|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Title of the Paper** | **Title of the Journal** | **Reference with DOI** | **Problem or gap addressed** | **Objective of the paper** | **Focus of the paper(discuss methods used)** | **Summary** |
| 1 | Payment card fraud: Challenges and solutions | [2012 IEEE International Conference on Intelligence and Security Informatics](https://ieeexplore.ieee.org/xpl/conhome/6269208/proceeding) | [10.1109/ISI.2012.6284315](https://doi.org/10.1109/ISI.2012.6284315) | 1. Accuracy  2. Evolving fraud tactics  3. Complex data patterns  4. Interpretability  5. Scalability and efficiency | This paper aims to offer a brief overview of payment card fraud, highlighting its financial impact, methods used by identity thieves, and solutions for detection and prevention, aiding financial institutions in bolstering their fraud prevention strategies. | It discusses techniques such as anomaly detection, signature-based detection, machine learning approaches, and data mining methods applied to network traffic analysis for identifying and mitigating cyber threats | The paper succinctly outlines the methods employed in payment card fraud, including phishing, skimming, CNP fraud, account takeover, and social engineering. By highlighting these tactics, it provides essential knowledge for bolstering fraud detection and prevention efforts among financial institutions and card issuers. |
| 2 | Review on fraud detection methods in credit card transactions | [2017 International Conference on Intelligent Computing and Control (I2C2)](https://ieeexplore.ieee.org/xpl/conhome/8316803/proceeding) | [10.1109/I2C2.2017.8321781](https://doi.org/10.1109/I2C2.2017.8321781) | 1. Rising Fraudulent Transactions  2. Detection Complexity  3. Need for Effective Solutions  4. Anomaly Detection  5. Comparative Analysis | The objective of the paper is to address the increasing incidence of fraudulent cashless transactions by examining customer spending behaviour using data mining techniques. It aims to provide a comparative analysis of various methods, such as decision trees, neural networks, and fuzzy clustering, to identify effective approaches for detecting and preventing fraud in cashless payment systems. | It explores different data mining techniques such as decision trees, rule-based mining, neural networks, fuzzy clustering approaches, hidden Markov models, and hybrid methods. | The paper investigates the surge in fraudulent cashless transactions and proposes using data mining techniques like decision trees, neural networks, and fuzzy clustering to detect anomalies in customer spending behaviour. It aims to provide a comparative analysis of these methods to enhance fraud detection in cashless payment systems. |
| 3 | Machine Learning for Credit Card Fraud Detection | [ICCIR '21: Proceedings of the 2021 1st International Conference on Control and Intelligent Robotics](https://dl.acm.org/doi/proceedings/10.1145/3473714) | [10.1145/3473714.3473749](https://doi.org/10.1145/3473714.3473749) | 1. Rising Credit Card Fraud  2. Need for Automatic Systems  3. Unbalanced Data Distribution  4. Limited Human Resources  5. Improving Prediction Accuracy | The paper aims to develop automatic systems for credit card fraud detection, addressing the challenges posed by the large volume of account data and the imbalance between fraudulent and legitimate transactions. It seeks to improve prediction accuracy by employing learning algorithms and sampling methods. | These methods may include anomaly detection algorithms, supervised learning algorithms such as decision trees, random forests, support vector machines (SVM), or neural networks, and possibly ensemble methods for improved performance. | The paper focuses on developing automatic systems for credit card fraud detection in the context of increasing E-banking usage. It addresses the challenges of handling large datasets and imbalanced data distributions. By employing various learning algorithms and sampling methods, the paper aims to enhance prediction accuracy and effectively identify fraudulent transactions amidst a sea of legitimate ones. |
