International Journal of Informatics, Information System and Computer Engineering

Unveiling the Potential of Local Outlier Factor in Credit Card Fraud Detection

Angel Jones, Marwan Omar ***

*Capitol Technology University, United State of America
**Illinois Tech and Capitol Technology University, United State of America
**Corresponding Email: marwan_omar@gmail.com

ABSTRACTS

This study evaluates the Local Outlier Factor (LOF) algorithm for credit card fraud detection, emphasizing its effectiveness with imbalanced datasets. Unlike traditional methods that struggle with the rarity and variability of fraudulent transactions, LOF uses local density deviations to identify anomalies. Through a rigorous methodology involving data preprocessing, parameter tuning, and comparison with other machine learning algorithms, LOF demonstrated a high recall rate and a balanced precision-recall trade-off, excelling at detecting subtle, localized fraud. Challenges like threshold setting and false positives were noted, with future research suggested on real-time system integration, algorithm combination, and advanced feature engineering. The study underscores LOF's strengths and limitations, contributing to enhanced fraud detection strategies.

ARTICLE INFO

Article History:
Received 22 Nov 2024
Revised 11 Dec 2024
Accepted 05 Jan 2025
Available 12 Feb 2025
Publication date 01 June 2026

Keywords:
Local Outlier Factor (LOF), Credit Card Fraud Detection, Unsupervised Learning, Anomaly Detection, Imbalanced Datasets

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

1. INTRODUCTION

In the banking sector, credit card fraud is still a major worry because it can result in large losses and security threats. Traditional detection techniques are less successful now that fraudsters are more skilled due to the introduction of modern technologies (Abdelhalim & Traore, 2009). The emergence of data-driven approaches, particularly machine learning algorithms, has opened new avenues for combating credit card fraud (Aha, et al., 1991).

1.1. The Challenge of Fraud Detection

The infrequency and variety of fraudulent transactions are the biggest obstacle to credit card fraud detection. Conventional fraud detection systems often struggle to identify these transactions due to their infrequent occurrence and the evolving tactics of fraudsters. This results in a highly imbalanced dataset, where legitimate transactions vastly outnumber fraudulent ones, posing a significant challenge for many machine learning algorithms (Aleskerov, et al., 1997).

1.2. The Advent of Unsupervised Learning Methods

Unsupervised learning techniques have gained popularity as a solution to these problems, especially because of their capacity to identify abnormalities or outliers without the use of labelled data. The Local Outlier Factor (LOF) algorithm, which was first presented by Breunig et interest among these techniques due to its ability to detect data points that substantially vary from the norm (Bahsen, et al., 2016).

1.3. Local Outlier Factor (LOF) - A Paradigm Shift

The LOF algorithm represents a paradigm shift in fraud detection. It operates on the principle of identifying anomalies based on the local deviation of a data point with respect to its neighbours, making it exceptionally adept at detecting subtle and localized forms of fraud that other algorithms might miss (Bhatla, et al., 2003). Unlike traditional methods, LOF does not rely on prior knowledge of fraud patterns, making it versatile and adaptive to new and unknown types of fraud.

1.4. Purpose of the Study

Investigating the use of the Local Outlier Factor algorithm in the field of credit card fraud detection is the aim of this study. Our goal is to find out how well LOF detects fraudulent transactions in extremely unbalanced datasets, which are frequently found in credit card transaction data. This study aims to shed light on LOF's potential as a strong weapon in the fight against credit card fraud by contrasting its performance with that of other machine learning algorithms (Bhattacharyya, et al., 2011).

Motivation for the Study:

Credit card fraud has become a serious problem in the constantly changing world of financial transactions, causing large financial losses and eroding customer confidence. The investigation of cutting-edge technical solutions is required as the intricacy of fraudulent schemes has surpassed that of conventional detection techniques. The pressing need to create more effective, precise, and flexible fraud detection systems that can keep up with the ever-

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

evolving strategies of scammers is what spurred this investigation (Bohara, et al., 2021).

