Review

Not peer-reviewed version

Anatomy of Peer-to-Peer (P2P) Lending Fraud: A Review with Managerial Implications

Ioana Florina Coita *, Marcos Machado, Lucia Gomez, Karsten Wenzlaff, Wouter van Heeswijk, Frederik Sinan Bernard, Marius Vlad Pop, Joerg Osterrieder

Posted Date: 15 September 2025

doi: 10.20944/preprints202509.1144.v1

Keywords: P2P lending; fraud; machine learning; systematic literature review

Review

Anatomy of Peer-to-Peer (P2P) Lending Fraud: A Review with Managerial Implications

Marcos R. Machado [1,*], Ioana Florina Coita [2,3,4,*], Lucia Gomez [5], Karsten Wenzlaff [6,7,8], Wouter van Heeswijk [1], Frédérik Sinan Bernard [1], Marius Vlad Pop [2] and Joerg Osterrieder [1]

[1] University of Twente, Department of Industrial Engineering and Business Information Systems, AE Enschede 7500, Netherlands
[2] University of Oradea, Department of Finance and Accounting, Universitatii street, No. 1, Oradea 410100, Romania
[3] University of Economics in Bratislava, Bratislava 852 35, SK
[4] University of Sofia, St. Kliment Ohridski, Sofia 1504, BG
[5] Bern University of Applied Sciences, Institute of Applied Data Science & Finance, Brückenstrasse 73, Bern 3005, Switzerland
[6] Hamburg University, Faculty of Business, Economics, and Social Sciences, Hamburg 34396,Germany
[7] University of Cambridge, Cambridge Centre for Alternative Finance, Cambridge 1QA, United Kingdom
[8] University of Utrecht, European Centre for Alternative Finance, Utrecht 3584CS, Netherlands
* Correspondence: m.r.machado@utwente.nl (M.R.M.); coita.iflorina@gmail.com (I.F.C.); Tel.: +31 534899045 (M.R.M.); +40744369226 (I.F.C.)

Abstract

Peer-to-peer (P2P) lending platforms have transformed the financial technology sector by facilitating direct interactions between borrowers and lenders, eliminating the need for traditional financial intermediaries. While this innovation enhances financial inclusion and efficiency, it is subject to significant fraud risks such as identity theft, misrepresentation, predatory lending, and Ponzi schemes. These fraudulent activities undermine platform integrity and erode user trust. This paper presents a comprehensive systematic literature review of fraud detection strategies in P2P lending platforms, emphasizing the role of advanced analytics and machine learning (ML) models in effectively identifying and preventing fraud. The study addresses key research questions, including the definition of fraud within the P2P lending context, the human dynamics influencing fraudulent behavior, and the ML and AI techniques suited for fraud prevention. Our findings highlight the importance of real-time data analysis, continuous updating of detection models, and the integration of behavioral insights to effectively mitigate fraud risks. By synthesizing current methodologies and technologies, the paper contributes to both theoretical advancements and practical applications in fraud detection. It underscores the need for robust, adaptable frameworks that ensure a secure lending environment, enhance platform sustainability, and strengthen user confidence in P2P lending systems.

Keywords: P2P lending; fraud; machine learning; systematic literature review

1. Introduction

In an era defined by rapid digital innovation, peer-to-peer (P2P) lending platforms have disrupted traditional finance, transformed the landscape of digital lending and e-commerce by enabling direct interactions between lenders and borrowers without the need for traditional intermediaries but through online services (Morse 2015). While P2P platforms offer opportunities for greater access to finance and marketplaces, and supports inclusion for those otherwise excluded from traditional financial systems, they are also subject to greater vulnerabilities, posing unique risks derived from digital nature of the platforms. Fraudulent activities, including misrepresentation, identity theft, and Ponzi schemes, are common concerns (Xu et al. 2022), which efficient and effective prevention, detection and correction is essential for maintaining trust and security in such decentralized systems. This systematic review synthesizes recent literature on P2P fraud detection methods, such those implementing machine learning applications, while as well discuss the challenges faced in this domain. Altogether, we here

 doi:10.20944/preprints202509.1144.v1

explore effective strategies for identifying and preventing fraudulent activities, pivotal for maintaining the integrity and trustworthiness of these financial systems.

