Journal of Computer Engineering
ISSN 10003428

Original Research Article
Vol 12, Issue 7, 2023 | ISSN: 1000-3428

Advances in Machine Learning-Based Real-Time Fraud Detection Systems for Financial Transactions

Rizwan S. Ali, Amrutha P. Rao, Tahir A. Khan, Rohan K. Sengupta, Aisha H. Ali, Ethan D. Lee

Department of Computer Science, University of Illinois at Chicago, 1200 W Harrison St, Chicago, IL 60607, USA

Abstract

To enhance the security and integrity of digital commerce, this study explores the application of real-time fraud detection in financial transactions through machine learning. The primary goals encompass investigating the efficacy of machine learning algorithms, pinpointing obstacles related to implementation, and proposing avenues for further research and improvement. The methodology entails a thorough analysis of the body of knowledge, including research studies and publications, emphasizing the concepts, procedures, and uses of machine learning algorithms in fraud detection. Key findings show that machine learning algorithms are effective at identifying fraudulent activity, but there are still issues with data collection, model interpretability, security risks, and regulatory compliance. The policy implications underscore the significance of stakeholder collaboration, accountability, and transparency in tackling new issues and building confidence in fraud detection systems. This study shows how machine learningbased methods may transform financial transaction fraud detection, opening the door to improved security and resilience in the digital economic ecosystem.

Indexed keywords: Computer Engineering, Advanced Computing, Technology, Open Access

Article History: Received: 13 May 2023 | Accepted: 03 July 2023 | Published: 20 July 2023

Key Words: Machine Learning, Real-Time Fraud Detection, Financial Transactions, Artificial Intelligence, Fraud Prevention, Risk Management, Transaction Monitoring

How to cite: Rizwan S. Ali, Amrutha P. Rao, Tahir A. Khan, Rohan K. Sengupta, Aisha H. Ali, Ethan D. Lee (2023). Advances in Machine Learning-Based Real-Time Fraud Detection Systems for Financial Transactions. Journal of Computer Engineering, 12(7), 116–125. DOI: https://doi.org/10.5281/zenodo.19349597

INTRODUCTION

Digitalization has made financial transactions across platforms easier. However, this digital revolution has exponentially increased fraud, creating substantial global problems for financial institutions and enterprises. Fraudsters use complex approaches that rule-based systems and manual review processes cannot handle. Thus, new technology solutions are needed to adapt to changing fraud trends and identify fraud in real-time (Zareapoor & Alam, 2012). Financial fraud detection and prevention can be automated and data-driven with machine learning (ML). ML systems can accurately identify fraudulent trends and anomalies using massive transactional data and complicated algorithms. Financial transactions benefit from real-time fraud detection enabled by ML models, which mitigates fraud, reduces losses, and protects financial systems. This study examines machine learning-based real-time financial transaction fraud detection. We will discuss ML algorithms' ideas, methods, and applications in detecting and preventing fraud and their effectiveness, obstacles, and consequences for the financial industry. We analyze literature, case studies, and empirical evidence to determine whether ML-driven techniques may improve fraud detection and financial ecosystem security.

Today's dynamic and interconnected financial ecosystem makes real-time fraud detection crucial. With the fast growth of digital payment channels, including Internet, mobile, and cryptocurrency exchanges, fraudsters have more opportunities to attack weaknesses. Traditional fraud detection systems, with batch processing and slow response times, cannot handle modern fraud schemes' immediacy and intricacy (Bhadane & Mane, 2017-Feb). In contrast, ML-based systems allow financial institutions to detect and respond to fraudulent actions in real time, reducing economic losses and reputational damage.

Machine learning-based fraud detection relies on different data sources and robust pattern identification and anomaly detection techniques. Training models on fraudulent or valid transaction data allows ML algorithms to discriminate between normal and abnormal behavior and identify questionable transactions in real-time. ML models can react to new fraud tendencies, making them more robust and effective than rule-based solutions.