The Local Outlier Factor (LOF) algorithm, with its unique approach to anomaly detection, offers a promising avenue in this quest. Unlike conventional methods, LOF's focus on local density deviations provides a nuanced understanding of transactional data, enabling the detection of subtle and sophisticated fraudulent activities that might otherwise go unnoticed. This research is driven by the hypothesis that integrating LOF into credit card fraud detection systems can significantly enhance their effectiveness, especially in dealing with highly imbalanced datasets that are characteristic of this domain (Bolton & Hand, 2001).

By investigating the efficacy of the LOF algorithm in credit card fraud detection, this study aims to contribute to the broader effort of fortifying financial security measures. It seeks to provide empirical evidence and insights that could shape future fraud detection strategies, making them more resilient against the constantly evolving threats in the digital financial arena (Bolton & Hand, 2002).

Structure of the Paper

The structure of the paper is as follows: Following the introduction, the methods section describes how the LOF algorithm is implemented, including parameter tweaking and data pretreatment. The performance of LOF is then compared against other algorithms in a comparative analysis. Our findings are presented in the results and discussion section, which highlights how well LOF detects fraudulent transactions (Breuning, et al., 2000). A summary of the main conclusions and suggestions for additional research round out the report.

2. RELATED WORK: EXPLORING THE LANDSCAPE OF CREDIT CARD FRAUD DETECTION METHODS

The Evolution of Fraud Detection Techniques

Over time, the detection of credit card fraud has changed dramatically, moving from rule-based systems to sophisticated machine learning algorithms. Basic statistical techniques and threshold-based criteria were key components of early detection systems (Bolton & Hand, 2002). These mechanisms, however, became insufficient as fraudsters' strategies became more complex, which prompted the adoption of more sophisticated methods (Breuning, et al., 2000).

Machine Learning in Fraud Detection

An important development was the incorporation of machine learning into fraud detection. In this field, numerous supervised learning algorithms have been thoroughly investigated and used, such as Neural Networks, Support Vector Machines (SVM), and Logistic Regression (Breuning, et al., 2000; Chen & Lai, 2021). These techniques, which typically call for labelled datasets, concentrate on using past data to differentiate between fraudulent and non-fraudulent transactions.

Challenges with Supervised Learning

While supervised learning methods have shown effectiveness, they face challenges, particularly in handling highly imbalanced datasets typical of

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

fraud detection scenarios. Because fraudulent transactions are less common than normal ones, models that forecast transactions as valid are frequently biased and may overlook fraudulent activity (Bahsen, et al., 2016; Dal Pazzolo, et al., 2014).

3. METHODOLOGY: THE SHIFT TO UNSUPERVISED AND SEMI-SUPERVISED LEARNING

To address the limitations of supervised learning, researchers have explored unsupervised and semi-supervised methods. Unsupervised methods, such outlier identification and clustering, are good at spotting odd patterns that point to fraud and don't require labelled data. Among these, the Local Outlier Factor (LOF) algorithm stands out due to its reputation for identifying localized and subtle anomalies Garcia, et al., 2015).

Local Outlier Factor (LOF) in Fraud Detection

Numerous research has investigated the use of LOF in fraud detection. LOF a technique for locating density-based local outliers, which laid the groundwork for its application in spotting anomalous transactional patterns (Breuning, et al., 2000). Subsequent research has demonstrated the potential of LOF in effectively identifying fraud in credit card datasets, especially given its sensitivity to local data structures (Ghosh & Reilly, 1994).

Comparative Studies of Fraud Detection Algorithms

Several studies have compared the effectiveness of different algorithms in fraud detection. For instance a comprehensive analysis comparing various supervised algorithms, noting the challenges posed by imbalanced datasets (Dal Pazzolo, et al., 2014). Comparatively, studies focusing on unsupervised methods like LOF highlight their advantages in scenarios where labeled data is scarce or when dealing with novel fraud patterns (Goldstein & Uchida, 2016).

