International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I1P115

Volume 73 Issue 1, 128-135, January 2025
© 2025 Seventh Sense Research Group®

Original Article

Optimizing Payment Risk with Machine Learning

Prerna Kaul[1], Abhai Pratap Singh[2]

[1]*Independent Researcher, Seattle, Washington, USA.*
[2]*Independent Researcher, Sunnyvale, California, USA.*

[2]*Corresponding Author : abhaipratapsingh1@gmail.com*

Received: 29 November 2024 Revised: 02 January 2024 Accepted: 18 January 2025 Published: 31 January 2025

Abstract - *Modern payment systems have become increasingly complex and have attracted various challenges, such as fraud risk, transaction failures, and regulatory compliance requirements. This article will discuss Machine Learning (ML) solutions that could adequately solve these problems. This study introduces two approaches: a payment risk detection model that mitigates the impact of fraudulent transactions before they happen and an alternative payment optimization model that recovers failed payments in a customer-friendly way. These systems provide considerable cost savings, improved user experiences, and regulatory compliance. It details the technical aspects, the measurable results, and the future paths available to do so, inspiring other businesses to modernize the payment experience through machine learning.*

Keywords - *Fraud risk management, Machine Learning (ML), Payment risk detection model, Transaction failures, User Experience.*

1. Introduction

The rapid proliferation of e-commerce and digital payment transactions has brought a new look and feel to the face of the payment landscape, presenting new opportunities that come with challenges for today's businesses. Indeed, in digitizing payments, seamless customer experiences have been enabled; these bring complexities such as fraud, chargebacks, credit risks, and transaction failures. These result in financial losses and, worst of all, are responsible for losing consumer trust and business reputation.[1]

It does indicate, however, that banks and eCommerce companies have already overcome some of the challenges by at least maintaining the continuity of the transaction in case of a payment outage [2]. With fraud techniques becoming increasingly sophisticated, pressures of a regulatory nature, and an introduction to much more complex operations, more robust solutions would be required. This work offers an overview of the integration of machine learning into the management of payment risk; insight is provided into how such models, driven by data, may help in fraud detection, optimization of payment success, and amplification of compliance.

Organizations can surmount such challenges across dimensions through the use of machine learning architectures, adaptive learning mechanisms(Systems that automatically update and improve their performance based on new data and experiences), and real-time analytics while balancing security and compliance with customer satisfaction.[3]

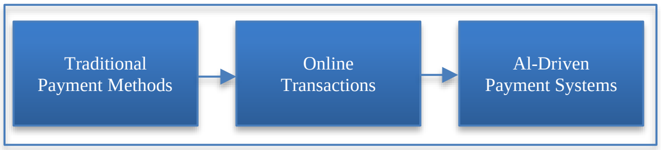

Fig. 1 Evolution of payment systems

2. Comprehensive Problem Breakdown

2.1. Payment Risk Challenges

a) Fraudulent Transactions: With the increased use of digital payment methods for goods and services, fraud techniques such as unauthorized transactions and identity theft have also been developed. Traditional rule-based systems mostly fail, requiring sophisticated machine-learning solutions for real-time detection and prevention [4].
b) Chargeback: Transfers caused by disputes of claims, which result in reversals of finances or losses in merchant credibility. Application machine learning models can show and analyze patterns of previous transactions for the prediction that minimizes such occurrences due to disputes or fraud against clients to reduce economic losses as well as maintain client trust in the system on one end and minimize fake/void transactions on the merchant end [5].
c) Credit Risk: Extending credit carries a risk of non-payment. Machine learning algorithms can analyze many data points to gauge creditworthiness, enabling better risk assessment and decision-making [6].
d) Transaction Failures: Transactions fail due to various technical and customer-related issues, lowering

customer satisfaction. Machine learning can be incorporated for prediction purposes, helping to avoid such failures and ensure a seamless payment experience [7].