Accompanying a rapidly evolving digital finance landscape, we also live an unprecedented expansion in the availability of intelligent algorithmic systems. With the proliferation of Big Data technologies and sophisticated analytical tools, such as machine learning (ML) and artificial intelligence (AI) solutions, P2P platforms have the potential to harness these advancements to detect and mitigate fraud risks effectively (Bello et al. 2024; Hassan et al. 2023). Specifically, combining the power of data and machine learning holds great promise for detecting fraudulent behavior in P2P lending by unraveling anomalous patterns hidden in large-scale trends. Leveraging computer science solutions on the large datasets P2P platforms collect, such as transaction history, user activity, or communication logs, platforms can pinpoint irregularities that deviate from default behaviors (Wu et al. 2022; Jayathilaka et al. 2018). The development and deployment of appropriate machine learning methods for fraud detection holds the potential to automatize and improve fraud risk management, ultimately fostering a safer lending environment, thus protecting both lenders and borrowers and ensuring a sustainable development and long-viability of P2P alternative finance (Xu et al. 2015, 2016).

In recent years, the implementation of advanced machine learning algorithms and predictive models has proven instrumental in elevating fraud detection capabilities, though much remains to be learned as P2P fraud is a rare event and, therefore, AI modeling frequently makes false negative predictions, tragic as these can lead to large losses (Xu et al. 2022). Another dimension in which P2P fraud ML/AI detection systems might be sensitive is on temporal dynamics, as even if these technologies facilitate real-time analysis of and rapid response to suspicious activities, fundamental for rapidly counteract the financial losses associated with detected fraud (Xu et al. 2015), the scalable integration of new data points requires flexible and expensive database systems. Therefore, a long path of improvement and debate is still open towards the continuous refinement of ML/AI solutions, requiring a deep understanding of both technological aspects and the behavioral patterns of fraudsters (Xu et al. 2016).

Practical examples of fraud in P2P lending evidence their diversity and complexity, including identity theft, where individuals falsify information to secure loans illegally, predatory lending practices, where borrowers are misled into agreeing to unfavorable terms, transaction manipulation, loan stacking, or Ponzi schemes. Effective fraud detection strategies, only if able to account for this behavioral diversity, could enable platforms to prevent such scenarios, ensuring fair practices and adherence to regulatory standards (Bello et al. 2024; Jayathilaka et al. 2018), but to do so need ML/AI systems need to be resilient and aware of human dynamics. Therefore, this review study also delves into the human dynamics, and socioeconomic factors and impacts of fraudulent activities in P2P lending.

The importance of leveraging technological solutions to detect and prevent P2P fraud is unquestionable, as an increasing number of platforms are investing in advanced security measures, regulatory compliance, and recognizing the significance of robust fraud detection technology. In addition, fraud detection, especially in connection with anti-money-laundering requirements and know-your-customer-obligations, are increasingly a regulatory condition to be able to operate a P2P lending platform (Wenzlaff et al. 2022; Alibrandi and Grossule 2022; Louisse 2022; Ferretti 2022). This technological adaptation path could lead to the enhancement of operational resilience and support regulatory compliance (Xu et al. 2015, 2016).

However, to start with, the necessity for a clear and precise definition of fraud in P2P lending is critical. The absence of a standardized definition hampers the development of effective detection algorithms and contributes to inconsistencies in research outcomes, leading to challenges in the comparability of studies, as different researchers may adopt varying definitions and thresholds Cumming et al. (2021). A unified definition would facilitate the creation of robust detection frameworks, which on the technology side suffer from the various challenges previously exposed Machado et al. (2024), and would ultimately also solve the evaluation dilemma, where the comparison of detection algorithms does not yet count with a unified benchmark system. If all these challenges are addressed,

 doi:10.20944/preprints202509.1144.v1

detection frameworks could ultimately help improve the interoperability of P2P systems across different platforms, which is essential given the decentralized nature of P2P networks Liu et al. (2024).