| 4 | Credit Card Fraud Detection using Machine Learning Techniques | [2022 11th International Conference on System Modelling & Advancement in Research Trends (SMART)](https://ieeexplore.ieee.org/xpl/conhome/10046659/proceeding) | [10.1109/SMART55829.2022.10047360](https://doi.org/10.1109/SMART55829.2022.10047360) | 1. Escalating credit card fraud  2. Need for effective fraud detection  3. Handling massive transaction volumes  4. Understanding strengths and limitations | The paper aims to assess machine learning techniques for credit card fraud detection in light of the surge in online transactions during the COVID-19 pandemic. It seeks to evaluate various fraud detection systems and identify their strengths and limitations to contribute insights for the development of effective algorithms. | The paper likely employs various machine learning algorithms and techniques. These methods include supervised learning algorithms such as logistic regression, decision trees, random forests, support vector machines (SVM), or neural networks. Additionally, it may incorporate unsupervised learning techniques like clustering or anomaly detection algorithms. | The paper explores machine learning techniques for credit card fraud detection in the context of increased online transactions due to the COVID-19 pandemic. Using algorithms like logistic regression and neural networks, it evaluates different fraud detection systems, aiming to identify their strengths and limitations. |
| 5 | Credit Card Fraud Detection: An Improved Strategy for High Recall Using KNN, LDA, and Linear Regression | [Journal of](https://www.sciencedirect.com/journal/journal-of-king-saud-university-computer-and-information-sciences)  MDPI,Sensors  Volume 23  Issue18  [Journal of](https://www.sciencedirect.com/journal/journal-of-king-saud-university-computer-and-information-sciences)  MDPI,Sensors  Volume 23  Issue18  **September 2023** | [10.3390/s23187788](https://doi.org/10.3390%2Fs23187788)  [10.3390/s23187788](https://doi.org/10.3390%2Fs23187788) | 1.Limited attention to recall in credit card fraud detection research  2.Lack of generalizability:  3.Imbalance in class distribution  4.Resource overhead  1.Limited attention to recall in credit card fraud detection research  2.Lack of generalizability:  3.Imbalance in class distribution  4.Resource overhead  5.Methodological limitations | The objective of this study was to develop a method prioritizing high recall in credit card fraud detection without compromising accuracy. We combined KNN, LDA, and LR models, demonstrating versatility across four datasets. Despite challenges, such as initial struggles with tree-based models, our approach succeeded. However, our study lacks precision enhancement strategies and benchmarking against state-of-the-art models. Future research should explore these areas to refine our approach further. | The methods employed in this study revolved around combining KNN, LDA, and LR to prioritize high recall in fraud detection, facing initial challenges with tree-based models and algorithmic fine-tuning. While effective across datasets, it lacked precision enhancement strategies and direct comparisons with state-of-the-art models, suggesting avenues for future research. | The study proposes a methodology enhancing recall in credit card fraud detection across four datasets, achieving recall scores of 1.0000, 0.9701, 1.0000, and 0.9362. It ensures competitive accuracy and offers potential for broader applications, including medical diagnostics and disaster forecasting. Looking forward, the method's adaptability could facilitate real-time fraud detection in online banking and other sectors like e-commerce and mobile payments. |
| 6 | Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning **Approach** | [Journal of](https://www.sciencedirect.com/journal/journal-of-king-saud-university-computer-and-information-sciences)  MDPI,big data and congitive computing  Volume 8  Issue1  [Journal of](https://www.sciencedirect.com/journal/journal-of-king-saud-university-computer-and-information-sciences)  MDPI,big data and congitive computing  Volume 8  Issue1  January 2024 | [**https://doi.org/10.3390/bdcc8010006**](https://doi.org/10.3390/bdcc8010006)  [**https://doi.org/10.3390/bdcc8010006**](https://doi.org/10.3390/bdcc8010006) | 1. Data Imbalance  2. Computational Efficiency  1. Data Imbalance  2. Computational Efficiency  3. Underreporting of Identity Theft Cases | The paper aims to propose a credit card fraud detection model using ensemble machine learning techniques to effectively identify fraudulent transactions in real-world scenarios. It addresses the challenges of imbalanced datasets common in fraud detection and seeks to enhance