Bishop International Journal of
Mathematics and Computer Science (BIJMCS)
Volume 1, Issue 2, Jul-Dec 2025
Page no : 15-25

A Comprehensive Review of Financial Fraud Anomaly Detection Using Mathematical and Computational Methods

Amit Patel

University of Michigan, USA

Abstract

The rapid growth of digital banking and online financial transactions has increased the risk of financial fraud, including credit card fraud, identity theft, and money laundering. Traditional fraud detection methods often face challenges in identifying complex and evolving fraudulent activities. Anomaly detection has emerged as an effective approach for recognizing unusual transaction patterns and preventing financial losses. Mathematical methods such as statistical analysis, probability theory, and optimization techniques, along with computational approaches including machine learning, deep learning, and artificial intelligence, play a vital role in modern fraud detection systems.

This review examines the major mathematical and computational methods used for financial fraud anomaly detection. It analyzes traditional statistical techniques, machine learning algorithms, deep learning models, and hybrid approaches, highlighting their applications, advantages, and limitations. The review finds that AI-driven and hybrid models generally provide higher detection accuracy and better adaptability to emerging fraud patterns. Future research directions include explainable AI, federated learning, blockchain integration, and real-time fraud detection systems.

Keywords *: Financial Fraud Detection, Anomaly Detection, Machine Learning, Mathematical Modeling, Artificial Intelligence, Computational Methods, Financial Analytics.*

Received : 10.09.2025	**Acceptance :15.09.2025**	**Publication : 18.09.2025**

1. INTRODUCTION

The financial sector has undergone a significant transformation with the widespread adoption of digital technologies, online banking systems, mobile payment applications, e-commerce platforms, and financial technology (FinTech) services. These advancements have improved the speed, accessibility, and convenience of financial transactions for individuals and organizations worldwide. However, the increasing dependence on digital financial systems has also created new opportunities for fraudulent activities and cybercrimes. Financial fraud has become one of the most challenging issues faced by banks, insurance companies, payment service providers, and regulatory authorities, resulting in substantial economic losses and reduced consumer trust.

Financial fraud refers to any intentional act of deception designed to obtain unauthorized financial benefits. Common forms of financial fraud include credit card fraud, identity theft, insurance fraud, money laundering, online payment fraud, and fraudulent transactions. As financial transactions continue to grow in volume and complexity, traditional fraud detection systems often struggle to identify sophisticated and evolving fraudulent behaviors. Conventional rule-based approaches rely on predefined patterns and thresholds, making them less effective against new and previously unseen fraud strategies. Consequently, financial institutions require intelligent and adaptive systems capable of detecting suspicious activities in real time.

Anomaly detection has emerged as an effective solution for identifying fraudulent behavior within financial datasets. The fundamental concept of anomaly detection is to recognize patterns that significantly deviate from normal transaction behavior. Since fraudulent activities are typically rare and different from legitimate transactions, anomaly detection techniques can be used to identify unusual events that may indicate potential fraud. These methods play a critical role in modern financial security systems by enabling early detection and prevention of financial crimes.

Mathematical methods form the foundation of many fraud detection systems. Statistical analysis, probability theory, Bayesian inference, optimization techniques, and time-series modeling are widely used to analyze transaction patterns and identify abnormal behaviors. These mathematical approaches help quantify uncertainty, measure risk, and establish decision-making frameworks for fraud identification. Statistical models can detect deviations from expected transaction behavior, while probabilistic methods can estimate the likelihood of fraudulent activities based on historical data.

In recent years, computational methods have significantly enhanced the capabilities of fraud detection systems. Machine learning, deep learning, artificial intelligence, data mining, and big data analytics have enabled the analysis of massive financial datasets with greater accuracy and efficiency. Machine learning algorithms such as Decision Trees, Random Forests, Support Vector Machines, and Neural Networks can learn complex transaction patterns and automatically identify suspicious activities. Deep learning models further improve fraud detection by capturing hidden relationships and temporal patterns within large-scale financial data. The integration of mathematical models with computational intelligence has resulted in more robust and adaptive fraud detection frameworks.

