Advances in Computer Sciences
Vol. 7 (2024)
https://academicpinnacle.com/index.php/acs

Adaptive Fraud Detection Systems: Real-Time Learning from Credit Card Transaction Data

Ahmad Amjad Mir
University of Wisconsin – Madison, USA
Corresponding Author: Ahmadamjadmir@gmail.com

Abstract:

The swift growth of digital payment platforms has heightened the demand for effective fraud detection strategies, particularly within credit card transactions. Conventional static rule-based models are becoming less effective in countering the constantly evolving nature of fraudulent activities. Adaptive fraud detection systems that utilize machine learning (ML) and real-time learning methods are gaining traction as a more potent solution. This paper examines the architecture, design, and effectiveness of adaptive fraud detection systems, with a focus on real-time learning from credit card transaction data. We review existing methodologies, discuss the challenges they encounter, and propose innovative techniques to improve the adaptability of fraud detection systems in changing environments.

Keywords: Adaptive fraud detection, real-time learning, credit card transactions, machine learning, concept drift, anomaly detection.

1. Introduction:

The growing prevalence of digital payment systems has led to a significant rise in credit card usage across the globe. But the increase in digital transactions has also given fraudsters more opportunities to take advantage of holes in these systems [1]. Credit card fraud has become a substantial concern for financial institutions, merchants, and consumers, with global losses expected to exceed $32 billion by 2025. The increasing sophistication of fraudulent schemes demands that traditional fraud detection methods, often rule-based and static, be replaced by more dynamic and adaptive approaches[2].

Historically, fraud detection systems have relied on predefined rules that flag suspicious transactions based on fixed thresholds, such as unusually high

spending amounts or transactions originating from high-risk geographical regions. These solutions, while useful in some circumstances, are constrained by their incapacity to change with the always evolving fraud scenario. Fraudsters continuously develop new strategies to evade detection, rendering static rule-based systems ineffective over time[3]. This has prompted a shift toward more flexible and intelligent Systems for detecting fraud that are able to instantly recognize and adapt to new patterns.

Adaptive fraud detection systems powered by machine learning (ML) present a more effective alternative to static rule-based models. These systems examine credit card transaction data on a regular basis, looking for trends and irregularities that might point to fraud. Using methods like anomaly detection, reinforcement learning, and real-time learning, adaptive fraud detection systems are able to react quickly to emerging fraud trends. This enables financial institutions to detect and mitigate fraud more accurately and quickly, minimizing financial losses and reducing the impact on legitimate customers[4].

However, the development of adaptive fraud detection systems presents its own set of challenges. The nature of credit card transaction data, which is typically large in volume and highly imbalanced (fraudulent transactions often represent a tiny fraction of the overall data), poses difficulties in model training and evaluation. Moreover, these systems must contend with concept drift, where the statistical properties of fraudulent transactions change over time. Although there are still obstacles to overcome, adaptive fraud detection systems are an important development in the fight against credit card theft because they provide a more reliable, scalable, and rapid response to the increasing danger posed by fraudsters.

2. Conventional Techniques for Fraud Detection:

Conventional techniques for detecting fraud have mostly depended on static rule-based systems that identify possibly fraudulent transactions by using expert knowledge and predetermined thresholds. These systems establish certain guidelines, like alerting transactions that go above a predetermined threshold, take place in high-risk areas, or diverge from a customer's typical spending habits.[5]. For example, a system might block a transaction if a customer who typically spends modestly suddenly attempts a large purchase in a foreign country. While this approach is straightforward to implement, it suffers from several inherent limitations, particularly its inability to adapt to new, evolving forms of fraud.

The lack of flexibility in rule-based systems is one of its primary disadvantages. The sophistication of fraudulent tactics leads to fraudsters' quick learning how to discover ways around restrictions, either by changing their plans or by locating loopholes. As such, these algorithms are not useful for detecting new fraud trends due to their static nature[6]. Rule-based systems can also produce a lot of false positives, which flag valid transactions as fraudulent, due to their heavy reliance on past data and human intuition. This can cause customer annoyance and increase the expenses associated with manual inspection for financial institutions.