2.2. Regulatory Compliance

a) Data Privacy Regulations: Companies partaking in the payment ecosystem cannot underestimate compliance with data privacy regulations such as the General Data Protection Regulation and the California Consumer Privacy Act. Design machine learning systems in such a way that processing, storage, and data protection are done responsibly, giving complete protection to sensitive information with strong controls. Differential privacy and secure multi-party computation are some techniques companies can use to improve data security while still being compliant with regulatory legislation. It protects against unauthorized access and helps to carry out fraud detection tasks without exposing fraud detection systems to users' private data. Data anonymization will also allow better modeling [9].

b) Anti-Money Laundering (AML) and Know Your Customer (KYC) Requirements: Financial institutions must comply with tight AML and KYC requirements to stop illegal activities such as money laundering and financing terrorism. Machine learning plays a vital role in automating customer verification and continued monitoring of transactions. Techniques such as Natural Language Processing (NLP), which are applied to document analysis and clustering algorithms to detect transaction patterns, decrease the need for manual effort and increase the precision of compliance [10]. Lawsuits in [10] Various ML processes: Continuous monitoring and adaptive learning mechanisms help ML models flag suspicious activities in real-time, ensuring businesses are not behind evolving threats [11]. Organizations must meet regulatory standards while ensuring operational scalability does not compromise this process.

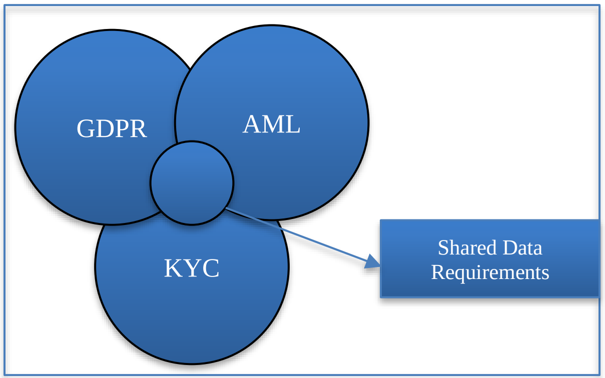

Fig. 2 Regulatory compliance overlaps

2.3. Operational Complexity

a) Balancing Security and User Experience: While stringent security protocols are imperative to prevent fraud and comply with regulations, they often compromise user experience. While strong authentication is crucial to keep companies at the front of the security arms race, customers will become frustrated and abandon transactions if it becomes too complicated — for example, when multi-factor verification is mandated. Machine Learning Solutions Through Intelligent Risk-Based Authentication These systems apply contextual information like user behavior, transaction size, and device history to adjust real-time security requirements. For example, low-risk transactions typically require only one authentication factor, whereas high-risk cases initiate further verification processes [12]. Finding the right balance between security and ease of use is essential to maintaining customer trust and decreasing cart abandonment rates.

b) Scalability and Integration: Scalability means that as business scales, with new payment technologies taken on board, the need to combine different disparate payment systems shall keep performance and ensure security. This is often inversely related to the very high volumes of transactions and sophistication in analytics expected from so many modern ML deployments. Besides those mentioned above, other examples could be microservices or a cloud-based architecture to build integrations for new incoming payment gateways and deploy fraud detection models. Besides, leveraging APIs and real-time data pipelines enables the entire ecosystem to be flexible with regard to changing business requirements.

3. Solution Overview

3.1. Payment Risk Detection Model

Objective: Implement a real-time fraud detection system that minimizes false positives while effectively identifying fraudulent transactions.

