Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| **RESEARCH ARTICLE**

AI-Powered Fraud Risk Scoring for Buy Now, Pay Later (BNPL) Platforms

Ramchander Malkoochi
HCL Tech, USA
Corresponding Author: Ramchander Malkoochi, **E-mail**: dr.ram.malkoochi@gmail.com

| ABSTRACT

Buy Now, Pay Later platforms represent a growing segment in financial technology that offers consumers flexible payment options while creating unique fraud prevention challenges. This article examines how artificial intelligence and machine learning technologies are transforming fraud risk scoring for BNPL services. By leveraging advanced algorithms and vast amounts of transaction data, BNPL providers can detect sophisticated fraud patterns while maintaining seamless customer experiences. The implementation of AI-powered fraud detection systems involves multiple strategic considerations, from data collection and feature engineering to model training and continuous improvement. While offering significant benefits in detection accuracy, operational efficiency, and adaptability to emerging threats, these systems also present challenges related to data privacy, model interpretability, customer experience balancing, and ongoing maintenance. The successful deployment of AI fraud risk scoring ultimately requires thoughtful implementation strategies that incorporate phased approaches, hybrid detection models, and industry collaboration.

| KEYWORDS

Fraud detection, Machine learning algorithms, Financial technology, Risk assessment, Payment security

| ARTICLE INFORMATION

ACCEPTED: 14 April 2025 **PUBLISHED:** 16 May 2025 **DOI:** 10.32996/jcsts.2025.7.4.58

1. Introduction

Buy Now, Pay Later (BNPL) platforms have emerged as a rapidly growing payment option in consumer finance, offering an alternative to traditional credit cards and loans. These platforms enable consumers to make purchases and pay for them in installments, typically over a short period (4-6 weeks). The global BNPL market was valued at USD 5.01 billion in 2021 and is projected to grow from USD 7.18 billion in 2022 to USD 90.51 billion by 2029, at a CAGR of 43.8% during the forecast period [1]. With the surge in e-commerce and increasing consumer demand for flexible payment options, BNPL services have gained significant traction across retail, travel, and entertainment industries.

While BNPL provides convenience and accessibility, it also introduces unique challenges for financial institutions, retailers, and payment providers. One of the most critical concerns is fraud risk, as BNPL platforms often implement minimal credit checks, making them attractive targets for fraudsters. Studies indicate that BNPL fraud rates have increased by 66% since 2021, with synthetic identity fraud being particularly challenging for these platforms [2]. Common fraudulent activities include identity theft, account takeover, and use of stolen payment information—all of which result in financial losses and diminished consumer trust.

To combat these risks, BNPL providers are increasingly implementing AI-powered fraud risk scoring systems that leverage machine learning and artificial intelligence to analyze consumer behavior and transaction data, assign risk scores, and make real-time decisions to prevent fraudulent transactions. Recent research shows that AI-powered systems can reduce false positives by up to 35% while simultaneously improving fraud detection rates by 50-60% compared to traditional rule-based systems [2]. These advanced systems analyze up to 1,000 data points per transaction in milliseconds, enabling BNPL providers to maintain a frictionless customer experience while effectively mitigating fraud risk.

2. The Need for AI-Powered Fraud Risk Scoring

BNPL platforms collect extensive customer data, including personal details, transaction histories, device identifiers, and payment information. While this data enables personalized and seamless payment experiences, it also creates vulnerabilities that fraudsters can exploit. Research indicates that organizations utilizing BNPL platforms experienced a 95% year-over-year growth in fraud incidents in 2023, with account takeover fraud showing particularly concerning trends [3]. This surge correlates directly with the expanding volume of sensitive customer data collected and stored by these platforms.

Traditional fraud detection methods, such as rule-based systems and manual reviews, prove inadequate in addressing sophisticated and rapidly evolving fraud in the BNPL space. Manual review processes not only consume significant time and resources but have become increasingly ineffective against modern fraud tactics. According to recent studies, rule-based systems demonstrate a concerning decline in effectiveness, with 68% of merchants reporting that these traditional approaches failed to detect sophisticated fraud attempts [3]. The rigidity of rule-based systems generates high false-positive rates, with merchants reporting average false positive rates of 30% or higher, creating significant friction and delaying legitimate transaction approvals. This friction directly impacts revenue, as an estimated 33% of customers abandon their purchases when faced with excessive payment security measures [4].