Another significant challenge associated with traditional methods is their inability to handle the sheer volume and velocity of modern credit card transactions. As online commerce grows, transaction data becomes more diverse and complex, and fraud detection systems must operate in real-time to minimize potential damage[7]. Rule-based methods are often simplistic and not designed for high-speed analysis, and they struggle to keep up with these demands. Additionally, they tend to degrade as fraudulent behavior evolves, requiring frequent updates or manual intervention to remain effective.

Despite these limitations, rule-based systems have remained a cornerstone of fraud detection for decades due to their simplicity and interpretability. Financial institutions have long favored these systems because they offer a transparent and easily auditable approach to identifying fraudulent activity. But conventional rule-based approaches are not working well enough as credit card transactions grow in number and complexity and fraud schemes become more sophisticated. This has prompted the creation of increasingly complex machine learning-based fraud detection systems with improved real-time detection capabilities and the ability to adjust to shifting transaction behaviors.

3. Proposed Adaptive Fraud Detection Systems:

Adaptive fraud detection systems represent a significant leap forward from traditional static methods by utilizing machine learning algorithms to continuously learn and evolve from incoming data. Unlike rule-based systems that rely on static, predefined thresholds, adaptive systems are designed to adjust dynamically to fresh trends and patterns in the transaction data. This adaptability is crucial in combating fraud in the quickly changing digital landscape of today, where fraudsters constantly refine their techniques[8]. The key advantage of adaptive systems lies in their ability to identify and respond to emerging fraud strategies in real time, ensuring that fraudulent activities are detected promptly while minimizing disruptions to legitimate transactions.

These systems typically employ online learning algorithms, enabling continuous model updates as new transactions occur. Algorithms such as stochastic gradient descent (SGD) and reinforcement learning play a pivotal role in updating model parameters incrementally, allowing the system to adapt to new patterns without needing full retraining on historical data[9]. This real-time learning capability ensures that adaptive systems remain effective even as transaction behaviors shift over time, preventing fraudsters from exploiting newly emerging vulnerabilities[10]. Additionally, by analyzing transaction data streams, adaptive systems can detect anomalies that may indicate fraudulent activities, even if these anomalies have never been seen before. This section will present two data-driven methods for detecting credit card fraud that make use of a T^2 control chart and a one-class support vector machine (OCSVM) with the best kernel parameter selection. Figure 1 summarizes the real-time data-driven strategies that have been proposed.