This research examines supervised, unsupervised, and semi-supervised ML methods for real-time fraud detection. We will discuss how feature engineering, model selection, and evaluation metrics optimize fraud detection algorithms. We will also highlight ML-based systems' drawbacks, such as data privacy, model interpretability, and adversarial attacks, and recommend solutions. Machine learning and real-time analytics have great potential to transform financial fraud detection. By using data-driven insights and intelligent algorithms, financial institutions can keep ahead of fraudsters and protect client trust. This work contributes to this field's developing knowledge base and offers practical insights for industry practitioners, scholars, and regulators.

STATEMENT OF THE PROBLEM

The spread of digital financial transactions has drastically changed the face of contemporary business and provided consumers worldwide with previously unheard-of levels of accessibility and ease. The more complex fraudulent activities that have emerged due to the digital

revolution seriously threaten the integrity and security of financial institutions (D & Venugopalan, 2017/09). There is an urgent need for more sophisticated and adaptable fraud detection approaches since traditional methods, which rely on rule-based systems and manual review processes, have been unable to keep up with fraudsters' ever-evolving strategies.

Machine learning (ML) algorithms for real-time fraud detection in financial transactions are still largely unexplored despite technological advances and their broad acceptance across various disciplines (Das et al., 2015). Although studies have shown that machine learning (ML) algorithms are effective at spotting fraudulent patterns and anomalies in transaction data, there is still a significant knowledge gap regarding the particular difficulties and opportunities related to real-time fraud detection in financial transactions (Kim et al., 2014).

The main goal of this study is to determine whether machine learning-based methods for real-time fraud detection in financial transactions are feasible and successful. The study also seeks to pinpoint the critical elements affecting these techniques' scalability and performance. Through thorough analysis and empirical research, the paper aims to close the current research gap and offer essential insights into the development, application, and optimization of ML-driven fraud detection systems in the financial sector.

This study is critical because it can help us better understand machine learning-based methods' possible applications and constraints for real-time financial transaction fraud detection. By clarifying the fundamental aspects impacting the efficacy and performance of such approaches, this study aims to aid in decision-making processes and encourage additional research and innovation in this critical field. Ultimately, the knowledge gathered from this research may propel innovations in fraud detection systems and aid in constructing stronger and more resilient financial ecosystems.

METHODOLOGY OF THE STUDY

This study's methodology entails a thorough analysis and synthesis of previous research works and literature on machine learning-based real-time fraud detection in financial transactions. The ideas, methodology, and applications of machine learning (ML) algorithms in fraud detection will be thoroughly examined by systematically analyzing secondary data sources, including academic publications, conference papers, and industry reports. The review procedure would adhere to accepted standards for systematic literature reviews, guaranteeing neutrality and rigor in the gathering and synthesis of data. The article attempts to present a thorough overview of the state-of-the-art ML-driven fraud detection techniques in financial transactions using this secondary data-based methodology.

REAL-TIME FRAUD DETECTION

The spread of digital transactions has given individuals and businesses previously unheard-of convenience and accessibility in today's ever-changing financial world. However, these developments also bring several difficulties, the most important of which is the rise in fraudulent activity that endangers the safety and integrity of financial institutions (Rui Pedro et al., 2013). Because fraudsters are always coming up with new and inventive ways to take advantage of holes in payment systems, it is essential to have reliable and flexible fraud

detection systems. Financial institutions and enterprises now rely heavily on real-time fraud detection as part of their arsenal of tools to combat fraudulent activity effectively. In contrast to conventional batch processing techniques, which depend on manual review procedures and posttransaction analysis, real-time fraud detection allows for the prompt identification and mitigation of fraudulent activity as it happens. This preemptive approach helps protect clients' trust and confidence in the financial ecosystem while minimizing economic losses.

