A Comprehensive Survey on Fraud Detection Methods in Financial Transactions

Shreenidhi T L[1], Sagar B M[2]

[1]Department of Information Science Engineering, RV College of Engineering, Bengaluru, India
[2]Head of Department, Department of Information Science Engineering, RV College of Engineering, Bengaluru, India

---***---

Abstract - Financial institutions have enormous hurdles as a result of fraudulent transactions, which makes the creation and application of strong detection techniques necessary. This research paper offers a thorough examination of the approaches currently in use for identifying fraudulent activity on different financial platforms. It examines both cutting-edge and conventional strategies, such as data mining, artificial intelligence, and machine learning algorithms, as well as statistical and rule-based systems. It also looks at how big data and real-time analytics may work together to improve detection accuracy. Future approaches in fraud detection research are also covered in this study, along with the advantages and disadvantages of these methods and the significance of adaptive learning models. Through an amalgamation of current developments and persistent obstacles, this assessment seeks to provide significant perspectives for scholars committed to battling financial deception.

***Key Words*:** Fraudulent transactions, financial platforms, rule-based systems, machine learning, data mining, real-time analytics, big data.

1.INTRODUCTION

An issue that global financial institutions must deal with is the rise in fraudulent transactions [21, 22], necessitating the ongoing development of robust detection methods. As financial platforms become more digitally connected, methods employed in committing fraud is becoming more complex and sophisticated [17, 16]. In response, scholars and practitioners are looking at a variety of strategies and technologies in order to effectively identify and reduce these hazards [18].

Traditional approaches that have been used for a long time in fraud detection attempts, such as rule-based systems and statistical techniques, are covered in this paper [2, 3]. Since they offer possible means of enhancing detection accuracy, contemporary techniques like artificial intelligence [8], data mining [7], and machine learning algorithms [4, 5] are also investigated. Furthermore, studies are conducted on the role that real-time analytics integration and big data utilisation have in improving detection capacities [9, 10].

With a thorough examination of the benefits and drawbacks of various approaches [12, 13], this review aims to provide academics and practitioners with insightful knowledge. It also explores the importance of adaptive learning models in adapting to evolving fraud trends and future directions in fraud detection research [11]. By carrying out this in-depth examination, the study seeks to support the ongoing initiatives to stop financial fraud and safeguard the integrity of financial systems.

2. Types of fraud detection

2.1 Supervised Learning methods

The critical problem of identifying credit card fraud in the middle of the increase in online transactions is addressed by Thennakoon et al. [1]. Their research uses machine learning models to analyse both numerical and categorical data with the goal of identifying four primary types of fraud. To overcome data imbalance, they use resampling techniques, and they choose the best algorithms for efficiently identifying fraud patterns. An API module, fraud detection models, and a data warehouse are all included in their suggested real-time fraud detection system for easy transaction monitoring and alerts. Categorical values from credit card transactions are among the key features; attributes are prioritised to effectively capture fraudulent tendencies. The technology is promising, but it has to overcome obstacles including data imbalance and data mining's time-consuming character. Support Vector Machine, Naive Bayes, K-Nearest Neighbour, and Logistic Regression are scalable algorithms that can be applied in real-time to large-scale fraud detection. Subsequent endeavours seek to augment the precision of forecasts and incorporate location-based fraud identification.

In order to combat credit card fraud detection, Cheng et al. [2] present a unique Spatio-Temporal Attention-Based Neural Network (STAN) that recognises both temporal and spatial patterns in transaction data. With attention mechanisms and 3D convolutions integrated, STAN improves accuracy and achieves great performance, as evidenced by its October, November, and December AUC values of 0.8832, 0.8789, and 0.8865. However, real-world implementation faces difficulties due to the model's complexity, which necessitates substantial computational resources and knowledge. Concerns may include limited interpretability and scalability. In order to facilitate integration and have wider use in financial systems, future research attempts to simplify and increase the scalability of the model.