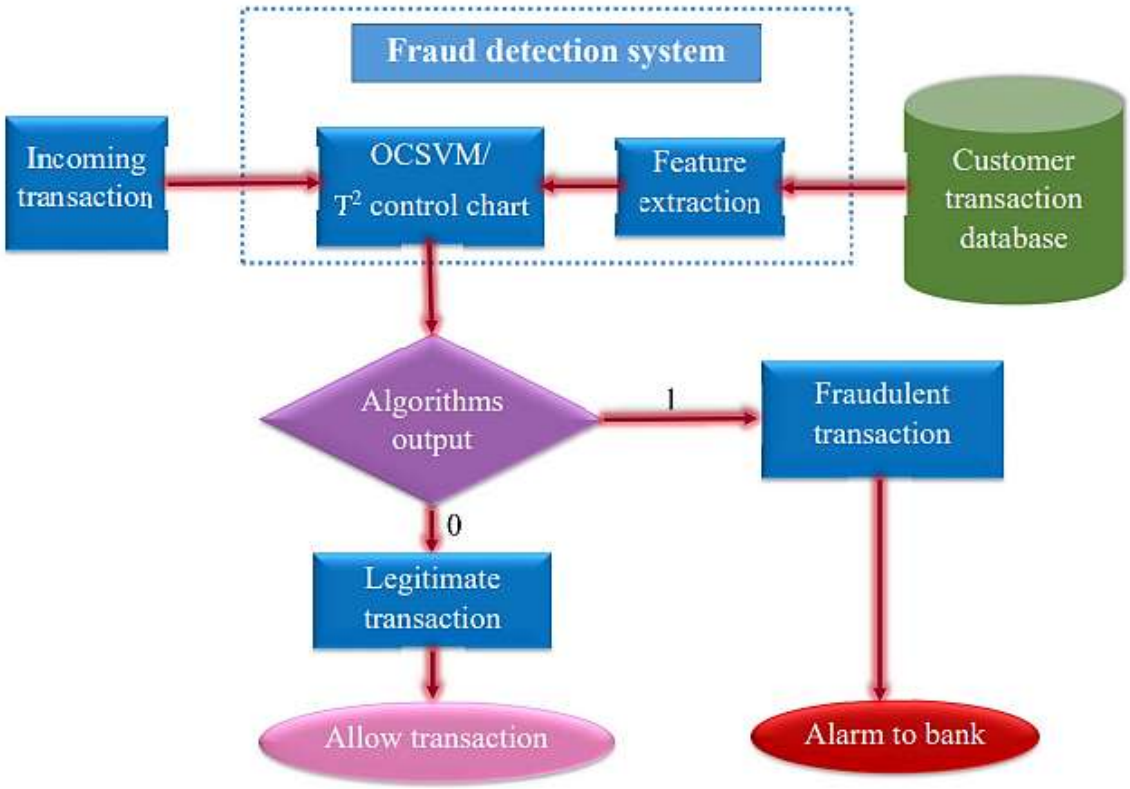

Fig.1: Data-driven strategies that have been suggested for detecting credit card fraud.

The capacity of adaptive fraud detection systems to manage concept drift is another essential feature. Concept drift is the statistical term for when fraud trends vary over time, usually as a result of new fraud techniques, market conditions, or changes in consumer behavior. To address this, adaptive systems incorporate drift detection mechanisms that monitor model performance continuously and trigger updates when significant changes are detected in transaction patterns[11]. By detecting concept drift early, these systems can quickly adjust their detection algorithms to maintain high levels of accuracy, ensuring that new fraud patterns do not go unnoticed for extended periods.

Furthermore, adaptive fraud detection systems often combine supervised and unsupervised learning techniques to enhance their detection capabilities. Supervised learning, which uses labelled data to train models, is highly effective when a sufficient amount of fraud data is available. However, because fraud cases are rare compared to legitimate transactions, unsupervised methods, such as anomaly detection and clustering, play a critical role in identifying outliers in unlabeled data[12]. By leveraging both approaches, adaptive systems can balance identifying known fraud patterns and detecting new, previously unseen fraudulent activities. This combination of techniques enables adaptive systems to maintain prominent levels of precision and recall, effectively reducing the potential for monetary losses as a result of fraud.

4. OCSVM-based credit card fraud detection:

One-Class Support Vector Machine is a popular unsupervised learning technique used in fraud detection, especially in highly imbalanced scenarios such as credit card transactions. The central idea behind OCSVM is to identify a boundary that encapsulates the majority of legitimate transactions, treating any data points outside this boundary as anomalies or potential frauds. Since fraudulent transactions typically represent a very small portion of the data (often less than 1%), OCSVM is particularly well-suited for detecting these anomalies without needing a large volume of labelled fraudulent data. Its ability to work effectively in high-dimensional spaces and model complex decision boundaries makes it a valuable tool for fraud detection[13].

In a high-dimensional feature space, the OCSVM algorithm trains a hyperplane to distinguish between outliers and typical data (regular transactions). It constructs this boundary by considering the distribution of normal transactions and determining the region where the density of points is highest. Transactions outside this region are flagged as anomalies and considered potentially fraudulent[14]. This method has the advantage of not requiring

labeled examples of fraudulent transactions, which can be hard to come by and expensive to acquire. Rather, the model concentrates on acquiring the traits of typical transactions, which helps it to effectively generalize unknown data and identify new kinds of fraud. The detection of credit card fraud via OCSVM is shown in Fig. 2.