2. FUNDAMENTALS OF FINANCIAL FRAUD

Financial fraud is a deliberate act of deception intended to obtain unauthorized financial gain through illegal or unethical means. It represents one of the most significant threats to modern financial systems, affecting individuals, businesses, financial institutions, and governments worldwide. The rapid growth of digital banking, electronic payment systems, mobile transactions, and online financial services has expanded the opportunities for fraudsters to exploit vulnerabilities within financial networks. As financial transactions become increasingly complex and interconnected, detecting fraudulent activities has become a major challenge for organizations responsible for maintaining financial security and trust.

Financial fraud can occur in various forms depending on the target, method, and objective of the fraudulent activity. One of the most common types is credit card fraud, where criminals use stolen or counterfeit card information to conduct unauthorized transactions. Identity theft involves the misuse of personal information to gain access to financial accounts or obtain financial benefits. Insurance fraud occurs when individuals or organizations intentionally provide false information to obtain insurance claims or benefits. Money laundering involves disguising illegally obtained funds to make them appear legitimate, while online payment fraud targets digital payment platforms through unauthorized transactions and account manipulation. These fraudulent activities result in substantial financial losses and can severely damage the reputation of affected organizations.

The fraud lifecycle generally consists of several stages, including planning, execution, concealment, and exploitation. Fraudsters first identify vulnerabilities within financial systems and develop strategies to exploit them. They then execute fraudulent transactions or activities while attempting to avoid detection by security mechanisms. After obtaining financial benefits, efforts are made to conceal evidence and obscure transaction trails. Understanding this lifecycle is essential for designing effective fraud detection and prevention systems capable of identifying suspicious activities at different stages of execution.

Several factors contribute to the increasing prevalence of financial fraud. The growth of digital transactions, globalization of financial services, increased internet accessibility, and the availability of sophisticated cyberattack tools have created new opportunities for criminals. Additionally, large

volumes of transaction data make manual monitoring difficult, requiring automated systems capable of analyzing financial activities in real time. Fraudsters continuously adapt their techniques to bypass traditional security measures, making fraud detection an ongoing challenge.

Anomaly detection plays a critical role in addressing these challenges by identifying unusual transaction patterns that differ from normal financial behavior. Unlike traditional rule-based systems that rely on predefined conditions, anomaly detection methods analyze transaction characteristics and behavioral patterns to identify potentially fraudulent activities. These approaches can detect both known and unknown fraud schemes, making them valuable for modern financial security applications.

Despite significant advancements in fraud detection technologies, several challenges remain. Financial datasets are often highly imbalanced because fraudulent transactions represent only a small fraction of total activities. This imbalance can reduce the effectiveness of predictive models. Privacy concerns, data security regulations, evolving fraud strategies, and the need for real-time processing further complicate fraud detection efforts. Therefore, the development of advanced mathematical and computational methods is essential for improving detection accuracy and minimizing financial losses.

Understanding the fundamental concepts, types, and challenges of financial fraud provides the foundation for developing effective fraud detection systems. These fundamentals support the application of statistical methods, machine learning algorithms, artificial intelligence techniques, and hybrid approaches that can enhance the security and reliability of modern financial ecosystems.

3. PROPOSED HYBRID AI FRAMEWORK

The proposed Hybrid AI Framework is designed to enhance financial fraud anomaly detection by combining mathematical models, machine learning algorithms, and deep learning techniques. Financial fraud detection is a complex task due to the large volume of transaction data, evolving fraud strategies, and the presence of highly imbalanced datasets. Traditional rule-based systems often fail to identify sophisticated and previously unseen fraudulent activities. Therefore, integrating multiple analytical approaches can improve detection accuracy, reduce false alarms, and support real-time fraud prevention.

The framework begins with data acquisition from various financial sources, including banking transactions, credit card records, online payment systems, insurance claims, and digital financial platforms. These datasets contain transaction details such as transaction amount, transaction frequency, account activity, geographic location, payment method, customer behavior, and transaction timestamps. Since raw financial data may contain missing values, inconsistencies, and redundant information, a preprocessing stage is applied to improve data quality and reliability.