Key Features

- Scalable Architecture of Machine Learning: Use ultra-modern machine learning algorithms that comfortably process millions of transactions daily while ensuring speed in fraud detection. [14]
- Adaptive Learning Mechanisms: Embed models that learn from new fraud pattern data, changing fraudster tactics continuously. [15]
- Integrated Compliance Modules: The systems will comply with all data protection laws, such as EU-GDPR and CCPA, by integrating all compliance checks and data handling within the framework for detection.[16]
- Real-Time Analytics and Reporting: Provide immediate insights and alerts to relevant stakeholders, enabling timely action to prevent potential fraud risks.[17]

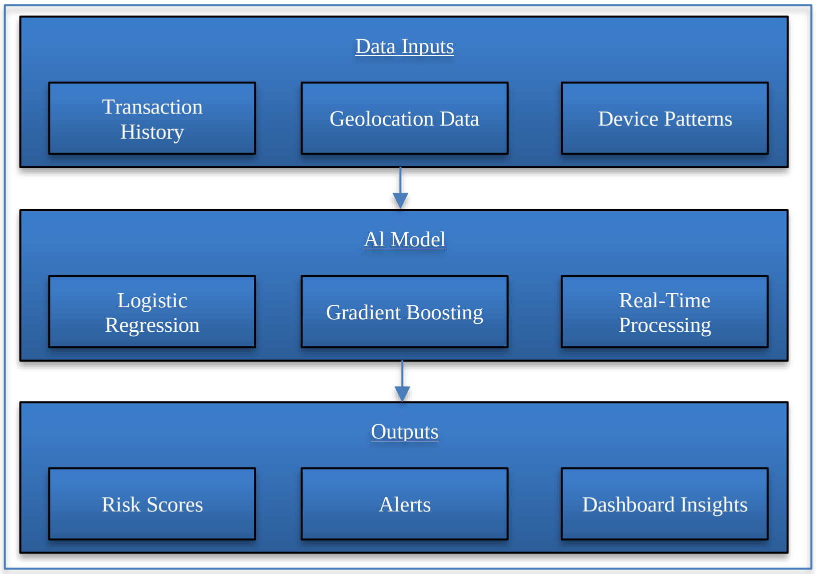

Fig. 3 Payment risk detection architecture

3.2. Alternative Payment Optimization Model

Objective: Increase transaction success rates by recommending alternative payment methods when primary options fail. These payment methods will reduce cart abandonment and improve customer satisfaction.

Use Cases:

a. Dynamic Payment Routing: Using transaction data analytics to predict customers' most likely reliable backup payment methods based on historical responses and current system status signals.
b. Personalized Payment Recommendations: This uses machine learning by personalizing payment options that best suit customers based on their preferences and historical success rates to achieve frictionless payment.
c. Multiple Payment Gateway Integration: Integrate various payment processors and allow multiple options to increase the chances of completing a transaction.
d. Real-time failure detection and recovery: This monitors transactions in real time to immediately detect any failure and proposes other means of payment. It, therefore, reduces disruptions in payment processing chains. [20]
e. Fraud and failure of transactions will be reduced by using these models, which reduces financial loss. Customers' trust will increase, and the regulatory standards will also be followed. [21]

4. Technical Deep Dive

4.1. Payment Risk Detection Model

Data Inputs

a) User Transaction History: Past transactions by a user are usually listed in detail regarding amount, frequency, and merchant categories on which a foundation of identifying anomalous behavior indicative of fraud may be laid. [22]
b) Geolocation Data: Knowledge of geographical locations where a transaction is initiated helps observe inconsistent information, such as unexpected international purchases.
c) Device patterns involve the knowledge of device usage, including device IDs and browser fingerprints, that provide much-needed context to identify unauthorized access attempts. [24]

ML Techniques

a) Ensemble Methods: This refers to when multiple algorithms are combined and predictive performance increases. By combining a linear model such as logistic regression with an ensemble approach using gradient-boosted trees, both the linear and more complex nonlinear relationships in the data are modeled. Some very successful examples of using these ensemble methods in payment fraud detection cases also exist. [25]
b) Real-Time Deployment: Deploying these models through real-time processing pipelines can execute transactions as fast as below a second latency in preparation for billions of transactions executing without negatively affecting customer or user experiences. [26]