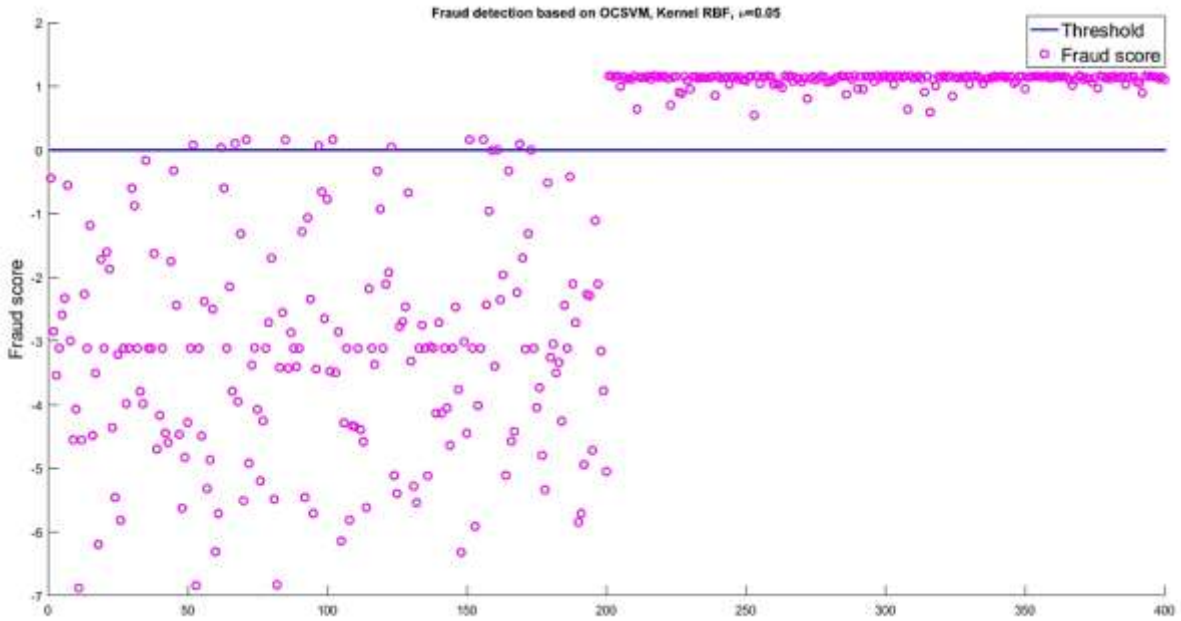

Fig.2: Method for utilizing OCSVM in credit card fraud detection.

Features retrieved from transaction data, such as quantity, frequency, location, and user-specific behavior patterns, are subjected to OCSVM.

Feature selection and engineering are critical for the effectiveness of the OCSVM model, as they help capture the underlying dynamics of fraud. For example, sudden spending increases, geographical deviations, or purchases made at odd times can help the OCSVM model identify outlier transactions. Support vector machines' signature kernel method can project the data into higher dimensions, which facilitates the identification of intricate correlations between features and improves the isolation of dataset abnormalities [15].

Using OCSVM for credit card fraud detection also comes with challenges. One of the primary limitations is the selection of an appropriate threshold for distinguishing between legitimate transactions and anomalies. Setting the threshold too low can result in high false positives, flagging many legitimate transactions as suspicious and frustrating customers. On the other hand, setting the threshold too high may allow fraudulent transactions to slip through undetected[16]. To address this issue, careful calibration of the model

and rigorous evaluation using techniques like cross-validation are essential. Furthermore, OCSVM's sensitivity to noise and outliers in the training set could cause the learnt boundary to be distorted, decreasing its ability to detect fraud.