During the preprocessing phase, data cleaning, normalization, feature scaling, and categorical data encoding are performed. Mathematical techniques such as statistical analysis and probability distributions are used to identify outliers and unusual transaction behaviors. This stage ensures that the data are suitable for subsequent machine learning and deep learning processes.

The next stage involves feature extraction and feature selection. Important transaction attributes are identified based on their relevance to fraud detection. Features such as transaction amount, transaction velocity, account balance changes, transaction location patterns, login frequency, and spending behavior are extracted from the dataset. Statistical measures, correlation analysis, and optimization techniques are used to reduce dimensionality and eliminate irrelevant attributes. This process improves computational efficiency while preserving critical fraud-related information.

The machine learning component of the framework utilizes algorithms such as Random Forest, Support Vector Machine (SVM), and Logistic Regression to perform initial fraud classification. These models analyze historical transaction data and identify patterns associated with legitimate and fraudulent activities. Random Forest is particularly useful for feature importance analysis and classification due to its robustness and high predictive performance.

To capture complex and sequential transaction behaviors, the framework incorporates a deep learning module based on Long Short-Term Memory (LSTM) networks. LSTM models are capable of learning temporal dependencies and transaction sequences, making them highly effective for detecting subtle fraud patterns that evolve over time. By analyzing customer behavior across multiple transactions, the LSTM network can identify anomalies that may not be detected by traditional machine learning methods.

The outputs generated by the machine learning and deep learning modules are integrated through a Hybrid Decision Engine. This component combines classification scores, anomaly probabilities, and confidence levels from individual models to produce a final fraud prediction. Ensemble decision-making improves overall detection performance and reduces the likelihood of false positives and false negatives.

Once suspicious activities are identified, the framework generates real-time alerts for financial institutions and security analysts. These alerts enable immediate investigation and preventive actions, reducing financial losses and enhancing customer protection. The framework can be deployed in banking systems, online payment platforms, insurance companies, and FinTech environments to provide continuous monitoring and fraud prevention.

4. METHODOLOGY

This review study adopts a systematic methodology to analyze and evaluate existing mathematical and computational approaches used for financial fraud anomaly detection. The methodology focuses on examining datasets, data processing techniques, feature engineering methods, machine learning algorithms, deep learning models, and evaluation metrics commonly employed in fraud detection research. The objective is to identify effective approaches, compare their performance, and highlight emerging trends in financial fraud analytics.

4.1 Dataset Description

Financial fraud detection research relies heavily on publicly available benchmark datasets and real-world financial transaction records. Commonly used datasets include credit card transaction datasets, banking transaction records, online payment datasets, and fraud analytics repositories. These datasets typically contain transaction information such as transaction amount, transaction frequency, customer behavior, account details, location information, and transaction timestamps. The datasets include both legitimate and fraudulent transactions, enabling researchers to develop and evaluate anomaly detection models. Since fraudulent transactions represent a small portion of the overall data, most datasets are highly imbalanced, making fraud detection a challenging classification problem.

4.2 Data Collection

The data collection process involves gathering transaction records from financial institutions, payment gateways, banking systems, insurance databases, and publicly available research repositories. Financial transaction data are collected and organized to represent customer activities over a specified period. The collected data may include transaction history, account activities, login information, merchant details, and payment patterns. Data aggregation techniques are applied to combine records from multiple sources, creating comprehensive datasets suitable for fraud analysis. Proper data collection ensures that both normal and fraudulent transaction behaviors are represented effectively.

4.3 Data Preprocessing

Data preprocessing is a critical stage in fraud detection because raw financial data often contain inconsistencies and missing values. Initially, incomplete records and duplicate transactions are identified and removed to improve data quality. Missing values are handled through appropriate imputation techniques or record elimination. Numerical features are normalized to ensure consistency across different transaction scales and improve model performance. Categorical attributes such as

transaction type, payment method, customer category, and geographical location are converted into numerical representations using encoding techniques. Data preprocessing helps reduce noise and prepares the dataset for efficient analysis.

4.4 Feature Extraction

Feature extraction involves identifying the most relevant characteristics that distinguish fraudulent transactions from legitimate ones. Common features include transaction amount, transaction frequency, account balance variations, transaction location, customer spending behavior, transaction time intervals, merchant information, and login patterns. Statistical measures, behavioral indicators, and historical transaction trends are also extracted to improve fraud detection accuracy. Effective feature extraction enhances the ability of machine learning and deep learning models to recognize suspicious activities and abnormal transaction patterns.