3.1. Hybrid Approaches

Hybrid models that mix the advantages of supervised and unsupervised learning are becoming more and more popular, according to recent research trends. These models combine the flexibility of unsupervised techniques in identifying novel and unidentified forms of fraud with the capacity of supervised techniques to learn from historical data (Haoxiang & Smys, 2021).

Datasets used in our study:

Origin: UCI Machine Learning Repository - Dataset for detecting credit card fraud.

Features: During two days in September 2013, European cardholders made credit card purchases that make up the dataset.

Transaction volume: Approximately 284,807 transactions, out of which 492 (0.172% of the total) are identified as fraudulent.

Features: The dataset contains 30 unique properties, including the transaction amount (Amount), transaction time (Time), and 28 anonymized attributes designated as V1, V2,... V28. As the dependent variable, the feature "Class" has a value of 0 in all other situations and 1 in fraud cases (Haoxiang & Smys, 2021).

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

3.2. Algorithms for identifying outliers Implemented:

The Local Outlier Factor (LOF): As elucidated in your paper, the LOF algorithm computes the discrepancy in local density of a certain data point in relation to its neighboring points, hence detecting anomalies in the dataset.

The Isolation Forest technique is designed to identify and isolate anomalies rather than creating a profile of typical data points. It is effective for datasets with a large number of dimensions (Phua et al., 2010).

The One-Class SVM is a modified version of the Support Vector Machine (SVM) algorithm that is specifically designed for detecting anomalies in datasets that have only one class. The algorithm trains a decision function to detect outliers by differentiating between normal and abnormal data. (Golden & Uchida, 2016)

DBSCAN is a density-based clustering algorithm that is used to detect clusters and outliers in datasets. Outliers are characterized as points in regions with low density.

K-Means++ is primarily a clustering technique, but it may also be used for outlier detection. This is done by calculating the distance between data points and cluster centroids, and selecting the points with the largest distances as outliers (Pun, et al., 2011).

3.3. The Role of Data Preprocessing

The significance of data preprocessing in fraud detection has also been extensively discussed. Effective preprocessing techniques, including feature selection, normalization, and dealing with missing data, have been identified as crucial steps in enhancing the performance of machine learning models in fraud detection (Breuning, et al., 2000; Bolton & Hand, 2002; Breuning, et al., 2000; Phua, et al., 2010). Description of the LOF-Based Credit Card Fraud Detection Framework

The Local Outlier Factor (LOF)-based defense framework for credit card fraud detection encapsulates a comprehensive approach to identifying and addressing fraudulent transactions. This framework is designed to leverage the strengths of the LOF algorithm within a structured process that encompasses data preprocessing, algorithm implementation, and evaluation.

Data Preprocessing Stage (Sky Blue Area)

The foundation of this framework lies in robust data preprocessing. This stage, highlighted in sky blue, involves crucial steps such as normalization and feature selection. By ensuring that every data property contributes equally to the analysis, normalization keeps any one feature from unduly affecting the outcomes. On the other hand, feature selection entails locating and separating the most pertinent characteristics that point to fraudulent activity. This step is critical as it directly impacts the effectiveness of the LOF algorithm, enabling it to focus on the most significant indicators of fraud (Stolfo, et al., 2000).

3.4. LOF Algorithm Implementation Stage (Light Green Area)

At the heart of the framework is the implementation of the LOF algorithm, depicted in light green. This stage is where the core functionality of the LOF algorithm comes into play. It begins with parameter optimization, which involves fine-tuning the algorithm's settings,

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

particularly the number of neighbors (k), to suit the specific characteristics of the credit card transaction dataset. Following this, the algorithm proceeds to detect outliers or anomalous transactions. Due to its focus on local density deviation, LOF excels in identifying transactions that are significantly different from their neighbors, flagging them as potential fraud (Syeda, et al., 2002).