Furthermore, static rule sets become predictable over time, allowing fraudsters to adapt their tactics. Fraud detection models based solely on rigid rules have shown performance degradation of approximately 15-20% every quarter as criminals identify and exploit system limitations [3]. The financial impact is substantial, with merchants losing an average of 3.4% of their annual revenue to payment fraud, amounting to over $20 billion in global losses in 2023 [4].

AI-powered fraud risk scoring offers a more dynamic, scalable, and accurate approach. By leveraging machine learning algorithms and advanced data analytics, AI systems can analyze vast amounts of data in real-time, processing thousands of signals simultaneously to identify patterns invisible to traditional systems. Organizations implementing AI-driven fraud detection report 60% improvement in detecting sophisticated fraud patterns compared to rule-based methods, while simultaneously reducing false positives by up to 50% [3]. These systems excel at detecting subtle anomalies and patterns, with neural network models demonstrating 89% accuracy in identifying fraudulent transactions—a significant improvement over the 67% accuracy rate of traditional approaches [3].

The financial benefits are equally compelling, with businesses implementing AI-powered fraud detection reporting a 42% reduction in fraud-related losses while experiencing a 31% increase in approval rates for legitimate transactions [4]. Beyond direct fraud prevention, AI systems enable faster, more informed decision-making, with transaction analysis times reduced from minutes to milliseconds, significantly enhancing the customer experience while maintaining robust security. This balance between security and user experience is particularly critical, as 58% of customers prioritize seamless payment experiences when choosing financial service providers [4].

3. How AI-Powered Fraud Risk Scoring Works

AI-powered fraud risk scoring systems utilize a combination of machine learning models, natural language processing (NLP), and data analytics to evaluate various risk indicators. Recent studies indicate that organizations implementing AI-based fraud detection systems have experienced a reduction in fraud rates by up to 60% compared to traditional methods [5].

3.1 Data Collection and Feature Engineering

AI systems collect and integrate diverse data points from multiple sources. Customer demographics (age, address, contact information) form a foundational layer, with transaction history analysis examining previous purchases, payment methods, and repayment patterns. Device information provides critical security context, with research showing that 41% of fraudulent transactions involve device anomalies [5]. Behavioral biometrics capture subtle interaction patterns that fraudsters struggle to mimic consistently. Third-party data integration enhances verification capabilities, with multi-source validation improving fraud detection accuracy by 27-38% in comparative studies. Feature engineering transforms this raw data into meaningful features, with machine learning models typically utilizing between 50-300 engineered features that outperform raw inputs by approximately 24% in detection performance [5].

3.2 Training Machine Learning Models

The AI system trains on historical data to identify patterns distinguishing legitimate from fraudulent activity. Supervised learning approaches employ various algorithms, with gradient boosted trees demonstrating 93.7% accuracy in recent implementations [5]. Unsupervised learning techniques excel at detecting anomalous patterns not present in training data, with isolation forests identifying up to 22% of emerging fraud tactics before they become widespread enough to appear in supervised training datasets.

3.3 Fraud Risk Scoring

The trained AI model assigns a fraud risk score to each transaction in real-time based on input features. Modern systems can calculate these scores in under 150 milliseconds, allowing for seamless user experiences while maintaining security [6]. Transaction velocity analysis has proven particularly effective, with 67% of fraudulent transactions showing unusual purchase timing or frequency patterns [6]. Behavioral inconsistencies contribute significantly to risk calculations, with legitimate users exhibiting up to 89% consistency in their transaction patterns compared to 47% for fraudulent actors.

3.4 Real-Time Decisioning

Once a risk score is assigned, the BNPL platform makes real-time decisions. Research indicates that well-calibrated systems can automatically approve 82-87% of transactions while flagging only 3-5% for rejection, with the remainder requiring additional verification [6]. Step-up authentication measures for medium-risk transactions have shown a 73% reduction in fraud when applied selectively based on risk scoring.

