and support more accurate decision-making. The integration of advanced analytical methods significantly improved the efficiency and effectiveness of fraud detection processes[12].

II. LITERATURE SURVEY

Priyadarshi et al. [1] presented a Graph Neural Network (GNN)-based financial fraud detection framework that models financial transactions as graph structures. The approach captures relationships among entities and transactions to identify hidden fraud patterns. The proposed model effectively detects interconnected fraudulent activities that are difficult to identify using conventional methods. Experimental results demonstrated improved fraud detection accuracy and enhanced capability for analyzing complex financial networks.

Duan et al. [2] introduced the CaT-GNN model for credit card fraud detection by integrating causal learning and temporal graph neural networks. The framework considers both transaction sequence information and causal relationships among entities. This combination improves the understanding of evolving fraud behaviors in dynamic financial environments. The results showed superior detection performance and robustness compared to traditional graph-based approaches.

Wang et al. [3] developed a deep learning-based credit card fraud detection system incorporating attention mechanisms. The attention layer enables the model to focus on important transaction features while reducing the influence of irrelevant information. The proposed architecture effectively learns complex transaction patterns associated with fraudulent behavior. Experimental evaluations demonstrated improved accuracy, precision, and recall over conventional deep learning models.

Zhang et al. [4] presented a hybrid machine learning framework for credit card fraud detection by combining multiple classification algorithms. The proposed system leverages the strengths of different learning techniques to improve classification performance. The framework effectively addresses issues related to class imbalance and transaction diversity. Experimental results indicated

enhanced fraud detection capability with reduced false-positive rates.

Fiore et al. [5] investigated the use of Generative Adversarial Networks (GANs) to improve fraud detection performance. The authors generated synthetic fraud samples to overcome the class imbalance problem present in credit card transaction datasets. The augmented dataset significantly improved classifier training and fraud identification accuracy. The study demonstrated the effectiveness of GAN-based data generation for financial fraud applications.

Roy et al. [6] explored deep learning techniques for detecting fraudulent credit card transactions. The proposed framework utilized neural network architectures to automatically learn hidden transaction patterns from large datasets. The model achieved higher detection accuracy compared to several traditional machine learning approaches. The study highlighted the suitability of deep learning for real-time fraud detection environments.

West et al. [7] conducted a comprehensive investigation of intelligent financial fraud detection practices. The study reviewed existing techniques including statistical analysis, data mining, machine learning, and hybrid detection approaches. Various challenges such as data imbalance, evolving fraud strategies, and real-time detection requirements were discussed. The authors also identified future research directions for developing more effective fraud detection systems.

Ravisankar et al. [8] focused on financial statement fraud detection using data mining and feature selection techniques. The study analyzed financial indicators and evaluated multiple classification algorithms for fraud prediction. Feature selection methods were employed to identify the most relevant attributes affecting fraudulent reporting. Results showed improved classification accuracy and reduced computational complexity.

Chen et al. [9] proposed a hybrid fraud detection framework combining stepwise regression, logistic regression, support vector machines, and decision trees. The objective was to forecast fraudulent financial statements more accurately than individual classifiers. The integrated approach benefited from the strengths of multiple predictive techniques. Experimental results demonstrated superior fraud prediction performance and increased classification reliability.

Gyamfi et al. [10] developed a bank fraud detection model based on Support Vector Machine (SVM) classification. The model analyzed banking transaction data to differentiate fraudulent activities from legitimate transactions. The proposed system achieved satisfactory accuracy and demonstrated strong classification capabilities. The study confirmed the effectiveness of SVM for banking fraud detection applications.

Sundarkumar et al. [11] introduced a one-class SVM-based undersampling technique for handling imbalanced datasets in insurance fraud detection. The proposed method improved the representation of minority fraud cases while maintaining data quality. Experimental analysis showed enhanced fraud detection performance and better classification results. The research emphasized the importance of data balancing in fraud analytics.