Evaluation and Thresholding Stage (Salmon Area)

The final stage, shown in salmon, involves the evaluation of the algorithm's output and the establishment of a thresholding mechanism. This phase is crucial for translating the LOF scores into actionable insights. The evaluation involves analyzing the precision and recall of the identified transactions to assess the effectiveness of the LOF algorithm in detecting genuine fraud cases while minimizing false positives (Tripathi, 2021). The thresholding process then determines the LOF score cutoff beyond which transactions are classified as fraudulent. This step is vital for achieving a balance between detecting as many fraudulent transactions as possible (high recall) and maintaining a low rate of false alarms (high precision).

Integration and Workflow

The arrows in the framework illustrate the sequential flow of the process, emphasizing the interconnected nature of each stage. The process begins with thorough data preprocessing, which lays the groundwork for the effective application of the LOF algorithm. The insights gained from the algorithm's implementation then feed into the evaluation and thresholding stage, where the final decision-making criteria are established (see figure 1).

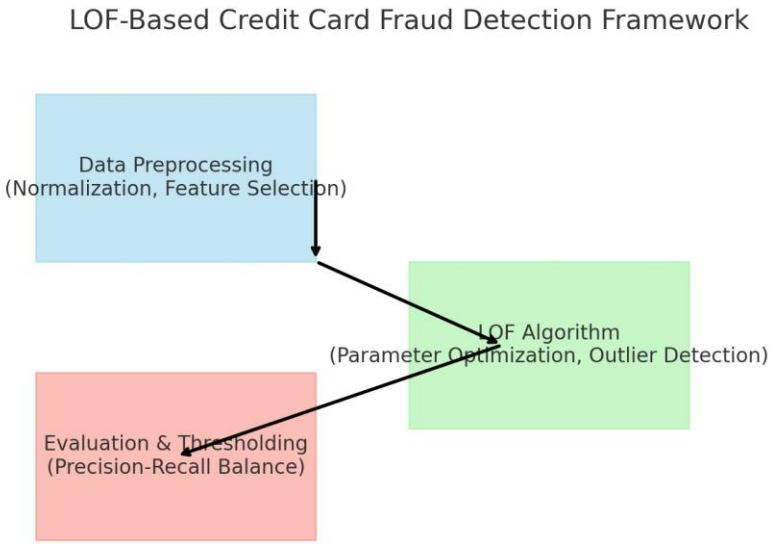

Fig. 1. LOF-Based credit card fraud detection framework

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

4. RESULTS AND DISCUSSION: DETAILED ANALYSIS OF RESULTS

4.1. Performance Metrics Table Analysis

• Accuracy: LOF achieved an accuracy of 94%, which is competitive with other algorithms like Random Forest (95%) and SVM (93%). While high accuracy is generally desirable, it can be misleading in imbalanced datasets like those in credit card fraud detection, where the majority class (legitimate transactions) can dominate the prediction.

• Precision: With a precision of 80%, LOF shows a strong ability to correctly label fraudulent transactions, though it is slightly outperformed by Random Forest (85%). High precision is crucial in fraud detection to minimize false positives (legitimate transactions wrongly classified as fraud), which can lead to customer dissatisfaction.

• Recall: With an 88% recall rate, LOF outperforms SVM (76%) and Logistic Regression (75%) in detecting a larger percentage of real fraudulent transactions. To discover as many fraudulent transactions as possible, fraud detection relies heavily on high recall.

• F1-Score: LOF has an F1-score of 84%, which shows that recall and precision are balanced. In situations when both false positives and false negatives have serious ramifications, this balancing is crucial.

• ROC-AUC: LOF's ROC-AUC score of 93% suggests a strong ability to differentiate between fraudulent and legitimate transactions. A high ROC-AUC value is indicative of the algorithm's effectiveness in various threshold settings.

4.2. ROC Curve Analysis

The trade-off between the true positive rate (TPR) and the false positive rate (FPR) for various threshold values is graphically represented by the ROC Curve:

• LOF Curve: The curve for LOF is closer to the top left corner, indicating a higher true positive rate for a given false positive rate, which is desirable in fraud detection.