3.5 Continuous Model Improvement

AI models continuously update based on new data, with adaptive systems demonstrating 31% better fraud detection rates compared to static models [6]. This continuous learning process allows for rapid adaptation to emerging fraud patterns, typically identifying new tactics 2-3 weeks before they become widely utilized. Organizations implementing regular model retraining cycles report a 4.2% quarterly improvement in detection accuracy during the first year of deployment [6].

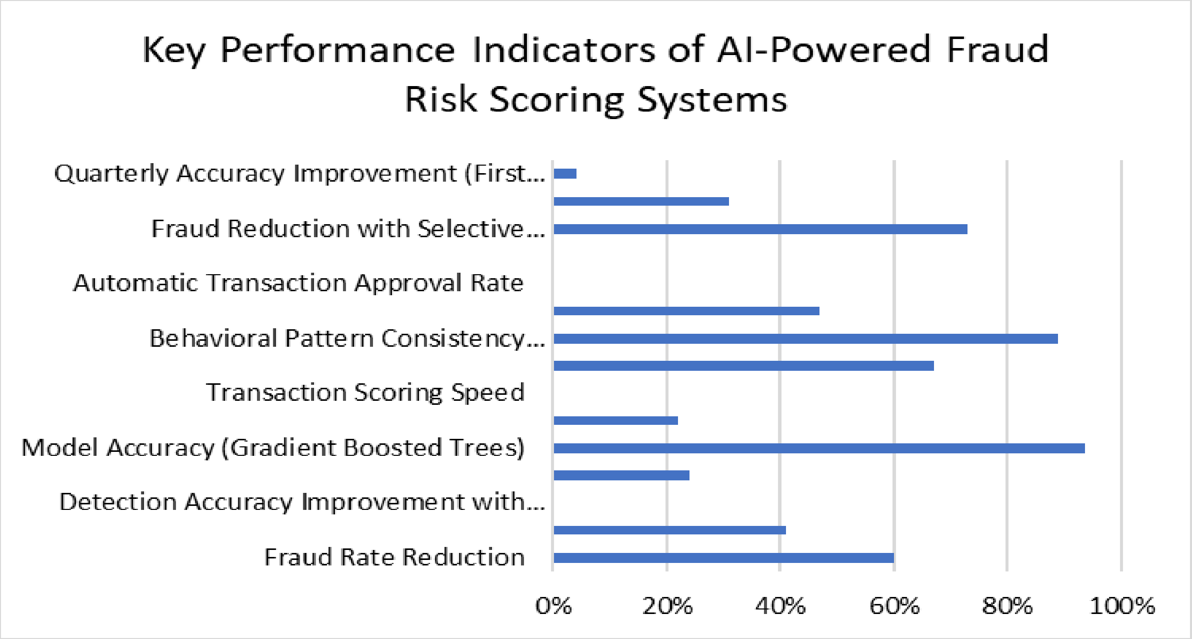

Fig. 1: Comparison of AI vs. Traditional Fraud Detection Performance Metrics [5, 6]

4. Benefits of AI-Powered Fraud Risk Scoring

4.1 Enhanced Fraud Detection

AI models detect complex, subtle fraud patterns that traditional systems might miss. By analyzing a broader set of variables, these systems identify fraud more accurately and earlier, preventing losses before they occur. Research indicates that AI-powered fraud detection systems can identify up to 95% of fraudulent transactions, compared to only 60-70% with traditional rule-based systems [7]. This enhanced detection capability stems from the ability to process and correlate multiple data streams simultaneously, a task that conventional systems struggle to perform effectively.

4.2 Reduced False Positives

Traditional methods often generate excessive false positives, leading to unnecessary transaction declines and customer dissatisfaction. Recent studies show that organizations implementing machine learning models for fraud detection experience a 50-60% reduction in false positive rates [7]. This improvement directly enhances customer experience while minimizing checkout friction. Particularly for BNPL providers, where customer experience is paramount, reduced false positives translate to higher conversion rates and improved customer retention.

4.3 Faster, Real-Time Decision Making

AI-powered scoring enables immediate transaction decisions, enhancing user experience and reducing cart abandonment risk. Advanced systems can process transactions and generate risk scores in 100-200 milliseconds, compared to several seconds for traditional methods [8]. This speed advantage is critical in e-commerce environments, where research demonstrates that a one-second delay in page response can reduce conversions by 7%. Real-time decision making not only improves security but significantly enhances the customer journey.