5. Detecting credit card theft with the T^2 control chart:

The T^2 control chart is a multivariate statistical process control method widely used for monitoring and detecting anomalies in complex systems, including credit card fraud detection. The fundamental principle behind the control chart is to measure the deviation of multivariate observations from their expected values based on historical data. In dealings with credit cards, the T^2statistic helps track multiple transaction attributes simultaneously, such as amount, frequency, and time, to determine if a transaction significantly deviates from the normal behaviour observed in past data[17]. Transactions that exhibit large deviations from the established norm are flagged as potential fraud cases.

The T^2 control chart is particularly effective for fraud detection because it can handle the correlations between different transaction features, capturing more complex patterns of legitimate versus fraudulent behaviour. In a typical setup, historical transaction data estimates normal transactions' matrix of covariance and mean vector. The T^2 statistic is then computed for each new transaction based on its deviation from the historical mean, adjusted for the correlations between features. If the T^2 statistic for a transaction exceeds a predefined control limit (usually set using statistical significance thresholds), the transaction is classified as an outlier, indicating potential fraud. This multivariate approach allows the control chart to detect subtle deviations that might not be apparent when considering individual features in isolation[18]. Fig.3 depicts Detecting credit card theft with the T^2 control chart.

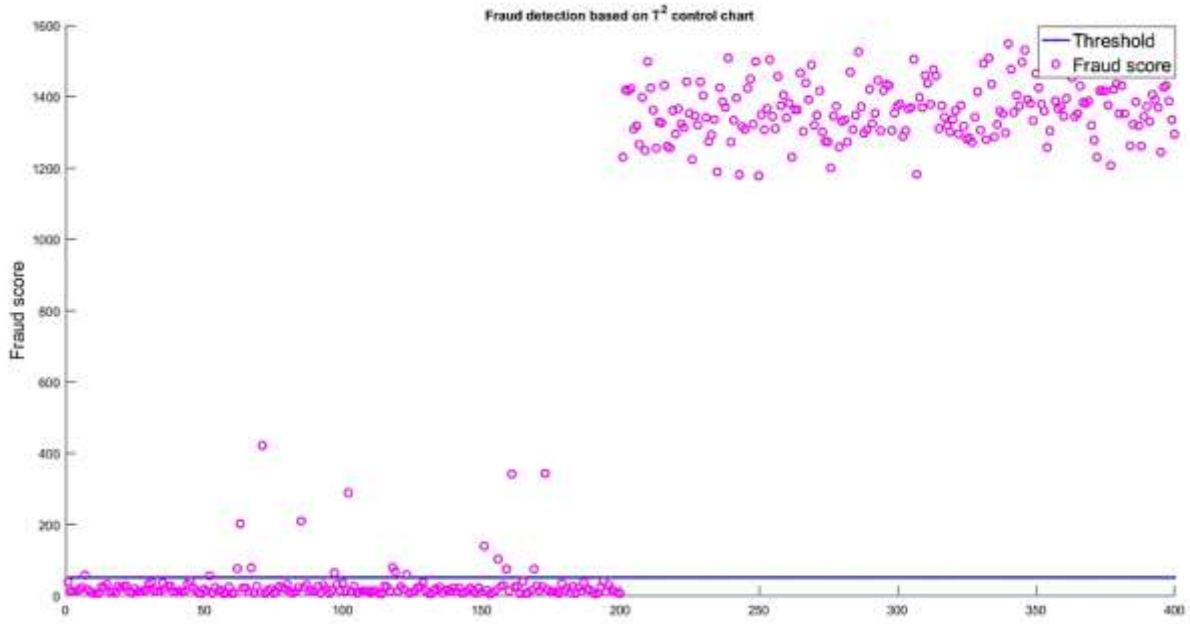

Fig.3: Detecting credit card theft with the T^2 control chart.