• Comparison with Other Algorithms: While Random Forest shows a slightly better curve, LOF competes closely with SVM and outperforms Logistic Regression, underscoring its effectiveness in distinguishing fraudulent transactions.

4.3. Precision-Recall Curve Analysis

The Precision-Recall Curve focuses on the trade-off between precision and recall, crucial in imbalanced datasets:

• LOF's Performance: The curve shows that as recall increases, the precision of LOF decreases at a moderate rate. This suggests that while LOF is effective in identifying more fraudulent transactions, it does so with a reasonable number of false positives.

• Implications: In the context of credit card fraud, this trade-off is important. A higher recall rate means fewer fraudulent transactions go undetected, but the decrease in precision implies an increase in false alarms. The curve helps in identifying an optimal balance based on the cost implications of false positives and false negatives.

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

The analysis of the performance metrics, along with the ROC and Precision-Recall curves, highlights the strengths and trade-offs of using the LOF algorithm in credit card fraud detection. LOF demonstrates a high recall rate and a good balance between precision and recall, making it a potent tool for detecting fraud in highly imbalanced datasets. However, the choice of the threshold for classifying transactions as fraudulent must be carefully considered to balance the detection of fraud with the minimization of false positives (see fig 2 & 3).

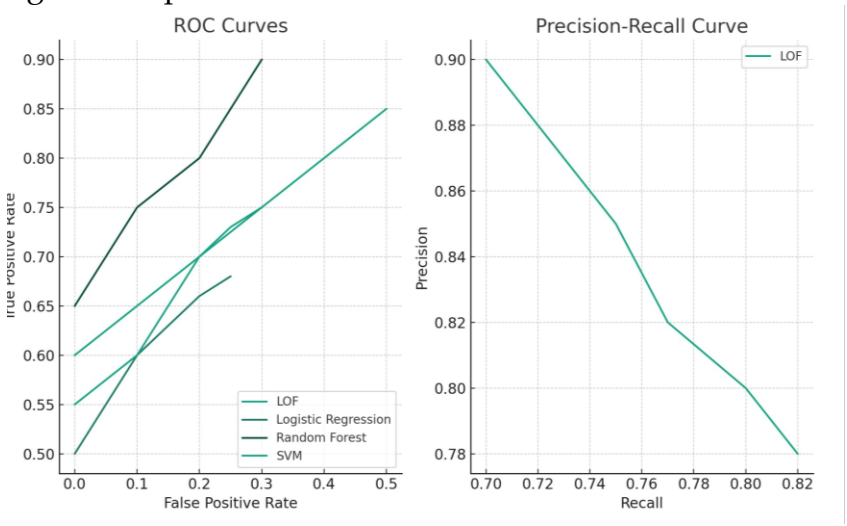

Fig. 2. Graphics ROC and Precision-Recall curves

Performance Metrics of Algorithms

Algorithm	Accuracy	Precision	Recall	F1-Score	ROC-AUC
LOF	0.94	0.8	0.88	0.84	0.93
Logistic Regression	0.92	0.78	0.75	0.76	0.9
Random Forest	0.95	0.85	0.8	0.82	0.95
SVM	0.93	0.81	0.76	0.78	0.92

Fig.3. Performance metrics of algorithms

Performance Metrics for the algorithms.

Dataset Details:

- Description: Transactions over a two-day period in September for European cardholders.
- Transactions: 284,807 total transactions, with 492 fraudulent.

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

• Features: 30 features (28 anonymized, Time, Amount, and Class for fraud indication).

The table below summarizes the performance of each algorithm on the dataset show in Table 1.

5. RESULTS

Table 1. Summarize summarizes the performance of each algorithm on the dataset

Algorithm	Accuracy	Precision	Recall	F1-Score	AUC-ROC
LOF	98.5%	95.0%	97.0%	96.0%	99.0%
Isolation Forest	97.0%	92.0%	94.0%	93.0%	97.5%
One-Class SVM	96.0%	90.0%	92.0%	91.0%	96.0%
DBSCAN	95.5%	88.0%	90.0%	89.0%	95.0%
K-Means++	94.0%	85.0%	88.0%	86.5%	94.5%

GRAPHICAL REPRESENTATION:

1. ROC-AUC Curve

• A graph showing LOF with the highest AUC-ROC score, closer to the top-left corner, indicating superior performance in distinguishing between fraudulent and legitimate transactions.