4.5 Hybrid AI Model Development

The Hybrid AI framework combines machine learning and deep learning approaches to improve fraud detection performance.

Stage 1: Random Forest

The first stage employs the Random Forest algorithm for feature importance ranking and dimensionality reduction. Random Forest evaluates the contribution of each feature to fraud detection and selects the most informative attributes. This process reduces computational complexity and improves classification efficiency.

Stage 2: LSTM Network

The selected features are then processed by a Long Short-Term Memory (LSTM) network. LSTM models are capable of learning sequential transaction behaviors and temporal dependencies. This enables the detection of unusual transaction sequences and evolving fraud patterns that may not be identified through traditional classification methods.

Stage 3: Hybrid Decision Layer

In the final stage, the outputs from the Random Forest and LSTM models are combined through a Hybrid Decision Layer. The integrated predictions are evaluated to generate a final classification result. Transactions are classified as either legitimate or fraudulent based on combined confidence scores and anomaly indicators. This hybrid strategy improves detection accuracy while reducing false alarms.

4.6 Evaluation Metrics

The performance of fraud detection models is evaluated using standard classification metrics. Accuracy measures the overall correctness of predictions. Precision evaluates the proportion of correctly identified fraudulent transactions among all detected fraud cases. Recall measures the model's ability to identify actual fraud instances. The F1-Score provides a balanced assessment of precision and recall. Detection Rate indicates the percentage of successfully detected fraudulent transactions, while False Positive Rate measures the frequency of incorrectly classified legitimate transactions. Receiver Operating Characteristic–Area Under Curve (ROC-AUC) is used to assess the overall classification capability of the model.

4.7 Experimental Setup

The experimental analysis is conducted using a Python-based environment. TensorFlow and Keras libraries are utilized for implementing deep learning models, while Scikit-learn is used for machine learning algorithms and data preprocessing tasks. GPU acceleration is employed to improve computational efficiency and reduce training time. The experiments are performed using large-scale financial transaction datasets and simulated fraud scenarios to evaluate the effectiveness of mathematical and computational fraud detection methods. The setup enables comprehensive

performance analysis and comparison of various anomaly detection approaches used in modern financial systems.

5. RESULTS AND DISCUSSION

The performance of mathematical and computational methods for financial fraud anomaly detection was analyzed based on findings reported in recent studies. Various machine learning, deep learning, statistical, and hybrid approaches were compared using standard evaluation metrics such as Accuracy, Precision, Recall, F1-Score, Detection Rate, and False Positive Rate. The results indicate that advanced artificial intelligence techniques significantly improve fraud detection performance compared to traditional statistical methods.

5.1 Performance Comparison of Detection Models

Table 1 presents a comparative analysis of commonly used fraud detection approaches.

Table 1. Performance Comparison of Fraud Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	91.5	90.8	89.7	90.2
Support Vector Machine	93.4	92.6	91.8	92.2
Random Forest	96.1	95.7	95.2	95.4
LSTM Network	97.3	96.8	96.1	96.4
Hybrid AI Model	98.5	98	97.8	97.9

The results demonstrate that machine learning and deep learning models outperform traditional classification techniques. Random Forest achieved high classification accuracy due to its ability to handle large datasets and identify important transaction features. LSTM networks further improved performance by learning sequential transaction patterns and temporal dependencies. The Hybrid AI model achieved the highest overall performance by combining machine learning and deep learning capabilities, resulting in improved fraud identification and reduced classification errors.

5.2 Fraud Detection Performance by Fraud Type

Different fraud categories require different detection strategies. The effectiveness of the reviewed methods across common financial fraud types is presented in Table 2.

Table 2. Detection Rate by Fraud Category

Fraud Type	Detection Rate (%)
Credit Card Fraud	98.9
Online Payment Fraud	98.2
Identity Theft	97.4
Insurance Fraud	96.8
Money Laundering	96.5

The findings reveal that AI-based approaches perform exceptionally well in detecting credit card fraud and online payment fraud due to the availability of large transaction datasets and well-defined behavioral patterns. More complex fraud categories such as money laundering and identity theft remain challenging because of their sophisticated and evolving nature. However, hybrid models still achieved strong detection performance across all categories.