In an era characterized by the rapid evolution of financial technologies, peer-to-peer (P2P) lending has emerged as a transformative force in alternative finance, connecting borrowers directly with lenders via online platforms Agarwal and Zhang (2020). By bypassing traditional financial intermediaries, P2P lending enhances financial inclusion and operational efficiency. However, this disruption comes with significant challenges, notably the risk of fraud, which includes activities such as identity theft, misrepresentation, predatory lending, and Ponzi schemes. These fraudulent practices undermine platform integrity, erode consumer trust, and pose significant operational and reputational risks.

Fraud in P2P lending can be broadly defined as deliberate acts of deception aimed at securing financial or reputational gains at the expense of others. Unlike conventional financial systems, where centralized oversight can mitigate risks, P2P platforms rely heavily on decentralized, data-driven processes. This reliance amplifies vulnerabilities, necessitating sophisticated detection and prevention strategies to maintain trust and sustain growth in this dynamic market.

This study presents a systematic literature review that synthesizes the state-of-the-art machine learning (ML) and artificial intelligence (AI) techniques used in P2P fraud detection. Beyond detecting fraud, we emphasize the integration of these technologies into platform operations to proactively prevent fraudulent activities. By providing a consensus definition of P2P fraud and examining the latest technological advancements, this study bridges the gap between theoretical research and practical applications, ultimately addressing critical managerial and consumer service implications.

By gathering evidence that meets predefined eligibility criteria, this study seeks to answer the following research questions:

1. What is the definition of fraud within the context of P2P lending?
2. Which machine learning and AI techniques and schemes are suited for P2P lending fraud detection and prevention?
3. What are the managerial and ethical implications?

Here reported insights are intended to benefit both practitioners and researchers, particularly but not exclusively in the finance field. For industry professionals, having an overview of fraud detection and prevention methods is a must starting point towards advancing platform integrity towards ultimately enhancing user trust towards using P2P lending. For academics, this SLR lays foundational knowledge on the field history and state-of-the-art, serving as groundwork for developing further research and innovative fraud detection techniques.

The paper is structured as follows: Section 2 outlines the methodology employed to conduct the systematic literature review. Section 3 presents the quantitative aspects of the literature concerning fraud detection models. Section 4 the role of AI in fraud detection. Section 5 provides a thematic analysis of the retrieved literature. Finally, Sections 6 and 7 present the managerial implications of the findings and the conclusion of this study.

2. Methodology

In our systematic literature review study, we follow a structured methodology to guarantee thorough and impartial results. Utilizing the framework employed by Varsha et al. (2024); Amato et al. (2024), our methodology consists of eight crucial steps that establish the direction and extent of our review.

- First, we define the study problem by formulating research questions.
- Second, we establish and verify a systematic approach for reviewing to offer direction for our data exploration and examination (i.e., we draw a research map, more details in Figure **??**).
- The third step involves conducting a thorough analysis and exploration of the relevant literature, ensuring a comprehensive examination of the subject area.
- Fourth, we use certain criteria to carefully evaluate the collected studies for inclusion, ensuring their relevance and high quality.

 doi:10.20944/preprints202509.1144.v1

- The fifth step involves a thorough evaluation of the quality of each selected study.
- Sixth, the data extraction procedure begins, when pertinent information is systematically gathered from each study.
- The seventh step, data analysis and synthesis, allows us to combine findings and extract meaningful insights.
- In the eighth and final step, we summarize the results in detailed reports, presenting our findings in a systematic and easily comprehensible manner.

The methodological approach used ensures the precision and dependability of our literature review, thus providing significant information on the topic.