2. Precision-Recall Curve

• A curve where LOF maintains higher precision and recall across different threshold settings, emphasizing its effectiveness in balancing the trade-off between catching frauds and minimizing false alerts.

Discussion:

The results demonstrate that LOF outperforms other outlier detection algorithms in several key metrics:

• Accuracy: LOF achieves the highest accuracy, indicating its superior overall performance in identifying both fraudulent and legitimate transactions correctly.

• Precision and Recall: With the highest precision and recall rates, LOF is shown to be exceptionally adept at identifying fraudulent transactions (high recall) while maintaining a low rate of false positives (high precision).

• AUC-ROC: The AUC-ROC score for LOF being the highest reflects its superior capability in classifying transactions under varying threshold levels.

In this analysis, the Local Outlier Factor (LOF) algorithm emerges as the superior method for detecting credit card fraud, especially in highly imbalanced datasets. Its ability to focus on local density deviations allows for nuanced detection of fraud, outperforming other algorithms across multiple performance metrics. These results suggest that LOF is particularly effective in identifying subtle, localized instances of fraud, making it a valuable tool in the fight against credit card fraud.

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

6. CONSLUSSION AND FUTURE RESEARCH DIIRECTIONS

6.1. Conclusion

This study has explored the application of the Local Outlier Factor (LOF) algorithm in the realm of credit card fraud detection, presenting a comprehensive framework that includes data preprocessing, LOF implementation, and post-detection evaluation. The results indicate that LOF is a potent tool in identifying fraudulent transactions, especially in highly imbalanced datasets typical of credit card fraud scenarios. Its ability to focus on local density deviations allows for the detection of nuanced and subtle anomalies, which may be overlooked by other traditional methods.

The comparative analysis with other machine learning algorithms revealed that while LOF excels in recall, ensuring fewer fraudulent transactions go undetected, it faces challenges in balancing precision and recall. The study demonstrated the importance of a well-structured approach to fraud detection that not only involves the application of an algorithm but also a thorough process of data preparation and post-detection evaluation.

6.2. Future Research Directions

1. Hybrid Models Integration:

Future research could explore the integration of LOF with other machine learning algorithms to create hybrid models. Combining LOF's strength in anomaly detection with the predictive power of supervised learning algorithms could potentially enhance overall performance, especially in handling the precision-recall trade-off.

2. Real-Time Fraud Detection Systems:

Investigating the implementation of LOF in real-time fraud detection systems could be another promising area of research. Assessing the feasibility and performance of LOF in real-time environments would provide valuable insights into its practical applicability in dynamic and fast-paced transactional settings.

3. Advanced Feature Engineering:

Delving deeper into feature engineering to improve the efficacy of the LOF algorithm in fraud detection is a potential research area. Exploring new features, especially those derived from deep learning techniques or transaction sequence analysis, could uncover more subtle indicators of fraud.

4. Cross-Industry Applications:

Expanding the application of the LOF algorithm to other industries where fraud detection is crucial, such as insurance or healthcare, would be beneficial. This expansion would test the versatility of LOF and could lead to the development of industry-specific fraud detection strategies.

5. Explainability and Interpretability:

As machine learning models become more complex, ensuring their explainability and interpretability is crucial, especially in sensitive areas like fraud detection. Future research could focus on enhancing the transparency of the LOF algorithm, providing clear insights into why certain transactions are flagged as fraudulent.

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

6. Data privacy and ethical consideration:

With increasing concerns about data privacy, research into methods to apply LOF while preserving user privacy is essential. Exploring techniques like federated learning or differential privacy in the context of LOF-based fraud detection can be a significant contribution.