A study on credit card fraud detection in the FinTech industry is presented by AbdulSattar and Hammad [3], which is important given the rise in e-commerce. Using the Task1 and Task2 datasets, they use machine learning methods such as Random Forest, J48, IBk, Decision Tree, and Stochastic Gradient Descent for binary classification. The best performer is Random Forest, which has high accuracy and precision ratings. The main features that are employed are transaction details, merchant category code, and customer behaviour. Reliability of the system is impacted by issues like unbalanced data and privacy concerns, even in the face of good performance indicators. Subsequent investigations aim to tackle these obstacles and augment the precision of fraud detection, hence augmenting the efficacy of preventive measures inside the FinTech domain.

Using machine learning methods, Bagga et al. [4] address the problem of identifying fraudulent bank transactions. To increase accuracy, they suggest a method that blends machine learning and deep learning models, such as the Bidirectional Gated Recurrent Unit (BiGRU) and Bidirectional Long Short-Term Memory (BiLSTM). Their model achieves a score of 91.37%, outperforming conventional classifiers. Nevertheless, the study ignores a thorough examination of the computing resource needs for practical deployment and fails to address implementation issues and result interpretability. OldbalanceDest, NewbalanceDest, isFraud, and isFlaggedFraud are among the important features that are used. Even though the Random Forest Classifier, MLP Regressor, and Decision Tree Classifier exhibit good accuracy rates, further research is needed to determine how to scale large-scale fraud detection for real-world financial systems and effectively manage enormous transaction datasets.

The Neural Aggregate Generator (NAG) is presented by Ghosh Dastidar et al. [5] in order to solve the difficulties associated with manual feature aggregation in credit card fraud detection. By using transaction relationships to replicate manual approaches, NAG automates feature extraction and improves interpretability and prediction performance. Large training datasets and deciphering the intricacy of learned features present challenges. Although it isn't mentioned specifically, the automated nature of NAG raises the possibility of scalability for big datasets. To confirm its efficacy in actual fraud detection settings, more investigation and optimisation are necessary.

Bahnsen et al. [6] provide a system that uses periodic-based features to improve the identification of credit card fraud. Specifically, they use the von Mises distribution to analyse transaction time behaviour. Savings with this method are 13% higher than with previous approaches. Nevertheless, adding these recurring features could make the current systems more complicated. Raw transactional data, aggregated data, extended aggregated features, and periodic-based features produced by examining transaction time patterns are examples of key data characteristics. Assessment metrics centre on the "savings measure," which exhibits an average 13% rise upon integration of the suggested periodic features. The application of machine learning techniques and the comparison of different feature sets suggest possible scalability to handle significant transaction volumes efficiently, even though scalability isn't expressly stated.

El Kafhali et al. [7] explore the crucial area of credit card fraud detection with the goal of improving the precision and dependability of the system. In order to optimise hyperparameters, their research investigates the effectiveness of three deep learning architectures: ANN, LSTM, and RNN, which are enhanced using Bayesian optimisation. Bayesian optimisation refines these models methodologically; among several iterations, RNN is the best performer, exhibiting higher accuracy and AUC scores than ANN and LSTM. Transaction amounts, time periods, and 28 other parameters that are modified using Principal Component Analysis (PCA) are used as main features in a European credit card dataset. The need for more study is highlighted by the hurdles in scalability and adaptation to emerging fraud strategies, despite encouraging results.

Fiore et al. [8] address imbalanced datasets and offer a novel way to improve credit card fraud detection. They create enhanced training datasets by combining artificial instances of minority class data with original sets using Generative Adversarial Networks (GANs). The experimental results show a considerable increase in classifier sensitivity, which is important for identifying fraud. This method not only improves the identification of credit card fraud but also has potential applications in other industries that deal with unbalanced data. Subsequent investigations seek to enhance GAN structures for better synthetic example production, supporting efforts to combat financial fraud and boosting confidence in online transactions.