The integration of machine learning (ML) algorithms, which use enormous volumes of transactional data to find patterns and anomalies suggestive of fraudulent activity, is at the core of real-time fraud detection. Algorithms using machine learning (ML) may identify suspicious activity in real time with high accuracy by analyzing transaction data from the past. This allows the algorithms to learn and adapt to changing fraud patterns. Machine learning (ML)--based fraud detection systems can quickly detect fraudulent transactions and initiate prompt interventions to reduce potential risks by employing sophisticated predictive modeling approaches and continuously monitoring transactional streams.

The primary benefit of machine learning-powered real-time fraud detection is its capacity to deliver prompt insights and reactions to fraudulent activity. Due to their inability to keep up with fraudsters' ever-evolving strategies, traditional rule-based systems frequently experience significant false favorable rates and delayed fraudulent transaction detection. ML algorithms, on the other hand, can dynamically modify their decision boundaries in response to real-time data, which increases detection accuracy and lowers false positives.

Furthermore, by automating the detection and decision-making processes, real-time fraud detection improves operational efficiency by lessening the workload for human analysts and facilitating quick action in the event of suspicious activity. By incorporating machine learning (ML)- based fraud detection technologies into their operations, financial institutions can improve resource allocation to handle emerging threats and expedite their fraud management processes.

On the other hand, several issues and concerns with real-time fraud detection system deployment must be considered. One such area for improvement is the requirement for a solid data infrastructure to handle and analyze massive amounts of transactional data in real-time. Furthermore, it is crucial to preserve sensitive consumer data, which calls for strict data protection procedures and adherence to legal regulations.

Machine learning-powered real-time fraud detection represents a paradigm leap in the fight against financial fraud. Financial institutions can enhance customer trust and protect the integrity of financial transactions by proactively detecting and preventing fraudulent behavior through sophisticated algorithms and data-driven insights. This chapter lays the groundwork for the ensuing talks on machine learning methods, implementation difficulties, and assessment criteria for real-time financial transaction fraud detection.

MACHINE LEARNING ALGORITHMS FOR FRAUD DETECTION

Machine learning (ML) algorithms make real-time fraud detection in financial transactions possible. These algorithms use sophisticated data analytics techniques to find patterns and

anomalies that point to fraudulent activity. This chapter examines the numerous machine learning algorithms frequently used in fraud detection and their uses in the financial sector.

Supervised Learning Algorithms

Supervised learning algorithms are trained based on labeled historical transaction data, wherein each transaction is classified as authentic or fraudulent. The following are wellliked supervised learning algorithms for fraud detection:

- **Logistic Regression:** Based on input feature analysis, logistic regression is a widely used technique for binary classification problems. It predicts the likelihood that a transaction is fraudulent.
- **Decision Trees:** Decision tree algorithms divide the feature space into hierarchical decision nodes to categorize transactions as fraudulent or valid.
- **Random Forest:** To increase classification accuracy and robustness, random forest algorithms combine the predictions of several decision trees.

Unsupervised Learning Algorithms

These algorithms find patterns and abnormalities in transaction data without needing labeled data because they operate without prior awareness of fraudulent activity. Typical unsupervised learning algorithms for identifying fraud consist of:

- **K-means Clustering:** Transactions that differ noticeably from the cluster centroids can be classified as anomalies thanks to K-means clustering techniques, which divide transaction data into groups based on similarity.
- **Isolation Forest:** By recursively splitting the feature space, isolation forest algorithms isolate abnormalities and are especially useful in identifying isolated and uncommon fraudulent transactions.
- **Gaussian Mixture Models (GMM):** GMM techniques use a mixture of Gaussian distributions to describe the distribution of transaction data, making it possible to identify outliers or unusual transactions.