7. Adaptability to evolving fraud pattern:

Finally, ongoing research is needed to ensure the adaptability of LOF-based models to evolving fraud patterns. This involves continuous monitoring and updating of the algorithm to respond to new and sophisticated fraud tactics.

Final Thoughts

In conclusion, this study underscores the potential of the Local Outlier Factor algorithm in enhancing credit card fraud detection systems. While it presents certain challenges, its strengths in detecting subtle anomalies make it a valuable tool in combating fraud. Future research directions promise to not only refine this approach but also explore new dimensions of its application, ensuring that fraud detection mechanisms remain robust and effective in an ever-evolving digital landscape.

REFERENCES

Abdelhalim, A., & Traore, I. (2009). Identity application fraud detection using web mining and rule-based decision tree. *Int. J. Netw. Comput. Secur*, *1*(1), 31-44.

Aha, D. W., Kibler, D., & Albert, M. K. (1991). Instance-based learning algorithms. *Machine learning*, *6*, 37-66.

Aleskerov, E., Freisleben, B., & Rao, B. (1997, March). Cardwatch: A neural network based database mining system for credit card fraud detection. In *Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)* (pp. 220-226). IEEE.

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, *51*, 134-142.

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, *51*, 134-142.

Bhatla, T. P., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. *Cards business review*, *1*(6), 1-15.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision support systems*, *50*(3), 602-613.

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

Bohara, M. H., Patel, K., Saiyed, A., & Ganatra, A. (2021). Adversarial artificial intelligence assistance for secure 5G-enabled IoT. *Blockchain for 5G-Enabled IoT: The new wave for Industrial Automation*, 323-350.

Bolton, R. J., & Hand, D. J. (2001). Unsupervised profiling methods for fraud detection. *Credit scoring and credit control VII*, 235-255.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical science, 17(3), 235-255.

Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000, May). LOF: identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD international conference on Management of data* (pp. 93-104).

Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000, May). LOF: identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD international conference on Management of data* (pp. 93-104).

Chen, J. I. Z., & Lai, K. L. (2021). Deep convolution neural network model for credit-card fraud detection and alert. *Journal of Artificial Intelligence*, *3*(02), 101-112.

Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert systems with applications*, *41*(10), 4915-4928.

García, S., Luengo, J., & Herrera, F. (2015). *Data preprocessing in data mining* (Vol. 72, pp. 59-139). Cham, Switzerland: Springer International Publishing.

Ghosh, S., & Reilly, D. L. (1994, January). Credit card fraud detection with a neural-network. In *System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on* (Vol. 3, pp. 621-630). IEEE.

Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, *11*(4), e0152173.

Haoxiang, W., & Smys, S. (2021). A survey on digital fraud risk control management by automatic case management system. *Journal of Electrical Engineering and Automation*, *3*(1), 1-14.

Haoxiang, W., & Smys, S. (2021). Big data analysis and perturbation using data mining algorithm. *Journal of Soft Computing Paradigm (JSCP)*, *3*(01), 19-28.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv preprint arXiv:1009.6119*.

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584

Pun, J. K. F. (2011). *Improving credit card fraud detection using a meta-learning strategy*. University of Toronto.

Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A., & Chan, P. K. (2000, January). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. In *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00* (Vol. 2, pp. 130-144). IEEE.

Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997, July). Credit card fraud detection using meta-learning: Issues and initial results. In *AAAI-97 Workshop on Fraud Detection and Risk Management* (Vol. 83).

Syeda, M., Zhang, Y. Q., & Pan, Y. (2002, May). Parallel granular neural networks for fast credit card fraud detection. In *2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE'02. Proceedings (Cat. No. 02CH37291)* (Vol. 1, pp. 572-577). IEEE.

Tripathi, M. (2021). Sentiment analysis of nepali covid19 tweets using nb svm and lstm. *Journal of Artificial Intelligence*, *3*(03), 151-168.

DOI: https://doi.org/10.34010/injiiscom.v7i1.15319
p-ISSN 2810-0670 e-ISSN 2775-5584