For the purpose of identifying transaction fraud, Poojitha and Malathi [9] suggest using machine learning, more especially the K-Nearest Neighbour (KNN) algorithm. The study uses under-sampling strategies to handle imbalanced data by comparing KNN with Logistic Regression (LR) and evaluating accuracy using the F1-Measure score. The results clearly demonstrate KNN's superiority, with a 99.4% accuracy rate compared to 99.1% for LR. While T-Test findings are not statistically significant, KNN shows resilience in fraud detection by using its capacity to identify the K-Nearest point to classify fresh transactions. The effectiveness of KNN in lowering false alarms and improving accuracy in fraud detection scenarios is highlighted in the paper.

The Neural Aggregate Generator (NAG), a state-of-the-art neural network module designed to automate feature extraction for fraud categorization in electronic payments, is presented by Ghosh Dastidar et al. [10]. NAG improves interpretability and performance by closely imitating hand feature aggregates, in contrast to previous techniques. NAG beats LSTM or generic CNNs in fraud classification tasks and outperforms manual aggregation through the use of soft feature value matching and relative weighting. A comparative study using real-world data highlights how effective NAG is with less parameters needed. Moreover, NAG improves interpretability by means of parameter examination, offering more profound understanding of the procedures involved in detecting electronic payment fraud.

In order to protect data privacy, Aurna et al. [11] present a unique Federated Learning (FL)-based fraud detection system that trains models without disclosing private credit card information online. Four sampling strategies are used in the study to address concerns about data imbalance, using Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP), and Long Short-Term Memory (LSTM) models inside the FL framework. The suggested method's efficacy is demonstrated by the experimental findings, which show high detection rates for various models. The study illustrates the promise of privacy-preserving FL approaches in improving fraud detection and ensuring secure financial transactions in the digital era by contrasting FL-based systems with cutting-edge techniques.

Liu et al. [12] introduce the LIC Tree-LSTM model to address fraud detection in e-commerce platforms. By restructuring user behaviors into a behavior tree structure, this model captures user intentions effectively, aided by attention mechanisms and calibration methods to balance local and global intentions. With an AUC of 0.9420, the LIC Tree-LSTM outperforms baseline models. However, challenges such as scalability, computational complexity, and interpretability persist. Nonetheless, it presents a promising solution to combat fraudulent transactions and uphold online marketplace integrity, leveraging key data features like user behaviors and historical transactions for evaluation.

In order to improve accuracy and validity in financial security, Wang et al. [13] introduce a Deep-Forest based fraud detection technique that integrates the Deep-Forest algorithm with differentiation feature creation. The method seeks to distinguish between legitimate and fraudulent transactions by introducing the Individual Credibility Degree (ICD) and Group Anomaly Degree (GAD) based on transaction time. The significant imbalance in online transactions is addressed by the Deep-Forest method, which is enhanced with outlier identification mechanisms, improving the accuracy of fraud detection. Testing against a Random Forest model shows significant improvements in recall and precision rates. It provides insights into using machine learning algorithms to fight online transaction fraud, pointing out problems like imbalance ratios and under-sampling. It also suggests future research directions for improving fraud detection systems in the face of computational difficulties and fraud concealment strategies.

2.2 Unsupervised learning methods

In order to detect banking fraud in the digital sphere, Abbassi et al. [14] provide a solid architecture that combines deep learning, big data engines, and unsupervised techniques like autoencoders and extended isolation forests for real-time detection. The methodology handles imbalanced transaction fraud datasets well, achieving an exceptional F1-Score of 90-91% and displaying superior classification impacts without synthetic data processing. Transaction details and rule-based heuristics are important characteristics; autoencoders provide further features to improve accuracy. Notwithstanding the encouraging outcomes, the framework still has issues with computing costs, data privacy, and real-world deployment. Technologies such as Spark streaming enable scalability for large-scale fraud detection, but performance requires constant optimisation.

Deshpande [15] suggests improving credit card fraud detection systems to solve problems such as missed fraud identification and a high false positive rate. The approach entails fine-tuning data description bounds, incorporating new groups for Merchant Category Code (MCC) behaviour, and expanding the safe MCC list, among other tactics, to improve the model. The identification of fraudulent patterns is aided by key data elements such transaction counts and values in particular categories. Performance measurements indicate a notable improvement, such as the Fraud Identified Percentage and False Positive Rate. In order to ensure a more dependable and efficient fraud detection system, future work will involve creating hybrid models that strike a balance between security and operational efficiency in financial institutions.