Evaluation Metrics

a) Precision (~95%): The ratio of identified fraudulent transactions that are truly fraudulent, which is about how well the model detects a given situation. [27]
b) Recall (~90%): The performance of the model in terms of the identification of actual fraudulent transactions shows the efficiency related to capturing fraud cases. [28]
c) False Positive Rate (< 3%): It is the rate of flagged legitimate transactions as fraudulent; actually, lower is better.[29]

4.2 Alternative Payment Optimization Model

Data Inputs

a) Success rates of historical payments: Analysis of past attempted payments, showing periodicity or regularity of successful versus failed transactions. [30]

b) User Preferences: It provides insight into user preferences regarding payment methods and behavior to give recommendations. [31]

c) Network Conditions: This enables the real-time evaluation of various payment gateways with regard to their status and connectivity for better routing. [32]

ML Techniques: Collaborative Filtering with Dynamic Weighting: It proposes employing collaborative filtering algorithms, commonly used in recommendation systems, to suggest alternative payment methods similar to those other users choose. In weighted collaborative filtering, weights are put on each factor to give more or less influence to every different factor considered, regarding user preference and success rate, among others, toward better recommendation quality. [33]

Evaluation Metrics

a) Transaction Abandonment Reduction (30%): Measures the decrease in users abandoning transactions due to payment issues, indicating improved user experience. [34]

b) Chargeback Reduction (20–30%): Assesses the decline in chargeback incidents, reflecting enhanced transaction reliability and fraud prevention. [35]

5. Case Study: Implementing Scalable Payment Risk Management

Challenge: A global e-commerce platform faced certain fraud rates and transaction failures, which increased during peak sales and resulted in heavy revenue losses and operational pain. The platform was clueless about scaling up its existing payment infrastructure based on static rule-based systems to meet the ever-increasing demand for secure and seamless transactions [36].

Solution

Payment Risk Detection

- It implemented fraud detection with the use of machine learning that was able to analyze millions of transactions in real time. It was based on ensemble models that combined decision trees and logistic regression to detect abnormal patterns and unauthorized activities.[37]
- Incremental model updates were made to continuously adapt to the evolving fraud tactics, which have been robustly detected over time [38].

Alternative Payment Optimization

- Introduced a recommendation system that would suggest other modes of payment in case of failure of the primary options.
- Collaborative filtering algorithms were used to compute the most suitable fallback methods for each user, considering the record of historical success rates of multiple payment methods and real-world network conditions [39].

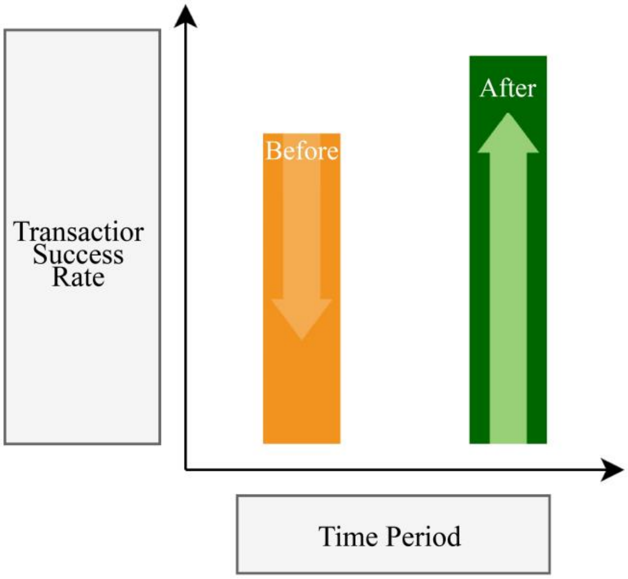

Fig. 4 Before-and-After Results in Transactions

Results

- Cost Savings: Achieved a 35% reduction in fraud-related financial losses through enhanced detection accuracy and fewer false positives [40]. Reduced operational costs by automating compliance processes, including Know Your Customer (KYC) checks and fraud reporting [41].
- Customer Impact: Retained 150,000+ transactions annually that would have been lost due to payment failures, significantly boosting customer satisfaction and loyalty [42]. Reduced transaction abandonment rates by 30%, ensuring a smoother payment experience during checkout [43].
- Scalability: The company successfully handled a 20% surge in transaction volume during holiday sales periods without performance degradation. The scalable architecture allowed seamless integration of new payment gateways and fraud detection models [43].