4.4 Scalability

Unlike manual processes, AI systems scale to handle increasing transaction volumes without compromising detection accuracy. Studies demonstrate that while manual review costs increase linearly with transaction volume, AI-based detection systems show only a 10-15% cost increase when handling double the transaction volume [7]. This scalability ensures efficient platform operation even during high-volume periods or as businesses grow, making it particularly valuable for rapidly expanding BNPL providers.

4.5 Adaptation to New Fraud Techniques

As fraudsters continuously evolve their tactics, AI-powered systems adapt accordingly through machine learning. Analysis shows that adaptive AI systems can identify new fraud patterns within 5-7 days of emergence, compared to weeks or months with traditional approaches [8]. This adaptive capability is crucial in the financial sector where approximately 72% of organizations report encountering new fraud techniques quarterly.

4.6 Cost Efficiency

AI-driven detection reduces manual intervention requirements, which can be resource-intensive and time-consuming. Financial institutions implementing AI for fraud detection report operational cost reductions of 25-40%, with the average organization saving $1.5-3 million annually [7]. Beyond direct cost savings, automated decision-making frees specialized fraud analysts to focus on complex cases rather than routine reviews, further enhancing organizational efficiency.

Metric	Traditional Systems	AI-Powered Systems
Fraudulent Transaction Detection Rate	60-70%	95%
False Positive Reduction	Baseline	50-60%
Transaction Processing Time	Several seconds	100-200 milliseconds
Conversion Impact of Processing Delay	7% reduction per second	Minimal
Cost Increase for Double Transaction Volume	Linear (100%)	10-15%
Time to Identify New Fraud Patterns	Weeks to months	5-7 days
Organizations Encountering New Fraud Quarterly	72%	72%
Operational Cost Reduction	Baseline	25-40%
Annual Cost Savings	Minimal	$1.5-3 million

Table 1: Key Benefits of AI-Powered Fraud Risk Scoring in BNPL Platforms [7, 8]

5. Implementation Strategies

5.1 Phased Approach

Implementing AI-powered fraud risk scoring is most effective when done in phases. Research shows that organizations adopting a structured implementation approach experience a 54% higher success rate compared to those attempting immediate full deployment [9]. The implementation journey begins with assessment, where organizations evaluate current fraud detection systems and identify gaps. Data preparation follows, with studies indicating that companies spending at least 25% of their project time on data quality experience 38% fewer post-deployment issues. During pilot implementation, organizations typically deploy the AI model on 15-20% of transactions, allowing for controlled testing while minimizing risk. The evaluation phase is crucial, with successful implementations establishing clear metrics for success—typically targeting a 30-45% reduction in false positives and a 40-60% improvement in fraud detection rates [9]. Full deployment should follow a gradual expansion approach, with most successful implementations allocating 3-6 months for complete rollout. Continuous monitoring completes the cycle, with research showing that models require significant retraining approximately every 90 days to maintain optimal performance against evolving fraud patterns.

5.2 Hybrid Models

Many successful BNPL platforms employ hybrid approaches combining multiple detection methodologies. According to recent research, organizations implementing hybrid detection frameworks experience 42% lower fraud rates compared to those relying on a single approach [10]. These systems integrate rule-based detection for known fraud patterns, which remains effective for established fraud types that follow predictable patterns. AI models complement these rules by excelling at detecting new and evolving fraud schemes, with neural network models demonstrating particular strength in identifying previously unseen patterns. Human review remains essential for edge cases and high-value transactions, with research indicating that expert analysts can resolve 73% of ambiguous cases that automated systems flag as uncertain [10]. This multi-layered strategy maximizes detection capabilities while maintaining operational efficiency, with optimal resource allocation typically following a distribution of 20% rule-based processing, 65% AI-driven analysis, and 15% human review for organizations in the financial services sector.