2.3 Data mining techniques

Hashemi et al. [16] address the shortcomings of conventional systems against emerging fraud techniques by tackling credit card fraud using creative feature engineering and algorithmic improvements. By

DOI: 10.55041/IJSREM35603

successfully identifying fraud trends, their method, which employs the von Mises distribution for periodic transaction analysis, produces a noteworthy 13% gain in savings. They offer an all-encompassing picture of fraudulent activity by merging new and old features, such as transaction information and spending patterns. Their research also explores the topic of cost-sensitive fraud detection, utilising decision trees and evolutionary algorithms to reduce expenses while boosting accuracy. It is still difficult to maximise computing efficiency in spite of encouraging results, which highlights the importance of effective decision-making procedures in fraud detection systems.

A comprehensive case study on credit card fraud detection within a major e-commerce corporation is presented by Carneiro et al. [17], with the goal of reducing revenue loss from fraudulent transactions. With a focus on pragmatism, the research explores different approaches for detecting fraud using both automatic and manual categorization methods. It encompasses the processes of data collection, preparation, model training, and deployment in accordance with the Cross Industry Standard Process for Data Mining (CRISP-DM). The study provides a thorough understanding of fraud detection system development by merging real-world data and experiences. It tackles deployment issues and offers suggestions for further study, making it an invaluable tool for e-commerce fraud prevention practitioners and researchers.

2.4. Other methods

2.4.1 Ensemble learning

Forough and Momtazi [18] offer a novel method that combines cutting-edge neural network algorithms to identify credit card fraud. To build a more potent fraud detection system, they combine Feedforward Neural Networks (FFNN) with Long Short-Term Memory (LSTM) networks and Gated Recurrent Units (GRU). Their technology can more accurately detect fraudulent activity by examining transaction history, time data, and patterns. When the model is tested using measures such as Precision, Recall, and F1-Measure, it outperforms the current models. But other applications may find the technology too complex, requiring additional study to guarantee a seamless real-world deployment..

The crucial problem of financial fraud detection in the financial sector is addressed by Almazroi and Ayub [19]. Although methods such as SMOTE and PCA are used to address feature selection constraints and data imbalance, the study notes enduring hazards such overfitting to minority classes. In order to address these issues, the study presents the RXT-J model, which improves fraud detection accuracy by utilising ensemble approaches. Broader applicability is limited, nevertheless, by generalizability issues that extend beyond the particular dataset utilised. By combining ensemble learning with an innovative classification technique, the suggested approach seeks to improve fraud detection. It highlights the importance of addressing changing fraudulent behaviour and interpretability criteria that are vital for financial institutions. Though the performance seems promising, issues with overfitting and restricted generalizability draw attention to the need for additional study to improve applicability and reliability.

2.4.2 Genetic algorithm

The urgent problem of credit card fraud is addressed by Ishu Trivedi et al. [20]. Because of its dynamic nature and rising frequency, credit card theft presents a number of issues. They suggest using Genetic Algorithm (GA) to improve fraud detection by streamlining the detection procedure, which lowers false alarms and raises accuracy levels overall. With the use of critical data aspects like location and frequency of credit card usage, the GA shows encouraging results in reducing risks for banks and customers. To strengthen fraud detection systems for practical implementation, the study does, however, recognise certain drawbacks, such as the dependence on sample data, and makes recommendations for future improvements, such as improving global fraud detection algorithms and adding variable misclassification costs.

2.4.3 Swarm intelligence

The S-AEKELM-DA approach, developed by Fatima Zohra El Hlouli et al. [21], integrates the Dandelion Algorithm for optimisation and Kernel Extreme Learning Machine (ELM) with Stacked Autoencoder (AE) to address the key challenge of credit card fraud detection. Enhancing prediction performance and robustness in handling imbalanced datasets is the goal of this strategy. Tested on multiple datasets such as credit card client defaults, loan prediction, and Australian and German numerical data, the approach shows better accuracy, precision, recall, F1-score, and AUC than more conventional models like BPN, GP, and SVM. Although promising for detecting fraud in the real world, implementation complexity and knowledge needs provide hurdles that necessitate additional validation across a variety of fraud situations and datasets.