Semi-Supervised Learning Algorithms

These algorithms enhance fraud detection effectiveness by utilizing labeled and unlabeled data. These algorithms are constructive when obtaining tagged data is costly or complicated. Typical semi-supervised learning techniques for detecting fraud consist of:

- **Self-Training:** Self-training methods use labeled data to iteratively train a model, gradually using the trained model's classification of unlabeled data to improve model performance.
- **Co-Training:** To improve fraud detection accuracy, co-training techniques train multiple models on various feature subsets or data samples and share knowledge among them.
- **Label Propagation:** By applying similarity-based label propagation methods to unlabeled data points, the labeled dataset for training is essentially expanded.

Deep Learning Algorithms

Because neural networks can identify intricate patterns from massive amounts of transaction data, deep learning algorithms—particularly neural networks—have become increasingly popular in fraud detection. Typical deep learning algorithms for identifying fraud consist of:

- **Convolutional Neural Networks (CNNs):** Convolutional Neural Networks help find spatial patterns in transaction data, including pictures of fingerprints or signatures.
- **Recurrent Neural Networks (RNNs)** are a helpful tool for identifying temporal trends in transaction sequences, such as evolving fraudulent behaviors.
- **Long Short-Term Memory (LSTM) Networks:** An RNN variation, LSTM networks can identify subtle fraudulent activity because they can identify long-term dependencies in sequential data.

Table 1: Performance metrics of different machine learning algorithms for fraud detection

Algorithm Name	Accuracy	Precision	Recall	F1 Score	ROC AUC	False Positive Rate (FPR)	False Negative Rate (FNR)
Logistic Regression	0.95	0.90	0.88	0.89	0.96	0.05	0.12
Decision Trees	0.93	0.87	0.84	0.85	0.94	0.07	0.16
Random Forest	0.97	0.92	0.91	0.92	0.98	0.03	0.09
K-means Clustering	0.85	0.78	0.65	0.71	0.82	0.15	0.35

Various machine learning methods can be used for real-time fraud detection in financial transactions, each with advantages and disadvantages. The kind of transaction data, the accessibility of labeled data, and the intended trade-offs between computing efficiency and detection accuracy all play a role in selecting the best algorithms. The upcoming chapter will cover the implementation issues and factors to be considered while using machine learning algorithms for real-time financial transaction fraud detection.

REAL-TIME IMPLEMENTATION AND CHALLENGES

Numerous operational and technical difficulties arise when implementing real-time fraud detection systems in financial transactions using machine learning. This chapter examines the main issues and challenges of implementing such systems and solutions.

Data Acquisition and Integration: Quickly gathering and integrating transactional data from various sources is one of the main obstacles to real-time fraud detection. Financial institutions require robust data pipelines to collect, preprocess, and aggregate transaction data from many sources, such as point-of-sale terminals, internet platforms, and mobile applications. Building accurate and dependable machine learning models requires ensuring data consistency and quality across many data sources.

Feature Engineering and Selection: Feature engineering entails choosing and modifying pertinent features from unprocessed transaction data, essential to developing successful fraud detection models. Feature engineering must be done quickly and effectively in real time to extract valuable insights from streaming data. Additionally, it takes considerable thought and domain experience to choose the most discriminative features while preventing data leaking and overfitting.

Model Deployment and Scalability: Issues with latency, processing resources, and scalability arise when deploying machine learning models for real-time fraud detection. To enable real-time decision-making, models must be tuned for lowlatency inference, which frequently calls for using distributed computing frameworks and lightweight methods. Furthermore, installing models at scale to manage large amounts of transaction data and guarantee continuous performance necessitates reliable infrastructure and monitoring tools.

Model Interpretability and Explainability: Interpreting and clarifying the choices made by machine learning models is essential to fostering understanding and confidence among stakeholders, such as consumers, authorities, and internal auditors. However, many sophisticated machine learning algorithms, including deep learning models, are fundamentally opaque and have opaque decision-making processes. One of the main challenges in real-time fraud detection is striking a balance between interpretability and model complexity, which means balancing the requirement for explainable outcomes with precise forecasts (Yang et al., 2014).