This technical deep dive shows how machine learning is crucial in bringing greater security and efficiency to the world of payments. This enables businesses to use rich ML models and real-time data analysis to proactively address payment risks, reduce fraud, and improve customer experience.

6. Ethical Implications in ML-driven Payment Systems

6.1. Algorithmic Bias

Algorithmic bias in ML systems raises a number of ethical issues that must be considered seriously, especially when one applies ML in assessing payment risk. First and foremost, the representation of training data has to be representative since biased datasets may result in very unfair risk scoring, whereby particular demographical groups bear a disproportionate burden. For example, historical data has been proven to contain systemic biases, which could easily propagate to ML algorithms without drawing a fair picture from the larger population [44, 45]; there are concerns about demographic fairness since discrimination against marginalized groups may be differently represented in risk factor assessment[46], leading to possibly greater risks of getting support refusals for finance. Therefore, the consequence of financial inclusion is huge because biased algorithms will further exacerbate the existing inequality and decrease access to basic financial services for those who are already under-served [47, 48].

6.2. Model Transparency

Transparency in the model will be helpful in fostering trust in ML-driven payment systems. Explainable AI techniques have started to be increasingly applied to demystify algorithms' decision-making processes and help stakeholders understand how risk scores are generated [46], [49]. Another important aspect is regulation, where financial institutions are bound by regulations that make algorithmic processes transparent [44]. Full model documentation must also be provided to enable regulators and consumers to understand how the algorithms work and their implications for fairness and accountability [50][45].

6.3. Privacy and Data Protection

Ethical handling of data in ML systems is paramount, especially with regard to privacy and data protection. Therefore, Data minimisation principles call for collecting only data necessary for specific purposes, hence decreasing the risk of misuse of the same data [47], [48]. There has to be a secure data handling practice to protect sensitive information from breaches since these cause substantial harm to individuals if they occur [51]. Also important are the consent and control of personal data by the user himself/herself: A person should have rights over his/her data regarding its usage and must be able to opt out if he/she so wishes [52] [53].

6.4. Fair Access and Financial Inclusion

However, the most important ethical issues with ML in payment systems revolve around issues of fair access and financial inclusion. Poorer sections of the population often suffer from barriers to access to financial services, and ML can mitigate or further exacerbate these problems [54]. Using alternative data sources allows the development of more inclusive risk assessments, considering the particular situation of underserved populations, hence increasing their access to credit and financial products [47, 48].

However, there should be a balance between risk management and accessibility to ensure that efforts to include marginalized groups do not affect the integrity of the financial system [46, 55].

6.5. Accountability Framework

Accountability frameworks are, therefore, important in the ethics of ML-driven payment systems. The algorithms' decision-making processes need to have mechanisms for human oversight that review and assess them regularly for any bias in them.[50, 44] This could be done by performing periodic audits for bias to show what changes have to be made in the ranking of risk assessments to assure fairness.[46, 45] Incident response mechanisms also enable an organization to respond better in case of an ethical breach of any kind, hence reinforcing accountability. [49, 53].