Scopus[1] was selected as the primary database for this systematic literature review due to its comprehensive coverage of peer-reviewed scholarly publications across a wide range of disciplines, including finance, computer science, and management—fields critical to understanding fraud detection in P2P lending platforms. Scopus is renowned for its advanced search capabilities, which allow for precise and customizable queries using logical operators, enabling researchers to filter and retrieve relevant studies efficiently. We did not choose Web of Science (WoS), as it is subscription based and Scopus is freely available. Majority of papers indexed in WoS are also indexed in Scopus so we eliminated duplicates from the start. Additionally, Scopus includes a robust citation tracking system, making it easier to identify influential papers and trends in the field (Kushwaha et al. 2021; Ngai et al. 2009). The advanced search function was employed to generate customized search queries, incorporating keywords such as: 'Fraud', 'Fraudulent Activities', 'Fraud detection', 'P2P Lending', 'P2P', and 'Alternative Financ*'. The keywords, along with the logical operators 'AND' and 'OR', were used to create one search query. These questions were designed to focus on fraud in P2P settings.

- ("Fraud" OR "Fraudulent Activities" OR "Fraud Detection") AND ("P2P Lending" OR "P2P" OR "Alternative Financ*")

This query targeted keywords, abstracts, and titles of articles in the initial retrieval phase. It was applied to Scopus and the resulting papers were filtered based on the exclusion criteria outlined in Table 1. Using a four-phase strategy, we start by collecting 134 publications using the systematic method as outlined in this section and depicted in Figure 1. Furthermore, the total number of publications analyzed in this study is 38.

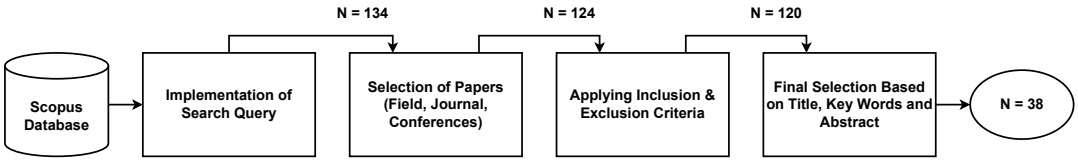

Figure 1. Illustration of the article selection process.

Table 1. Summary of article selection criteria.

Criteria	Decision
Inclusion of pre-defined keywords in title, abstract, or keyword list	Inclusion
Article publication in a scientific journal	Inclusion
Article written in English	Inclusion
Duplicates of an original article	Exclusion
Relevance of abstract, title, and content to research objective	Exclusion

[1] https://www.scopus.com/home.uri

 doi:10.20944/preprints202509.1144.v1

3. Deconstructing the Research Landscape

The current literature landscape presents a diverse range of studies distributed across various fields with a concentration in Business & Finance, Computer Science, and Engineering, indicating the multidisciplinary nature of the topics covered (see Figure 2). This is substantiated by the keyword word cloud, which highlights terms like "Peer Networks," "Finance," "Machine Learning," and "Fraud Detection" as prominent themes. These keywords (see Figure 3) not only underscore the primary focus areas but also reflect ongoing concerns and developments in financial technologies and cybersecurity within digital transaction systems. The substantial representation of topics related to electronic commerce, peer-to-peer lending, and fraud detection suggests a strong emphasis on understanding and innovating within the digital transaction space.

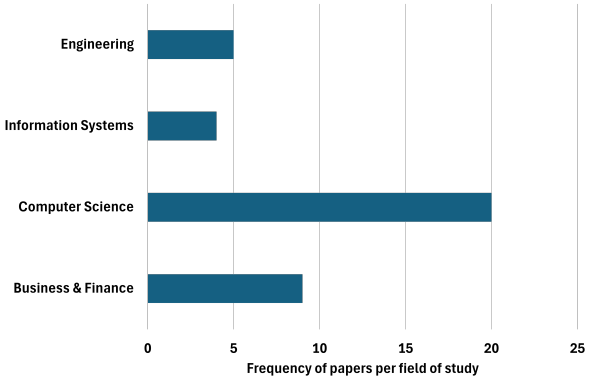

Figure 2. Field of study of published papers.

Figure 3. Word Cloud of Keywords from Published Papers: The size of each word corresponds to its frequency of appearance in papers reviewed.