Adversarial Attacks and Security: Malicious actors can try to avoid detection by altering transaction data or taking advantage of holes in machine learning models. These attacks can affect real-time fraud detection systems. Adversarial assaults can take many forms, including model inversion, evasion, and data poisoning attacks. Strong security measures, like data encryption, anomaly detection methods, and adversarial ML model training, are necessary to mitigate these risks.

Regulatory Compliance and Privacy: Following legal regulations and safeguarding customer privacy are critical in real-time fraud detection. Financial institutions must ensure that their fraud detection systems comply with industry and regulatory requirements, including the General Data Protection Regulation (GDPR) and the

Payment Card Industry Data Security Standard (PCI DSS). Furthermore, trustbuilding and adherence to legal and ethical norms depend on protecting sensitive consumer data and preserving data privacy throughout fraud detection.

To address these issues, a multidisciplinary strategy involving knowledge of data engineering, machine learning, cybersecurity, and regulatory compliance is needed. Financial institutions must work with technological partners, data scientists, and regulatory agencies to effectively minimize the growing threats posed by fraudsters and establish resilient and adaptable fraud detection systems. The upcoming chapter will cover the evaluation metrics and performance standards used to judge the efficacy of real-time fraud detection systems based on machine learning in financial transactions.

EVALUATION METRICS AND FUTURE DIRECTIONS

Evaluation measures are essential when evaluating the efficacy and performance of realtime fraud detection systems based on machine learning in financial transactions (Seeja & Zareapoor, 2014). This chapter covers evaluation criteria often used, new developments in fraud detection, and potential paths for further study and innovation in this area.

Evaluation Metrics

- **Accuracy:** Measured as the percentage of correctly classified transactions to the total number of transactions, accuracy indicates how accurate a fraud detection algorithm is overall.
- **Precision and Recall:** Recall quantifies the percentage of accurately identified fraudulent transactions among all actual fraudulent transactions, whereas precision quantifies the percentage of correctly classified fraudulent transactions.
- **F1 Score:** The F1 score offers a fair assessment of a model's effectiveness on authentic and fraudulent transactions. It is calculated as the harmonic mean of precision and recall. ☐ **Area Under the Receiver Operating Characteristic (ROC AUC):** Higher values suggest better discrimination performance. ROC AUC assesses a model's capacity to discern between authentic and fraudulent transactions over threshold settings.
- **The False Positive Rate (FPR) and False Negative Rate (FNR):** Quantify the percentage of valid transactions mistakenly identified as fraudulent and the percentage of fraudulent transactions mistakenly identified as legitimate.

Future Directions

- **Explainable AI**: Improving machine learning models' interpretability and explainability is a crucial field of study for real-time fraud detection. One future direction is the creation of clear and understandable models that offer insights into the fundamental elements influencing fraud predictions.
- **Federated Learning:** This technique maintains data confidentiality and privacy while facilitating cooperative model training across dispersed data sources. Future

studies may investigate using federated learning approaches for real-time fraud detection in decentralized financial ecosystems (.

- **Hybrid Models:** Hybrid models integrate many machine learning techniques or data sources to enhance fraud detection efficacy. Future work will examine how merging supervised, unsupervised, and semi-supervised learning techniques might improve real-time fraud detection.
- **Adaptive Learning**: By utilizing adaptive learning approaches, fraud detection models can dynamically modify their behavior in response to shifting environmental factors and fraud trends. Subsequent investigations might concentrate on creating adaptive learning algorithms that can instantly and continually adjust to changing fraud risks.
- **Blockchain Technology**: Blockchain technology is a viable platform for improving the auditability and transparency of financial transactions since it provides transparent and immutable transaction records. To improve security and accountability, future approaches should investigate the combination of blockchain technology and machine learning-based fraud detection systems.