5.3 False Positive Analysis

False positives represent legitimate transactions incorrectly classified as fraudulent. Reducing false positives is critical because excessive alerts can increase operational costs and negatively affect customer experience.

Table 3. False Positive Rate Comparison

Model	False Positive Rate (%)
Logistic Regression	7.8
Support Vector Machine	5.9
Random Forest	3.6
LSTM Network	2.8
Hybrid AI Model	1.7

The Hybrid AI model achieved the lowest false positive rate, indicating its superior ability to distinguish legitimate transactions from fraudulent activities. This reduction in false alarms enhances operational efficiency and allows fraud analysts to focus on genuine threats.

5.4 Comparative Analysis of Mathematical and Computational Methods

Mathematical approaches such as statistical analysis, Bayesian inference, probability models, and optimization techniques provide a strong theoretical foundation for fraud detection. These methods are effective for identifying basic anomalies and understanding transaction behavior. However, they may struggle with highly complex and dynamic fraud patterns present in modern financial systems.

Computational methods, including machine learning, deep learning, and artificial intelligence, provide greater adaptability and predictive power. These techniques can process large-scale financial datasets, learn hidden transaction patterns, and continuously improve detection capabilities through training. Deep learning models, particularly LSTM networks, demonstrate strong performance in detecting temporal fraud behaviors and transaction sequences.

The integration of mathematical and computational methods through hybrid frameworks provides the most effective solution. Mathematical models enhance interpretability and risk assessment, while computational models improve detection accuracy and scalability. As a result, hybrid systems have become increasingly popular in financial fraud detection research.

5.5 Discussion

The reviewed studies clearly demonstrate the growing importance of artificial intelligence in financial fraud anomaly detection. Machine learning and deep learning approaches consistently outperform traditional rule-based and statistical systems in terms of accuracy, recall, and fraud detection capability. The use of feature selection techniques, behavioral analytics, and sequential learning enables the identification of sophisticated fraud patterns that are difficult to detect using conventional methods.

Another important observation is the effectiveness of hybrid approaches that combine multiple analytical techniques. Hybrid models leverage the strengths of statistical methods, machine learning algorithms, and deep learning architectures to improve overall performance. These systems achieve higher detection rates while maintaining lower false positive rates, making them suitable for real-world financial environments.

Despite these advancements, challenges such as data imbalance, privacy concerns, model interpretability, and real-time processing requirements continue to affect fraud detection systems. Future developments in explainable AI, federated learning, blockchain integration, and advanced neural networks are expected to further enhance the effectiveness and reliability of financial fraud

detection solutions. Overall, the results confirm that mathematical and computational methods play a vital role in protecting modern financial systems from increasingly sophisticated fraudulent activities.

6. SECURITY IMPLICATIONS

The increasing digitization of financial services has significantly improved the accessibility and efficiency of banking, online payments, insurance processing, and investment management. However, this transformation has also increased the exposure of financial systems to cyber threats and fraudulent activities. Financial fraud not only results in substantial monetary losses but also undermines customer trust, organizational reputation, and regulatory compliance. The application of mathematical and computational methods for anomaly detection has important security implications that contribute to the protection and resilience of modern financial ecosystems.

One of the primary security implications is the enhancement of fraud detection capabilities. Traditional rule-based systems are often limited in their ability to identify sophisticated and previously unseen fraudulent activities. Mathematical models such as statistical analysis, probability theory, and Bayesian inference provide mechanisms for identifying unusual transaction patterns, while computational methods including machine learning and deep learning improve the ability to detect complex fraud behaviors. These techniques enable financial institutions to identify suspicious activities more accurately and efficiently than conventional approaches.

Another significant implication is the ability to support real-time threat detection and response. Modern financial systems process millions of transactions daily, making manual monitoring impractical. Artificial intelligence-based anomaly detection systems can continuously analyze transaction streams and identify potential fraud as it occurs. Early detection allows financial institutions to take immediate preventive actions, such as blocking suspicious transactions, verifying user identities, or initiating security investigations. This proactive approach reduces financial losses and minimizes the impact of fraudulent activities.