Li et al. [12] proposed a Lib-SVM-based financial statement fraud detection model using data from Chinese listed companies. The framework analyzed financial indicators to identify profit manipulation and fraudulent reporting activities. Support Vector Machine classification was employed to distinguish fraudulent and non-fraudulent financial statements. Results demonstrated the effectiveness of the proposed model in detecting financial reporting fraud with high reliability.

III. CHALLENGES

Financial fraud detection faces numerous challenges due to the increasing complexity of financial transactions, rapid growth of digital payment systems, and continuously evolving fraud techniques. Modern fraudsters frequently modify their strategies to bypass existing security mechanisms, making fraud detection a dynamic and difficult task. Financial datasets are often characterized by high volume, velocity, and variety, which increases computational requirements and analysis complexity. Additionally, the imbalance between legitimate and fraudulent transactions can reduce model effectiveness and increase the likelihood of misclassification. Ensuring real-time detection while maintaining high accuracy and low false alarm rates remains a significant challenge for researchers and financial institutions. Furthermore, privacy concerns, data quality issues, and the need for model interpretability further complicate the development of reliable fraud detection systems.

1. **Class Imbalance Problem:** In financial transaction datasets, fraudulent transactions typically account for less than 1% of the total records. As a result, machine learning models become biased toward the majority class (legitimate transactions) and may fail to identify rare fraud cases accurately. This imbalance often leads to poor recall and reduced fraud detection performance.
2. **Evolving Fraud Techniques:** Fraudsters continuously modify their attack strategies to avoid detection. New fraud methods such as synthetic identity fraud, account takeover attacks, and sophisticated phishing schemes emerge regularly. Detection systems trained on historical data may struggle to recognize these new fraud patterns, requiring continuous model updates and retraining.
3. **Large-Scale Transaction Data:** Modern financial institutions process millions of transactions every day through online banking, mobile payments, and digital commerce platforms. Analyzing such large volumes of data requires significant computational resources, efficient storage systems, and scalable algorithms capable of handling high-speed transaction streams.
4. **High False Positive Rates:** Many fraud detection systems incorrectly classify legitimate transactions as fraudulent. These false alarms can result in unnecessary transaction blocking, customer dissatisfaction, and increased operational costs due to manual investigations. Reducing false positives while maintaining high fraud detection accuracy remains a major challenge.
5. **Real-Time Detection Requirements:** Financial fraud must often be detected within seconds before a transaction is completed. Real-time fraud detection systems need to process incoming transactions instantly and make accurate decisions with minimal delay. Achieving both high speed and high accuracy simultaneously is a difficult task for many detection frameworks.
6. **Data Privacy and Regulatory Compliance:** Financial data contains highly sensitive customer information, including account details, transaction histories, and personal identifiers. Fraud detection systems must comply with privacy regulations and security standards while still allowing effective analysis. Balancing data accessibility and privacy protection is a significant challenge.
7. **Poor Data Quality and Missing Information:** Financial datasets may contain incomplete records, missing values, duplicate entries, inconsistent formats, and noisy information. Poor-quality data can negatively impact feature extraction and model training processes, resulting in reduced detection accuracy and unreliable fraud predictions.
8. **Model Interpretability and Transparency:** Advanced AI techniques such as Deep Learning and Graph Neural Networks often operate as black-box models. Although they may achieve high detection accuracy, understanding the reasoning behind their decisions can be difficult. Financial institutions and regulatory agencies require transparent and explainable models to justify fraud alerts and support decision-making processes.