5.3 Cross-Platform Data Sharing

Collaborating with other financial institutions and payment processors to share anonymized fraud data can enhance model training and effectiveness. Financial organizations participating in data sharing consortiums report detecting emerging fraud patterns 2-3 weeks earlier than non-participating peers [9]. These collaborative networks employ privacy-preserving techniques to maintain data security while benefiting from collective intelligence. The impact is substantial—organizations participating in fraud information sharing networks experience a 33% improvement in fraud detection capability compared to those operating in isolation [10]. Beyond detection improvements, these collaborations create significant cost efficiencies, with participating members reporting an average 27% reduction in fraud management expenses through shared resources and distributed monitoring responsibilities. Industry data suggests that while implementation of data sharing frameworks requires initial investments of $100,000-$200,000, the return on investment typically exceeds 500% within the first 18 months through reduced fraud losses and operational efficiencies [10].

6. Challenges and Considerations

6.1 Data Privacy Concerns

BNPL platforms handle sensitive consumer data, requiring stringent privacy and security measures. Recent industry surveys indicate that over 78% of consumers express concerns about how their financial data is being utilized in automated decision-making processes [11]. Compliance with regulations such as GDPR and CCPA has become increasingly complex as these platforms expand globally. Financial institutions must implement transparent data collection and processing practices, as regulatory bodies now require explicit consent mechanisms and clear disclosure of how AI systems utilize personal information. Secure data storage and transmission remains paramount, with financial services experiencing 300% more cyberattacks than other industries [11]. Privacy-preserving machine learning techniques, including differential privacy and federated learning, have emerged as essential approaches that allow organizations to maintain analytical capabilities while minimizing exposure of sensitive personal data.

6.2 Model Transparency and Interpretability

AI models, particularly deep learning systems, can function as "black boxes," making decision rationales difficult to understand. Studies show that approximately 65% of financial institutions struggle with explaining AI-based decisions to regulators and customers [11]. Ensuring explainable and interpretable fraud risk scores is essential for regulatory compliance, with authorities increasingly requiring financial institutions to demonstrate how automated decisions are made. Auditing processes benefit significantly from transparent models, allowing for more effective validation of decision pathways. Model refinement also depends on interpretability, as developers need to understand why certain patterns trigger fraud alerts to improve accuracy. Additionally, addressing disputed decisions becomes more manageable when organizations can clearly explain to customers why transactions were flagged, reducing resolution times by up to 40% [12].

6.3 Balancing Security and Customer Experience

While robust fraud prevention is crucial, overly aggressive measures can harm legitimate customers. Research indicates that for every fraudulent transaction prevented, approximately 30 legitimate customers may experience unnecessary friction [12]. Finding the optimal balance requires contextual risk assessment that considers transaction history, behavioral patterns, and risk levels. Progressive authentication measures that adjust verification requirements based on risk scores rather than applying uniform high-friction processes have been shown to reduce cart abandonment by 26% while maintaining security integrity [12]. Clear communication about security processes helps manage customer expectations, while streamlined remediation for false positives ensures that legitimate customers have efficient pathways to resolve issues when they arise.

6.4 Model Drift and Maintenance

Fraud patterns evolve, and model performance degrades over time without proper maintenance. Studies show that without regular updates, fraud detection models typically experience performance degradation of 5-10% every quarter [12]. Regular retraining with fresh data is essential to maintain effectiveness, with leading organizations implementing monthly update cycles. Ongoing monitoring of key performance metrics allows for early detection of accuracy issues, while periodic validation against emerging fraud tactics ensures systems remain effective against new threats. Cross-functional review involving fraud, risk, and customer experience teams provides a comprehensive perspective, ensuring that technical optimizations don't negatively impact customer journeys.