2.4.4 Hybrid system (both supervised and unsupervised learning)

A hybrid machine learning approach is presented by Olena Vynokurova, Vadim Ilyasov, Dmytro Peleshko, Vladislav Serzhantov, Oleksandr Bondarenko, and Marta Peleshko from Lviv State University of Life Safety [22] in order to handle the issues associated with fraud detection in electronic transactions. This method combines the use of Random Forest for anomaly type interpretation with Isolation Forest for anomaly detection. The hybrid approach tries to improve accuracy and interpretability, while traditional rule-based systems suffer from issues including reduced system speed with large rule sets and rely on expert knowledge. Notwithstanding several limitations, such as expensive expansion, the system's effective fusion of supervised and unsupervised learning approaches makes it a promising real-time fraud detection tool.

3. CONCLUSION

Conclusively, the wide range of approaches and advancements exhibited in the scrutinised articles provide significant perspectives into the intricate field of financial transaction fraud detection. Together, these findings highlight how important it is to use cutting-edge technologies, such as neural networks, machine learning algorithms, and hybrid models, to successfully counteract the ever-evolving nature of fraudulent activities. According to the research, combining state-of-the-art methods like ensemble learning, deep learning, and genetic algorithms can greatly increase the accuracy of fraud detection and lower false positives. For example, using sophisticated feature engineering and Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), and Feedforward Neural Networks (FFNN) networks together show encouraging results in detecting fraudulent patterns in transaction data.

Furthermore, combining supervised techniques like Random Forest with unsupervised techniques like Isolation Forest and Kernel Extreme Learning Machine (ELM) emphasises the value of a hybridised strategy in tackling the problems caused by unbalanced datasets and developing fraud strategies. The studies also stress how important feature engineering, model optimisation, and interpretability are to creating reliable fraud detection systems. While offering insights into fraudulent behaviours, techniques including attention processes, ensemble learning, and periodic-based feature analysis help to increase detection accuracy.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Dr. Sagar B M for his invaluable guidance, unwavering support, and insightful feedback throughout the course of this research. His expertise and encouragement have been instrumental in shaping the direction and quality of this work.

I am also deeply thankful to R V College of Engineering for providing the necessary resources and conducive environment for conducting this research. The academic atmosphere and facilities at the college have greatly contributed to the success of this endeavor.

Lastly, I extend my heartfelt thanks to all those who have directly or indirectly contributed to this research project

REFERENCES

[1] Thennakoon, Anuruddha, Chee Bhagyani, Sasitha Premadasa, Shalitha Mihiranga, and Nuwan Kuruwitaarachchi. "Real-time credit card fraud detection using machine learning." In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 488-493. IEEE, 2019.

[2] Cheng, Dawei, Sheng Xiang, Chencheng Shang, Yiyi Zhang, Fangzhou Yang, and Liqing Zhang. "Spatio-temporal attention-based neural network for credit card fraud detection." In *Proceedings of the AAAI conference on artificial intelligence*, vol. 34, no. 01, pp. 362-369. 2020.

[3] AbdulSattar, Khadija, and Mustafa Hammad. "Fraudulent transaction detection in FinTech using machine learning algorithms." In *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, pp. 1-6. IEEE, 2020.

[4] Bagga, Siddhant, Anish Goyal, Namita Gupta, and Arvind Goyal. "Credit card fraud detection using pipeling and ensemble learning." *Procedia Computer Science* 173 (2020): 104-112.

[5] Ghosh Dastidar, Kanishka, Johannes Jurgovsky, Wissam Siblini, and Michael Granitzer. "NAG: neural feature aggregation framework for credit card fraud detection." *Knowledge and Information Systems* 64, no. 3 (2022): 831-858.

[6] Bahnsen, Alejandro Correa, Djamila Aouada, Aleksandar Stojanovic, and Björn Ottersten. "Feature engineering strategies for credit card fraud detection." *Expert Systems with Applications* 51 (2016): 134-142.