IV. CONCLUSION

Financial fraud detection has become an essential component of modern financial security due to the rapid growth of digital transactions and increasingly sophisticated fraudulent activities. This review examined various approaches ranging from traditional machine learning techniques such as Support Vector Machines, Decision Trees, and Logistic Regression to advanced Artificial Intelligence methods including Deep Learning, Generative Adversarial Networks, Attention-Based Networks, and Graph Neural Networks. The reviewed studies demonstrate that AI-driven models provide superior capability in identifying complex fraud patterns, handling large-scale transaction data, and improving detection accuracy. Recent developments in graph-based learning and hybrid intelligence frameworks have further enhanced the effectiveness of fraud detection systems by capturing hidden relationships among financial entities. Despite these advancements, challenges such as class imbalance, evolving fraud strategies, real-time processing requirements, data privacy concerns, and model interpretability continue to affect system performance. Future research should focus on developing explainable, scalable, and adaptive AI models capable of addressing these challenges while ensuring

robust and reliable fraud detection in dynamic financial environments.

REFERENCES

1. S. Priyadarshi, J. Kumar and A. N, "Financial Fraud Detection Using Graph Neural Networks," *2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC)*, GB Nagar, Gwalior, India, 2025, pp. 537-541, doi: 10.1109/AIC66080.2025.11212157.
2. Duan, Y., Zhang, G., Wang, S., Peng, X., Ziqi, W., Mao, J., Wu, H., Jiang, X., Wang, K., 2024. CaT-GNN: Enhancing Credit Card Fraud Detection via Causal Temporal Graph Neural Networks. *arXiv preprint* arXiv: 2402.14708.
3. Wang, J., Li, Y., Zhang, H., and Chen, X., "Deep Learning-Based Credit Card Fraud Detection Using Attention Mechanisms," IEEE Access, vol. 11, pp. 118420–118432, 2023, doi: 10.1109/ACCESS.2023.3317421.
4. Zhang, Y., Liu, Q., and Zhou, Z., "Hybrid Machine Learning Framework for Credit Card Fraud Detection," Expert Systems with Applications, vol. 213, pp. 118901, 2023, doi: 10.1016/j.eswa.2022.118901.
5. Fiore, U., De Santis, A., Perla, F., Zanetti, P., and Palmieri, F., "Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection," Information Sciences, vol. 479, pp. 448–455, 2022, doi: 10.1016/j.ins.2018.02.046.
6. Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., and Beling, P., "Deep Learning Detecting Fraud in Credit Card Transactions," 2018 Systems and Information Engineering Design Symposium (SIEDS), IEEE, 2022, pp. 129–134, doi: 10.1109/SIEDS49339.2022.9624093.
7. J. West, M. Bhattacharya, and R. Islam, "Intelligent Financial Fraud Detection Practices: An Investigation," in *10th International ICST Conference on Security and Privacy in Communication Networks (Se-cureComm)*, Beijing, China, Sep. 2014, pp. 186–203. doi: 10.1007/978-3-319-23802-9-16.
8. P. Ravisankar, V. Ravi, G. R. Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," *Decision Support Systems*, vol. 50, no. 2, pp. 491–500, 2011. doi: https://doi.org/10.1016/j.dss.2010.11.006.
9. S. Chen, Y. Goo, and Z. Shen, "A Hybrid Approach of Stepwise Regression, Logistic Regression, Support Vector Machine, and Decision Tree for Forecasting Fraudulent Financial Statements," *The Scientific-WorldJournal*, vol. 2014, Sep. 2014. doi: 10.1155/2014/968712.
10. N. K. Gyamfi and J. Abdulai, "Bank Fraud Detection Using Support Vector Machine," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, pp. 37–41. doi: 10.1109/IEMCON.2018.8614994.
11. G. G. Sundarkumar, V. Ravi, and V. Siddeshwar, "One-class support vector machine based undersampling: Application to churn prediction and insurance fraud detection," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2015, pp. 1–7. doi: 10.1109/ICCIC.2015.7435726.
12. X. Li and S. Ying, "Lib-SVMs Detection Model of Regulating-Profits Financial Statement Fraud Using Data of Chinese Listed Companies," in *2010 International Conference on Electrical and Electronics Engineering (ICEEE)*, 2010. doi: 10.1109/ICEEE.2010.5660371.