6.6. Future Considerations

As ML-driven payment systems evolve, so do the ethical challenges associated with them. The arriving regulations will finally shape how organizations contemplate algorithmic fairness, transparency, and accountability.[56] Therefore, it becomes the duty of the industry stakeholders to be aware of these changes and then follow best practices that keep ethical concerns at the forefront of operations. [54, 47] In conclusion, continued discourse on the impact of AI in finance shall create a balanced and inclusive financial world [47, 48]

References

[1] Robert J. Moore, and Raphael Arar, *Conversational UX Design: A Practitioner's Guide to the Natural Conversation Framework*, ACM Books, pp. 1-316, 2019. [Google Scholar] [Publisher Link]

[2] A. Saputra and S. Suharjito, “Fraud Detection using Machine Learning in E-Commerce,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 9, pp. 1-8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ajay Vikram Singh et al., “Machine-Learning-based approach to Decode the Influence of Nanomaterial Properties on their Interaction with Cells,” *ACS Applied Materials & Interfaces*, vol. 13, no. 1, pp. 1943-1955, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ebenezer Esenogho et al., “A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection,” *IEEE Access*, vol. 10, p. 16400-16407, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Fumiko Hayashi, Zach Markiewicz, and Richard J. Sullivan, “Chargebacks: Another Payment Card Acceptance Cost for Merchants,” *SSRN Electronic Journal*, pp. 1-72, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[6] Trilok Nath Pandey et al., “Machine Learning-Based Classifiers Ensemble for Credit Risk Assessment,” *International Journal of Electronic Finance*, vol. 7, no. 3-4, p. 227-249, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[7] KamalaKanta Mishra, and Sachin Kumar Manjhi, “Failure Prediction Model for Predictive Maintenance,” *2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, Bangalore, India, pp. 72-75, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sahar Bhaimia, “The General Data Protection Regulation: the Next Generation of EU Data Protection,” *Legal Information Management*, vol. 18, no. 1, pp. 21-28, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[9] Benjamin C.M. Fung, Ke Wang, and Philip S. Yu, “Anonymizing Classification Data for Privacy Preservation,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 5, pp. 711-725, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[10] Etinosa Igbinenikaro, and Adefolake Olachi Adewusi, “Financial Law: Policy Frameworks for Regulating Fintech Innovations: Ensuring Consumer Protection While Fostering Innovation,” *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 515-530, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Devraj Basu, and Godsway Korku Tetteh, “*Using Automation and AI to Combat Money Laundering*,” FRIL White Paper Series, University of Strathclyde, pp. 1-17, 2024. [Google Scholar] [Publisher Link]

[12] Joseph Bonneau et al., “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” *2012 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, pp. 553-567, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[13] Eric Amankwa, Marianne Loock, and Elmarie Kritzinger, “Enhancing Information Security Education and Awareness: Proposed Characteristics for a Model,” *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, Cape Town, South Africa, pp. 72-77, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[14] Richard J. Bolton, and David J. Hand, “Statistical Fraud Detection: A Review,” *Statistical Science*, vol. 17, no. 3, pp. 235-255, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[15] Siddhartha Bhattacharyya et al., “Data Mining for Credit Card Fraud: A Comparative Study,” *Decision Support Systems*, vol. 50, no. 3, pp. 602-613, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[16] O. Sohaib, H. Lu, and W. Hussain, “Internet of Things (IoT) in E-Commerce: For People with Disabilities,” *2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, Siem Reap, Cambodia, pp. 419-423, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[17] Purva Grover, and Arpan Kumar Kar, “Big Data Analytics: A Review on Theoretical Contributions and Tools Used in Literature,” *Global Journal of Flexible Systems Management*, vol. 18, pp. 203-229, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[18] Geetha Manoharan et al., “Fraud Detection in E-commerce Transactions: A Machine Learning Perspective,” *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Chennai, India, pp. 1-5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Vivek Bagaria, Joachim Neu, and David Tse, “Boomerang: Redundancy Improves Latency and Throughput in Payment-Channel Networks,” *Financial Cryptography and Data Security: 24th International Conference*, Kota Kinabalu, Malaysia, pp. 304-324, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Denis Leite et al., “An Automated Machine Learning Approach for Real-Time Fault Detection and Diagnosis,” *Sensors*, vol. 22, no. 16, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Susie Xi Rao et al., “xFraud: Explainable Fraud Transaction Detection,” *Arxiv*, pp. 1-27, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Mohammad Reza Nosouhi et al., “Blockchain for Secure Location Verification,” *Journal of Parallel and Distributed Computing*, vol. 136, pp. 40-51, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Antoine Vastel et al., “FP-STALKER: Tracking Browser Fingerprint Evolutions,” *2018 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, pp. 728-741, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Jerome H. Friedman, “Greedy Function Approximation: A Gradient Boosting Machine,” *The Annals of Statistics*, vol. 29, no. 5, pp. 1189-1232, 2001. [Google Scholar] [Publisher Link]