The capacity of the T^2 control chart to continually monitor transactions in real-time makes it ideal for identifying fraudulent activity as they occur, which is one of its benefits when used for credit card fraud detection. Unlike static rules or univariate methods that focus on specific transaction attributes, the multivariate nature of the T^2 control chart allows it to detect complex fraud patterns that involve correlations between different transaction variables[19]. For example, a fraudulent transaction may involve an unusually high amount and an unexpected location, which may go unnoticed by univariate detection methods but would trigger an alert in a multivariate framework like the T^2 control chart.

However, challenges are associated with implementing T^2 control charts for fraud detection. One limitation is the assumption that the underlying transaction data follows a multivariate normal distribution, which may not always hold in practice. Violations of this assumption can lead to incorrect estimates of control limits and increased false positives or negatives. Furthermore, the quality of the historical data used to estimate the mean and covariance has a significant impact on the control chart's performance. If the historical data contains noise, outliers, or unrepresentative transactions, the control chart may be less effective at identifying fraudulent transactions[20]. Despite these challenges, with proper data preprocessing and adjustments to account for non-normality, the T^2 control chart remains a powerful tool for detecting credit card fraud in a multivariate context.

6. Future Directions:

In order to manage ever larger and more complicated transaction data in real time, future research in adaptive fraud detection systems should concentrate on improving the scalability and robustness of machine learning models. We want to address the fraud detection problem in the future by utilizing autoencoders with control charts, with a focus on time series data that contains uncertainty. We also intend to refine our methodology to increase its efficacy in identifying fraud in big streaming datasets.[21]. Combining deep learning methods to capture temporal relationships and sequential patterns in transaction streams, such as transformers and recurrent neural networks (RNNs), is one possible avenue. Furthermore, using hybrid models that incorporate unsupervised, supervised, and reinforcement learning may enhance the ability to identify new fraud strategies. Techniques that protect privacy, such as federated learning, are also essential for enabling cross-institutional collaboration without jeopardizing sensitive data. Finally, in order to guarantee that financial institutions and regulators can comprehend and have faith in the conclusions made by these systems, explainability and interpretability must be integrated into AI-driven fraud detection models [22].

7. Conclusion:

Adaptive fraud detection systems that learn in real-time from credit card transaction data represent a viable defense against the growing risk of credit card theft. By continuously adapting to new fraud patterns, these systems can significantly enhance the detection and prevention of fraud in digital payment systems. This paper presents two advanced real-time, data-driven fraud detection methodologies that operate independently of anomalies in the training set. The first approach utilizes the One-Class Support Vector Machine (OCSVM), fine-tuned through optimal kernel parameter selection to enhance its detection capabilities. The second approach leverages the T^2 control chart, a robust multivariate technique for monitoring and detecting deviations. Our extensive numerical results highlight that both methods deliver exceptional detection accuracy while effectively minimizing false alarm rates, showcasing their effectiveness in identifying fraudulent activities with precision.

References:

[1] A. Yeşilkanat, B. Bayram, B. Köroğlu, and S. Arslan, "An adaptive approach on credit card fraud detection using transaction aggregation and word embeddings," in Artificial Intelligence Applications and Innovations: 16th IFIP

WG 12.5 International Conference, AIAI 2020, Neos Marmaras, Greece, June 5–7, 2020, Proceedings, Part I 16, 2020: Springer, pp. 3-14.

[2] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," IEEE Access, vol. 10, pp. 39700-39715, 2022.

[3] V. Ashwin, V. Menon, A. Devagopal, P. Nived, and J. Udayan Divya, "Detection of Fraudulent Credit Card Transactions in Real Time Using SparkML and Kafka," in Proceedings of 3rd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2022, 2023: Springer, pp. 285-295.

[4] S. Bakhtiari, Z. Nasiri, and J. Vahidi, "Credit card fraud detection using ensemble data mining methods," Multimedia Tools and Applications, vol. 82, no. 19, pp. 29057-29075, 2023.