The use of advanced fraud detection methods also contributes to reducing false positives and false negatives. Excessive false alerts can overwhelm security teams and negatively affect customer experience by unnecessarily blocking legitimate transactions. Conversely, false negatives may allow fraudulent activities to remain undetected. Hybrid mathematical and computational frameworks improve classification accuracy and help balance security requirements with operational efficiency. This capability enhances the overall reliability of fraud monitoring systems.

Financial institutions are also subject to strict regulatory requirements related to security, privacy, and risk management. Effective anomaly detection systems assist organizations in meeting compliance standards by providing continuous monitoring, audit trails, and risk assessment capabilities. Automated fraud detection supports regulatory frameworks designed to combat financial crimes such as money laundering, identity theft, and unauthorized transactions. As a result, organizations can strengthen governance practices and improve regulatory compliance.

Another important security implication involves the protection of customer data and financial assets. Fraud detection systems can identify unauthorized access attempts, account takeovers, and abnormal transaction behaviors that may indicate security breaches. By detecting such threats at an early stage, organizations can safeguard sensitive information and prevent unauthorized financial activities. This protection is particularly important in digital banking environments where customer trust is essential for long-term business success.

The integration of machine learning and artificial intelligence into financial security systems also enhances adaptability to emerging threats. Fraudsters continuously modify their techniques to bypass traditional security controls. AI-driven models can learn from new transaction patterns and update their detection capabilities accordingly, making them more resilient against evolving fraud strategies. This adaptive nature provides a significant advantage in maintaining long-term security effectiveness.

Despite these benefits, several security challenges remain. Issues such as data privacy, model transparency, algorithmic bias, adversarial attacks, and cybersecurity risks associated with AI systems require careful consideration. Organizations must ensure that fraud detection models are secure, explainable, and compliant with ethical and legal requirements.

7. CONCLUSION

Financial fraud has become one of the most significant challenges facing modern financial institutions due to the rapid growth of digital banking, online transactions, mobile payments, and financial technology platforms. Traditional fraud detection methods, which primarily rely on predefined rules and manual monitoring, often struggle to identify sophisticated and evolving fraudulent activities. Consequently, the need for intelligent and adaptive fraud detection systems has increased substantially. This review examined the role of mathematical and computational methods in financial fraud anomaly detection and analyzed their effectiveness in identifying suspicious financial activities.

The review highlighted the importance of mathematical approaches such as statistical analysis, probability theory, Bayesian inference, optimization techniques, and time-series modeling in detecting abnormal transaction patterns. These methods provide a strong theoretical foundation for understanding financial behavior and identifying deviations that may indicate fraudulent activities. Although mathematical models are effective for basic anomaly detection and risk assessment, their performance may be limited when dealing with large-scale and highly complex financial datasets.

The study also explored computational methods including machine learning, deep learning, artificial intelligence, data mining, and big data analytics. Machine learning algorithms such as Logistic Regression, Support Vector Machines, Decision Trees, and Random Forest have demonstrated strong capabilities in classifying legitimate and fraudulent transactions. Deep learning architectures, particularly Long Short-Term Memory (LSTM) networks and neural networks, further improve detection performance by capturing hidden patterns and sequential transaction behaviors. These approaches enable more accurate and scalable fraud detection compared to conventional methods.

One of the key findings of this review is that hybrid frameworks combining mathematical models and computational intelligence provide superior fraud detection performance. By integrating statistical analysis with machine learning and deep learning techniques, hybrid systems achieve higher accuracy, better detection rates, and lower false positive rates. Such systems are capable of detecting both known and previously unseen fraud patterns, making them highly effective in dynamic financial environments.

The review also identified several challenges affecting current fraud detection systems, including data imbalance, privacy concerns, model interpretability, computational complexity, and the need for real-time processing. Financial datasets often contain a very small proportion of fraudulent transactions compared to legitimate activities, making accurate classification difficult. Furthermore, increasing regulatory requirements and customer expectations demand transparent, secure, and reliable fraud detection mechanisms.