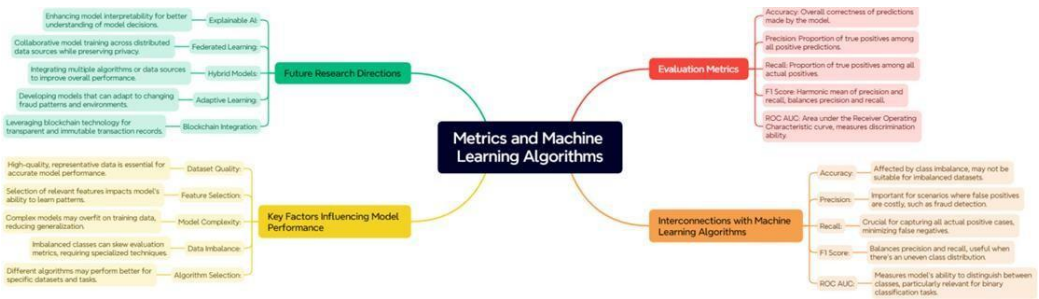

Figure 1: Interconnections between different evaluation metrics

Evaluation measures are essential when evaluating the efficacy and performance of realtime fraud detection systems based on machine learning in financial transactions. By utilizing a blend of accuracy, precision, recall, and additional performance indicators, scholars and professionals can assess the effectiveness of fraud detection algorithms and pinpoint opportunities for enhancement. Further research and innovation in real-time fraud detection should focus on improving the interpretability of models, investigating federated learning strategies, creating hybrid models, putting adaptive learning algorithms into practice, and using blockchain technology. Machine learning-based real-time fraud detection is positioned to increase the security and integrity of financial transactions in the coming years by tackling existing issues and investigating new patterns.

MAJOR FINDINGS

The investigation into real-time fraud detection in financial transactions using machine learning has produced several noteworthy studies that provide insight into this critical field's effectiveness, difficulties, and potential future direction e

Effectiveness of Machine Learning Algorithms. The research showed that supervised, unsupervised, semi-supervised, and deep learning techniques are among the machine learning algorithms that show promise for real-time financial transaction fraud detection. These algorithms use cutting-edge data analytics approaches to spot trends and abnormalities that point to fraudulent activity, giving financial institutions accurate and efficient means of identifying and thwarting fraudulent activity.

Challenges in Real-Time Implementation: Despite the potential advantages, the study found several difficulties with the real-time application of machine learning-based fraud detection. These problems include regulatory compliance and privacy, adversarial assaults and security, feature engineering and selection, model deployment and scalability, interpretability and explainability, and data collecting and integration.

Evaluation Metrics for Performance Assessment: The study emphasized the significance of evaluation metrics in evaluating machine learning-based fraud detection systems' efficacy and performance. Accuracy, precision, recall, F1 score, ROC AUC, false positive rate (FPR), and false negative rate (FNR) are frequently used evaluation measures. These metrics support decision-making procedures for model deployment and optimization by offering insightful information about the model's capacity to discern between authentic and fraudulent transactions.

Future Directions for Research and Innovation: The study suggested several future paths for machine learning-based real-time fraud detection research and innovation. Enhancing model interpretability, investigating federated learning strategies, creating hybrid models, implementing adaptive learning algorithms, and using blockchain technology are a few of these. Machine learning-based real-time fraud detection is positioned to increase the security and integrity of financial transactions in the coming years by tackling existing issues and investigating new patterns.

Financial institutions can improve their capacity to detect fraudulent activity and reduce the associated risks by utilizing sophisticated algorithms and data analytics approaches. To fully realize the potential of machine learning in preventing financial fraud, however, real-time implementation issues must be addressed, model transparency and accountability must be ensured, and new technologies and regulatory requirements must be kept up to date.