Furthermore, the analysis of publication types (see Figure 4) and years (see Figure 5) reveals that the majority of the literature comprises journal papers, which make up 58% of the studies, followed by conference papers at 39%. This distribution indicates a balanced mix of theoretical exploration and practical applications that are shared at academic and professional gatherings. The temporal distribution of publications highlights peaks in research output during certain years, with notable increases in recent years, which may correspond to technological advancements and heightened industry interest in blockchain technologies and AI-driven financial solutions. Moreover, the frequency distribution of citations per publication (see Figure 6), particularly the clustering around papers with 10-25 citations, reflects a consistent engagement with these topics within the academic and professional communities, highlighting their ongoing relevance and the community's acknowledgement of the importance of continued research in these areas.

 doi:10.20944/preprints202509.1144.v1

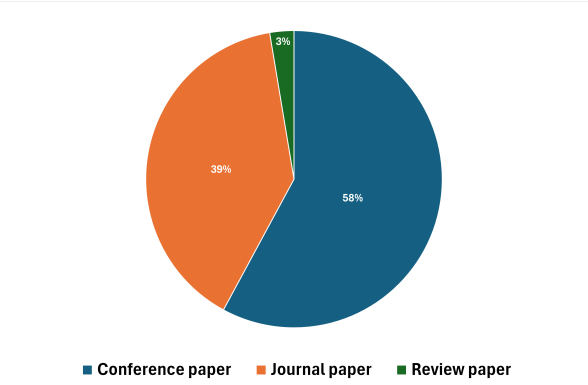

Figure 4. Type of papers published: Journal, Review, and Conference papers are peer-reviewed studies.

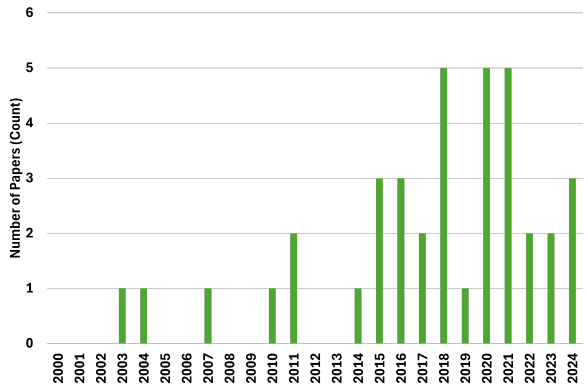

Figure 5. Year distribution of publications.

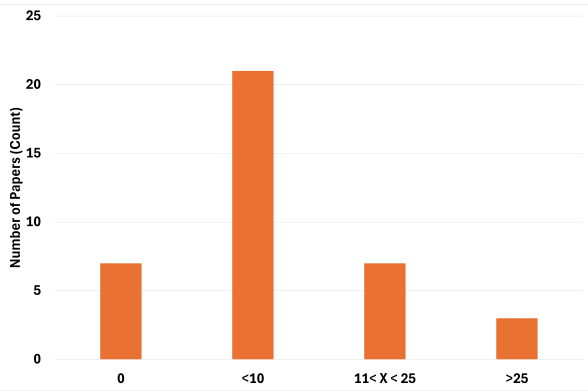

Figure 6. Frequency of citations of publications.

 doi:10.20944/preprints202509.1144.v1

Table 2. Fraud detection research categories, papers, advantages, limitations, and applications.