[25] Andrei Paleyes, Raoul Gabriel Urma, and Neil D. Lawrence, “Challenges in Deploying Machine Learning: A Survey of Case Studies,” *ACM Computing Surveys*, vol. 55, no. 6, pp. 1-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Patrick Wessa, and Bart Baesens, “Fraud Detection in Statistics Education Based on the Compendium Platform and Reproducible Computing,” *2009 WRI World Congress on Computer Science and Information Engineering, Los Angeles*, CA, USA, pp. 50-54, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[27] Kalaivani Balaji et al., “Improved Fraud Detection in Banking Systems through Machine Learning and Big Data Analytics with Management Key Components,” *2024 International Conference on Advances in Computing, Communication and Applied Informatics*, Chennai, India, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] Rob Matheson, Reducing False Positives in Credit card Fraud Detection, MIT News, 2018. [Online]. Available: https://news.mit.edu/2018/machine-learning-financial-credit-card-fraud-0920

[29] Puja Agrawal, and Urvashi Tiwari, “Real-time Data Analytics for Financial Decision Making,” *International Journal of Research and Analytical Reviews*, vol. 6, no. 1, pp. 149-154, 2019. [Publisher Link]

[30] Mia Olsen, Jonas Hedman, and Ravi Vatrapu, “Designing Digital Payment Artifacts,” *ICEC '12: Proceedings of the 14th Annual International Conference on Electronic Commerce*, Singapore, pp. 161-168, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[31] Lifan Mei et al., “Realtime Mobile Bandwidth Prediction Using LSTM Neural Network,” *Lecture Notes in Computer Science*, vol. 11419, pp. 34-47, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[32] Haobo Wang et al., “Collaboration Based Multi-Label Propagation for Fraud Detection,” *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence*, pp. 2477-2483, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[33] Heng Tang, and Xiaowan Lin, “Curbing Shopping Cart Abandonment in C2C Markets — An Uncertainty Reduction Approach,” *Electronic Markets*, vol. 29, pp. 533-552, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[34] E.W.T. Ngai et al., “The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature,” *Decision Support Systems*, vol. 50, no. 3, pp. 559-569, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[35] Leo Breiman, “Random Forests,” *Machine Learning*, vol. 45, pp. 5-32, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[36] Charu C. Aggarwal, *Data Streams: Models and Algorithms*, Springer New York, NY, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[37] G. Adomavicius, and A. Tuzhilin, “Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 6, pp. 734-749, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[38] Philip Kin Wah Chan, and Salvatore Stolfo, “Toward Scalable Learning with Non-Uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection,” *Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining*, New York NY, pp. 164-168, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[39] Marc Vartabedian, AI Can Take the Slog out of Compliance Work, but Executives Not Ready to Fully Trust it, The Wall Street Journal, 2024. [Online]. Available: https://www.wsj.com/articles/ai-can-take-the-slog-out-of-compliance-work-but-executives-not-ready-to-fully-trust-it-7cd60a16

[40] Iuliia Moroz, Six eCommerce Customer Retention Strategies That Work, Support Your App, 2024. [Online]. Available: https://supportyourapp.com/blog/ecommerce-customer-retention-strategies/