[7] El Kafhali, Said, Mohammed Tayebi, and Hamza Sulimani. "An Optimized Deep Learning Approach for Detecting Fraudulent Transactions." *Information* 15, no. 4 (2024): 227.

[8] Fiore, Ugo, Alfredo De Santis, Francesca Perla, Paolo Zanetti, and Francesco Palmieri. "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection." *Information Sciences* 479 (2019): 448-455.

[9] Poojitha, S., and K. Malathi. "An Original Approach to Identify the Better Accuracy in Credit Card Fraud Transaction by Comparing Logistic Regression with K-Nearest Neighbours Algorithm." In *2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, pp. 6-11. IEEE, 2022.

[10] Ghosh Dastidar, Kanishka, Johannes Jurgovsky, Wissam Siblini, and Michael Granitzer. "NAG: neural feature aggregation framework for credit card fraud detection." *Knowledge and Information Systems* 64, no. 3 (2022): 831-858.

[11] Almazroi, Abdulwahab Ali, and Nasir Ayub. "Online Payment Fraud Detection Model Using Machine Learning Techniques." *IEEE Access* 11 (2023): 137188-137203.

[12] Liu, Can, Qiwei Zhong, Xiang Ao, Li Sun, Wangli Lin, Jinghua Feng, Qing He, and Jiayu Tang. "Fraud transactions detection via behavior tree with local intention calibration." In *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pp. 3035-3043. 2020.

[13] Wang, Lizhi, Zhaohui Zhang, Xiaobo Zhang, Xinxin Zhou, Pengwei Wang, and Yongjun Zheng. "A Deep-forest based approach for detecting fraudulent online transaction." In *Advances in computers*, vol. 120, pp. 1-38. Elsevier, 2021.

[14] Abbassi, Hanae, Saida El Mendili, and Youssef Gahi. "Real-Time Online Banking Fraud Detection Model by Unsupervised Learning Fusion." *HighTech and Innovation Journal* 5, no. 1 (2024): 185-199.

[15] Deshpande, Poonam Manish. "Fraud Detection in Debit Card Transactions." Assistant Professor, Department of Humanities and Applied Science (Mathematics), Atharva College of Engineering, Malad (W), Mumbai-400095, India.

[16] Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. "Fraud detection in banking data by machine learning techniques." *IEEE Access* 11 (2022): 3034-3043.

[17] Carneiro, Nuno, Gonçalo Figueira, and Miguel Costa. "A data mining based system for credit-card fraud detection in e-tail." *Decision Support Systems* 95 (2017): 91-101.

[18] Forough, Javad, and Saeedeh Momtazi. "Ensemble of deep sequential models for credit card fraud detection." *Applied Soft Computing* 99 (2021): 106883.

[19] Almazroi, Abdulwahab Ali, and Nasir Ayub. "Online Payment Fraud Detection Model Using Machine Learning Techniques." *IEEE Access* 11 (2023): 137188-137203.

[20] Trivedi, Ishu, and Mrigya Mridushi Monika. "Credit card fraud detection." *International Journal of Advanced Research in Computer and Communication Engineering* 5, no. 1 (2016): 39-42.

[21] El Hlouli, Fatima Zohra, Jamal Riffi, Mhamed Sayyouri, Mohamed Adnane Mahraz, Ali Yahyaouy, Khalid El Fazazy, and Hamid Tairi. "Detecting Fraudulent Transactions Using Stacked Autoencoder Kernel ELM Optimized by the Dandelion Algorithm." *Journal of Theoretical and Applied Electronic Commerce Research* 18, no. 4 (2023): 2057-2076.

[22] Vynokurova, Olena, Dmytro Peleshko, Oleksandr Bondarenko, Vadim Ilyasov, Vladislav Serzhantov, and Marta Peleshko. "Hybrid machine learning system for solving fraud detection tasks." In *2020 IEEE Third International Conference on Data Stream Mining & Processing (DSMP)*, pp. 1-5. IEEE, 2020.