predictive accuracy while maintaining interpretability and computational efficiency. | The research employs a blend of techniques including anomaly detection (k-means, LOF), supervised learning (decision trees, random forests, SVM), and ensemble methods to enhance credit card fraud detection. These methods leverage transaction data to identify irregularities and classify transactions, aiming to improve overall detection accuracy and efficiency. | This paper conducts an extensive review of credit card fraud, exploring various detection techniques including machine learning models like SVM, KNN, DT, RF, Bagging, and Boosting. It proposes an ensemble model combining these classifiers, showcasing robust performance in mitigating false positives and negatives. Future research should focus on improving computational efficiency, exploring deep learning integration, dynamic data sampling strategies, adversarial attack resilience, and scalability for larger datasets. |
| 7 | Credit card fraud detection in the era of disruptive technologies: A systematic review | [Journal of King Saud University - Computer and Information Sciences](https://www.sciencedirect.com/journal/journal-of-king-saud-university-computer-and-information-sciences) [Volume 35, Issue 1](https://www.sciencedirect.com/journal/journal-of-king-saud-university-computer-and-information-sciences/vol/35/issue/1), January 2023, Pages 145-174 | <https://www.sciencedirect.com/science/article/pii/S1319157822004062> | 1. Lack of real data  2.Class Imbalanced  3.Data overlapping  4.Data draft | The paper aims to analyze recent research on credit card fraud detection from 2015 to 2021, categorizing articles based on topics like class imbalance and feature engineering. By identifying gaps and challenges in existing approaches, the goal is to guide researchers in developing more effective fraud detection systems. | This paper reviews credit card fraud detection research, categorizing methods like logistic regression, decision trees, neural networks, and deep learning. It examines how advanced technologies like big data analytics, cloud computing, and IoT are integrated. The goal is to assess their effectiveness and suggest improvements to counter evolving fraud tactics. | The paper reviews 40 works on credit card fraud detection, highlighting a lack of emphasis on deep learning, big data analytics, IoT, real-time monitoring, and security. It identifies research gaps and proposes future directions, aiming to advance fraud detection methods in the digital payment landscape. |
| 8 | Developing a Credit Card Fraud Detection Model  using Machine Learning Approaches  Developing a Credit Card Fraud Detection Model  using Machine Learning Approaches | (IJACSA) International Journal of Advanced Computer Science and Applications,  Vol. 13, No. 3, 2022  (IJACSA) International Journal of Advanced Computer Science and Applications,  Vol. 13, No. 3, 2022 | <https://www.researchgate.net/publication/359635597_Developing_a_Credit_Card_Fraud_Detection_Model_using_Machine_Learning_Approaches>  <https://www.researchgate.net/publication/359635597_Developing_a_Credit_Card_Fraud_Detection_Model_using_Machine_Learning_Approaches> | 1. Dataset and preprocessing  2. Privacy preserving techniques  3.Adaption to new technologies  1. Dataset and preprocessing  2. Privacy preserving techniques  3.Adaption to new technologies  4. Scalability and Real time detection | This paper aims to develop effective credit card fraud detection models by addressing data imbalance, evaluating performance comprehensively, and implementing privacy-preserving techniques, contributing to enhanced fraud detection in e-commerce and financial systems. | This paper focuses on developing credit card fraud detection models using three supervised machine learning approaches: logistic regression, artificial intelligence, and support vector machine. It addresses data imbalance, evaluates performance using various metrics, and implements privacy-preserving techniques like principal component analysis, aiming to enhance fraud detection in e-commerce and financial systems. | This paper develops credit card fraud detection models using logistic regression, artificial intelligence, and support vector machine. It addresses data imbalance and implements privacy-preserving techniques like principal component analysis to enhance fraud detection in e-commerce and financial systems.system |