[41] Matt McFarland, These Smart Shopping Carts will let you Skip the Grocery Store Line, CNN Business, 2019. [Online]. Available: https://edition.cnn.com/2019/12/23/tech/smart-shopping-cart/index.html

[42] Xiaoxue Zhang, Shouqian Shi, and Chen Qian, “WebFlow: Scalable and Decentralized Routing for Payment Channel Networks with High Resource Utilization,” *Arxiv*, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[43] Fabio Motoki, Valdemar Pinho Neto, and Victor Rodrigues, “More Human than Human: Measuring ChatGPT Political Bias,” *Public Choice*, vol. 198, pp. 3-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[44] McKane Andrus, and Sarah Villeneuve, “Demographic-Reliant Algorithmic Fairness: Characterizing the Risks of Demographic Data Collection in the Pursuit of Fairness,” *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, Seoul Republic of Korea, pp. 1709-1721, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[45] Nikita Kozodoi, Johannes Jacob, and Stefan Lessmann, “Fairness in Credit Scoring: Assessment, Implementation and Profit Implications,” *European Journal of Operational Research*, vol. 297, no. 3, pp. 1083-1094, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[46] Temitayo Oluwaseun Jejeniwa, Noluthando Zamanjomane Mhlongo, and Titilola Olaide Jejeniwa, “AI Solutions for Developmental Economics: Opportunities and Challenges in Financial Inclusion and Poverty Alleviation,” *International Journal of Advanced Economics*, vol. 6, no. 4, pp. 108-123, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[47] Omotayo Bukola Adeoye et al., “Leveraging AI and Data Analytics for Enhancing Financial Inclusion in Developing Economies,” *Finance & Accounting Research Journal*, vol. 6, no. 3, pp. 288-303, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[48] Vaibhav Sinha, Ajit Kumar, and Tuhin Siddharth, “The Effect of Artificial Intelligence on Digital Financial Inclusion in India,” *Journal of Informatics Education and Research*, vol. 3, no. 2, pp. 2366-2371, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[49] Richard Berk et al., "Fairness in Criminal Justice Risk Assessments: The State of the Art,” *Sociological Methods & Research*, vol. 50, no. 1, pp. 3-44, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[50] Richard A. Berk, Arun Kumar Kuchibhotla, and Eric Tchetgen Tchetgen, "Improving Fairness in Criminal Justice Algorithmic Risk Assessments Using Optimal Transport and Conformal Prediction Sets,” *Sociological Methods & Research*, vol. 53, no. 4, pp. 1629-1675, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[51] Joaquina C Baranda et al., “Expanding Access to Early Phase Trials: The CATCH-UP.2020 Experience,” *JNCI Cancer Spectrum*, vol. 7, no. 1, pp. 1-7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[52] Anushree Tiwari et al., “Artificial Intelligence in Oral Health Surveillance among under-Served Communities,” *Biomedical Informatics*, vol. 19, no. 13, pp. 1329-1335, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[53] Brittney Crock Bauerly et al., “Broadband Access as a Public Health Issue: The Role of Law in Expanding Broadband Access and Connecting Underserved Communities for Better Health Outcomes,” *The Journal of Law Medicine & Ethics*, vol. 47, no. S2, pp. 39-42, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[54] Diane Longhurst Johnson, and Courtney Grant Davis, “Bridging the Gap for Underserved Populations: Personalized AI Solutions for College Access and Learning Support,” *New Directions for Higher Education*, vol. 2024, no. 207, pp. 47-62, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[55] Jonathan Xin Wang et al., “Health Equity in Artificial Intelligence and Primary Care Research: Protocol for a Scoping Review,” *JMIR Research Protocols*, vol. 10, no. 9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[56] Ansarullah Hasas et al., "AI for Social Good: Leveraging Artificial Intelligence for Community Development,” *Journal of Community Service and Society Empowerment*, vol. 2, no. 2, pp. 196-210, 2024. [CrossRef] [Google Scholar] [Publisher Link]