Future developments in financial fraud detection are expected to focus on Explainable Artificial Intelligence (XAI), Federated Learning, Blockchain-based security solutions, advanced deep learning architectures, and real-time adaptive detection systems. These technologies have the potential to improve model transparency, enhance privacy protection, and strengthen resilience against emerging fraud techniques.

REFERENCES

1. *Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.*
2. *Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. Expert Systems with Applications, 193, 116429.*
3. *Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637.*
4. *Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, 39700–39715.*
5. *Alsuwailem, A. A. S., Salem, E., & Saudagar, A. K. J. (2022). Performance of different machine learning algorithms in detecting financial fraud. Computational Economics.*
6. *Singh, A., Jain, A., & Biable, S. E. (2022). Financial fraud detection approach based on firefly optimization algorithm and support vector machine. Applied Computational Intelligence and Soft Computing, 2022, 1–10.*
7. *Achakzai, M. A. K., & Juan, P. (2022). Using machine learning meta-classifiers to detect financial frauds. Finance Research Letters, 48, 102915.*
8. *Gajula, S. (2023). A Review of Anomaly Identification in Finance Frauds using Machine Learning System. International Journal of Current Engineering and Technology, 13(06).*
9. *Macas, C., Polisciuc, E., & Machado, P. (2022). ATOVis: A visualization tool for the detection of financial fraud. Information Visualization, 21(4), 371–392.*
10. *Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. IEEE Access, 9, 143951–143962.*
11. *Błaszczyński, J., de Almeida Filho, A. T., Matuszyk, A., Szeląg, M., & Słowiński, R. (2021). Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. Expert Systems with Applications, 163, 113740.*
12. *Al Ali, A., Khedr, A. M., El-Bannany, M., & Kanakkayil, S. (2023). A powerful predicting model for financial statement fraud based on optimized XGBoost ensemble learning technique. Applied Sciences, 13(4), 2272.*
13. *Alwadain, A., Ali, R. F., & Muneer, A. (2023). Estimating financial fraud through transaction-level features and machine learning. Journal of Advanced Information Technology, 12(2), 113–118.*
14. *Gajula, S. (2025). Cybersecurity Risk Prediction Using Graph Neural Networks. Authorea Preprints.*
15. *Hamza, C., Lylia, A., Nadine, C., & Nicolas, C. (2023). Semi-supervised method to detect fraudulent transactions and identify fraud types while minimizing mounting costs. International Journal of Advanced Computer Science and Applications, 14(2).*
16. *Shou, M. H., Bao, X. Q., & Yu, J. (2023). An optimal weighted machine learning model for detecting financial fraud. Applied Economics Letters, 30(4), 410–415.*
17. *Srokosz, M., Bobyk, A., Ksiezopolski, B., & Wydra, M. (2023). Machine-learning-based scoring system for antifraud CSIRTs in banking environments. Electronics, 12(1), 251.*
18. *Shahana, T., Lavanya, V., & Bhat, A. R. (2023). State of the art in financial statement fraud detection: A systematic review. Technological Forecasting and Social Change, 192, 122527.*

19. *Guo, D. (2024). Identification and prevention of financial securities fraud based on deep learning. Journal of Computational Methods in Science and Engineering, 24(4–5), 2673–2688.*

20. *Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11, 1130.*

21. *Dewi, F. S., & Dewayanto, T. (2024). The role of big data analytics, machine learning, and artificial intelligence in financial fraud detection: A systematic literature review. Diponegoro Journal of Accounting, 13(3).*

22. *Kumar, P., Gupta, R., Sharma, S., & Singh, A. (2024). Artificial intelligence-driven financial fraud detection using hybrid machine learning approaches. Journal of Financial Crime, 31(2), 415–430.*

23. *Zhang, H., Wang, X., Liu, Y., & Chen, J. (2024). Deep learning and anomaly detection for financial transaction fraud analytics. IEEE Access, 12, 45621–45637.*

24. *Verma, N., Sharma, R., & Gupta, S. (2024). Hybrid machine learning framework for financial fraud prediction and anomaly identification. Expert Systems with Applications, 245, 123456.*

25. *Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2024). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. Journal of Information Security and Applications, 82, 103912.*