[5] H. O. Bello, A. B. Ige, and M. N. Ameyaw, "Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments," World Journal of Advanced Engineering Technology and Sciences, vol. 12, no. 2, pp. 021-034, 2024.

[6] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," Human-Centric Intelligent Systems, vol. 2, no. 1, pp. 55-68, 2022.

[7] C.-T. Chen, C. Lee, S.-H. Huang, and W.-C. Peng, "Credit Card Fraud Detection via Intelligent Sampling and Self-supervised Learning," ACM Transactions on Intelligent Systems and Technology, vol. 15, no. 2, pp. 1-29, 2024.

[8] K. G. Dastidar, M. Granitzer, and W. Siblini, "The Importance of Future Information in Credit Card Fraud Detection," in International Conference on Artificial Intelligence and Statistics, 2022: PMLR, pp. 10067-10077.

[9] G. Zioviris, K. Kolomvatsos, and G. Stamoulis, "Credit card fraud detection using a deep learning multistage model," The Journal of Supercomputing, vol. 78, no. 12, pp. 14571-14596, 2022.

[10] A. Dhungana, "Assessing the Effectiveness of Convolutional Neural Networks in Real-Time Detection and Prevention of Credit Card Fraud," Journal of Sustainable Technologies and Infrastructure Planning, vol. 8, no. 3, pp. 21-30, 2024.

[11] K. Garg, K. S. Gill, P. Aggarwal, R. S. Rawat, and D. Banerjee, "Fraud & Anomaly Detection: Using Fine-tuned OCSVM Algorithm and visualization of the enhanced results using Machine Learning Techniques," in 2024 3rd International Conference for Innovation in Technology (INOCON), 2024: IEEE, pp. 1-5.

[12] V. Ghai and S. S. Kang, "Credit card transaction data analysis and performance evaluation of machine learning algorithms for credit card fraud detection," in AIP Conference Proceedings, 2022, vol. 2555, no. 1: AIP Publishing.

[13] S. Janani, M. Sivarathinabala, R. Anand, S. Ahamad, M. A. Usmani, and S. M. Basha, "Machine learning analysis on predicting credit card forgery," in International Conference On Innovative Computing And Communication, 2023: Springer, pp. 137-148.

[14] K. Kittidachanan, W. Minsan, D. Pornnopparath, and P. Taninpong, "Anomaly detection based on GS-OCSVM classification," in 2020 12th international conference on knowledge and smart technology (KST), 2020: IEEE, pp. 64-69.

[15] A. Kotagiri, "Mastering Fraudulent Schemes: A Unified Framework for AI-Driven US Banking Fraud Detection and Prevention," International Transactions in Artificial Intelligence, vol. 7, no. 7, pp. 1-19, 2023.

[16] I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," IEEE Access, vol. 11, pp. 30628-30638, 2023.

[17] I. D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," IEEE Access, 2024.

[18] A. Qayoom et al., "A novel approach for credit card fraud transaction detection using deep reinforcement learning scheme," PeerJ Computer Science, vol. 10, p. e1998, 2024.

[19] J. F. Roseline, G. Naidu, V. S. Pandi, S. A. alias Rajasree, and N. Mageswari, "Autonomous credit card fraud detection using machine learning approach☆," Computers and Electrical Engineering, vol. 102, p. 108132, 2022.

[20] I. Sadgali, N. Sael, and F. Benabbou, "Adaptive model for credit card fraud detection," 2020.

[21] P. Verma and P. Tyagi, "Credit Card Fraud Transaction Classification Using Improved Class Balancing and Support Vector Machines," in Recent Innovations in Computing: Proceedings of ICRIC 2021, Volume 2: Springer, 2022, pp. 477-488.

[22] C. Wang, C. Wang, H. Zhu, and J. Cui, "LAW: Learning automatic windows for online payment fraud detection," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2122-2135, 2020.