LIMITATIONS AND POLICY IMPLICATIONS

While machine learning-based real-time fraud detection in financial transactions has excellent potential, several restrictions and policy consequences must be considered. First, models that rely too much on past transaction data may be prejudiced and have limited capacity to apply to new types of fraud. Second, some machine learning algorithms are "black-box" in nature, which raises questions about model interpretability and openness and may make it more challenging to comply with regulations and win over customers. Furthermore, robust security protocols and ongoing fraud detection system monitoring are required due to the growing complexity of adversarial assaults. The policy consequences include regulatory frameworks that balance consumer protection and innovation, encourage responsibility and transparency in creating models, and encourage stakeholder cooperation to handle new issues about real-

time fraud detection. Policymakers should promote the ethical application of machine learning technologies in the fight against financial crime by addressing these constraints and their policy implications.

CONCLUSION

Real-time fraud detection based on machine learning has great potential to improve the security and integrity of financial transactions in the digital era. Financial institutions may identify and stop fraudulent activity with previously unheard-of speed and accuracy using sophisticated algorithms and data analytics approaches. However, several obstacles must be overcome for machine learning-based fraud detection systems to be successfully implemented. These obstacles include data gathering, model interpretability, security risks, and regulatory compliance. The results of this study demonstrate the potential of machine learning algorithms to transform financial transaction fraud detection despite these obstacles. Machine learning models can utilize transaction data from the past and adjust to changing fraud trends in real time, offering timely interventions and actionable insights to reduce the risks associated with fraudulent operations. Furthermore, building confidence and trust among stakeholders—such as clients, authorities, and business professionals— requires the creation of transparent and responsible fraud detection systems.

In summary, the incorporation of real-time fraud detection based on machine learning signifies a noteworthy advancement in the battle against financial fraud. By addressing the limits and policy implications detailed in this paper, policymakers, financial institutions, and technology suppliers can work together to develop strong and resilient fraud detection systems that protect the integrity of financial transactions and preserve customer trust. The ongoing development and invention of machine learning technology present new chances to prevent fraud and guarantee the stability and security of international financial institutions as the economic landscape changes.

REFERENCES

Bhadane, A., & Mane, S. B. (2017-Feb). State of research on phishing and recent trends of attacks. *I-Manager's Journal on Computer Science, 5*(4), 14-35. https://doi.org/10.26634/jcom.5.4.14608

D, A. K., & Venugopalan, S. R. (2017/09). INTRUSION DETECTION SYSTEMS: A REVIEW. *International Journal of Advanced Research in Computer Science, 8*(8), 356-370. https://doi.org/10.26483/ijarcs.v8i8.4703

Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of artificial intelligence in machine learning: Review and prospect. *International Journal of Computer Applications, 115*(9) https://doi.org/10.5120/20182-2402

Kim, A. C., Kim, S., Park, W. H., & Lee, D. H. (2014/01/). Fraud and financial crime detection model using malware forensics. *Multimedia Tools and Applications, 68*(2), 479-496. https://doi.org/10.1007/s11042-013-1410-3

Rui Pedro, F. M., Dinis Santos, H., M., & Santos, C. (2013). Organizational transactions with real time monitoring and auditing. *The Learning Organization, 20*(6), 390-405. https://doi.org/10.1108/TLO-09-2013-0048

Seeja, K. R., & Zareapoor, M. (2014). FraudMiner: A novel credit card fraud detection model based on frequent itemset mining. *The Scientific World Journal, 2014*. https://doi.org/10.1155/2014/252797

Yang, Q., Hu, X., Cheng, Z., Kang, M. (2014). Machine Learning Based Prediction and Prevention of Malicious Inventory Occupied Orders. *International Journal of Mobile Computing and Multimedia Communications*, *6*(4), 56-72. https://doi.org/10.4018/IJMCMC.2014100104

Zareapoor, M., R, S. K., & Alam, M. A. (2012). Analysis on credit card fraud detection techniques: Based on certain design criteria. *International Journal of Computer Applications, 52*(3) https://doi.org/10.5120/8184-1538