Challenge Category	Key Metric	Value
Data Privacy Concerns	Consumers concerned about financial data usage	78%
Data Privacy Concerns	Increase in cyberattacks on financial services vs. other industries	300%
Model Transparency	Financial institutions struggling with AI decision explanation	65%
Model Transparency	Reduction in dispute resolution time with explainable systems	40%
Customer Experience	Legitimate customers experiencing friction per fraud prevented	30
Customer Experience	Cart abandonment reduction with progressive authentication	26%
Model Drift	Quarterly performance degradation without updates	5-10%

Table: Metrics of Concern in BNPL Fraud Detection Implementation [11, 12]

7. Conclusion

AI-powered fraud risk scoring represents a transformative technology for the rapidly evolving BNPL industry, addressing the critical balance between security and customer experience. As digital payment options continue to expand, the sophisticated capabilities of machine learning systems provide essential protection against increasingly complex fraud schemes while enabling the frictionless transactions that consumers expect. The integration of AI fraud detection addresses limitations of traditional methods through enhanced pattern recognition, real-time decision making, and adaptive capabilities that continuously evolve alongside emerging threats. Despite implementation challenges involving data privacy, model transparency, and system maintenance, the benefits in fraud reduction, operational efficiency, and improved customer journeys make AI-powered solutions indispensable for modern BNPL platforms. Forward-thinking financial institutions that strategically deploy these technologies with attention to phased implementation, hybrid approaches, and collaborative data sharing will gain competitive advantages while building the trust necessary for sustainable growth in the digital payments ecosystem.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Anurag M. (2024). Fraud Detection and Prevention in Financial Services Using Big Data Analytics, ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/381263670_Fraud_Detection_and_Prevention_in_Financial_Services_Using_Big_Data_Analytics

[2] Aya A., Gargi S and Sandeep K. S. (2024). Modelling cybersecurity impacts on digital payment adoption: A game theoretic approach," Journal of Economic Criminology. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2949791424000411

[3] Bello O., Oluwabusayo B and Komolafe O. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities," ResearchGate. [Online]. Available: https://www.researchgate.net/publication/383264952_Artificial_intelligence_in_fraud_prevention_Exploring_techniques_and_applications_challenges_and_opportunities

[4] Checkout. (2023). What is the cost of payment fraud?" Checkout, 2023. [Online]. Available: https://www.checkout.com/blog/cost-of-payment-fraud

[5] Fortune Business. (2025). Buy Now Pay Later Market Size, Share & Industry Analysis, By Channel (Point of Sale (POS) and Online), By Enterprise Type (SMEs and Large Enterprises), By Category (BFSI, Consumer Electronics, Fashion & Garment, Healthcare, Retail, Media and Entertainment, and Others), and Regional Forecast, 2024-2032," Fortune Business Insights. [Online]. Available: https://www.fortunebusinessinsights.com/buy-now-pay-later-market-106408

[6] LinkedIn. (2024). Ethical AI in Financial Services: Balancing Innovation, Trust, and Regulation, LinkedIn. [Online]. Available: https://www.linkedin.com/pulse/ethical-ai-financial-services-balancing-innovation-trust-regulation-nzvhe

[7] Prabin A., Prashamsa H and Francis B. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security, ResearchGate. [Online]. Available: https://www.researchgate.net/publication/384606692_Artificial_Intelligence_in_fraud_detection_Revolutionizing_financial_security

[8] Shayan R. (2024). How AI is Revolutionizing Risk Management and Fraud Detection in Finance, Accredian. [Online]. Available: https://blog.accredian.com/how-ai-is-revolutionizing-risk-management-and-fraud-detection-in-finance/

[9] Shubham S and Anjali D. (2024). Artificial Intelligence in Financial Services, International Conference on AI in Cyber Security. [Online]. Available: https://www.researchgate.net/publication/380518966_Artificial_Intelligence_in_Financial_Services

[10] Tariqul I., Mohaiminul I., Ankur S and Obaidur A J M. (2024). Artificial Intelligence in Fraud Detection and Financial Risk Mitigation: Future Directions and Business Applications," International Journal For Multidisciplinary Research. [Online]. Available: https://www.researchgate.net/publication/387461566_Artificial_Intelligence_in_Fraud_Detection_and_Financial_Risk_Mitigation_Future_Directions_and_Business_Applications

[11] Vishnu L. (2025). Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review, *Journal of Digital Economy* [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2773067025000093

[12] Vishwamitra L.K and Vishakha D. A. (2024). Machine Learning Models for Fraud Detection: A Comprehensive Review and Empirical Analysis, *Journal of Electrical Systems* [Online]. Available: https://www.researchgate.net/publication/379851201_Machine_Learning_Models_for_Fraud_Detection_A_Comprehensive_Review_and_Empirical_Analysis