Category	Paper(s)	Advantages	Limitations	Applications
Data-Driven Analysis	Wang Y.; Li F.; Hu J.; Zhuang D.	Correctly detects fraud users and creates mean index combinations for fraud recognition.	Classification of fraud is limited; sample size limited to one website and one cryptocurrency.	Fraud detection in P2P lending by identifying users with negative ratings.
	Xu J.J.; Lu Y.; Chau M.	Potential use of many different methods and a unique dataset.	Work in progress, potential bias form sample bias - single platform China.	(Potential) Fraud detection in P2P lending using meta-learning and classification algorithms.
	Tsuchiya T.; Cuevas A.; Christin N.	Builds machine learning models to predict account suspension.	limited transferability across markets.	Predicting account suspension on P2P platforms.
	Chen Y.; Wang D.	Designs and analyzes the detailed design process of the prototype system of anti-fraud.	Needs more classifiers for AdaBoost.	Anti-fraud system design in P2P lending.
	Chengeta K.; Mabika E.R.	XGBoost, Deep Learning, and CatBoost performed better in classifying P2P lending defaults; identifies key parameters leading to loan defaults.	Suggest future work in quantum ML, cloud computing.	Classifying P2P lending defaults and identifying key risk factors.
	Wang H.; Wang Z.; Zhang B.; Zhou J.	Provides an overview of a data collection system for anti-fraud in P2P financial markets, addressing challenges like ActiveX controllers and JavaScript encryption.	Does not specify detailed validation methods.	Data collection for anti-fraud systems in P2P lending.
	Folino F.; Folino G.; Pontieri L.	Introduces an incremental learning framework for detecting deviant business process instances; demonstrates scalability with a distributed peer-to-peer architecture.	Performance can be improved.	Detecting deviant business process instances in P2P systems.
	Lu S.; Xu X.; Wang H.; Zhao J.; Wu Z.	Unsupervised learning approach to extract groups that exhibit potentially fraudulent behavior.	No advanced labels; relies on clustering methods.	Identifying potentially fraudulent groups in P2P lending.
	Wang H.	Study shows that standard ML methods yield quite good predictions (AUC > 0.780).	Fraudulent users and users with overdue payments are labeled, but it is not mentioned how; only features from transaction data; only Chinese market.	Fraud detection using standard ML methods.
	Xu J.J.; Chen D.; Chau M.; Li L.; Zheng H.	Empirical evidence of features that predict P2P loan fraud based on meaningful fraud labels.	Needs more borrower behavior features.	Predicting P2P loan fraud using various ML models.
	Yang B.; Garcia-Molina H.	Robust scheme that makes fraudulent behavior unattractive and protects against it.	No data (theoretical instance).	Preventing coin fraud using rule-based detection.
Behavioral Analysis	Liu F.; You Y.	Leverages social network and consumption data.	Few ML models tested.	Fraud detection based on consumption behavior.
	Islam M.M.; Sohag A.; Hasan M.; Islam M.K.; Sultan M.N.	Random Forest outperforms other algorithms; uses XAI tools to find the explainability of the datasets with the top-score model.	Models and explanations derived from this study are specific to the dataset used.	Fraud detection using behavioral data and explainable AI.
	Lai W.	Provides a new method that combines feature extraction with imbalanced data processing, and verifies the effectiveness of this combination.	Model robustness and applicability need further validation.	Fraud detection using imbalanced data processing.
	Fu X.; Zhang S.; Chen J.; Ouyang T.; Wu J.	It is helpful to use changes in investor sentiment to study trading volume; this data may provide important reference information for government and enterprises.	Precision and recall values still have room for improvement.	Using investor sentiment to detect fraud.
Text Analysis	Li L.; Zhao T.; Xie Y.; Feng Y.	Mixes text method and theory from behavioral theory to not only detect but also try to explain why companies are fraudulent.	Only applies when there is a lot of text describing the company.	Fraud detection using text analysis and behavioral theory.
Network Analysis	Li Y.; Bu H.; Wu J.	Novel approach using company ownership structure.	Only Chinese firms, features are country specific.	Fraud detection using ego-network models.
	Musau F.; Wang G.; Abdullahi M.B.	Model can deal with malicious attacks efficiently compared with existing models.	Reliance on simulations; real-world applicability and scalability need further validation.	Fraud detection using trust mechanisms and simulation techniques.
	Wang Q.; Liu Y.	Contributes a new approach to incorporating graph and text data for P2P lending fraud detection; demonstrates improved performance over existing methods.	The complexity of the attention mechanisms may require significant computational resources.	Fraud detection using graph attentive networks.
Trust and Reputation Analysis	Acampora G.; Alghazzawi D.; Hagras H.; Vitiello A.	Proposes a new method (type-2 fuzzy logic) to evaluate reputation; aims at not only buyers but also sellers in the P2P environment.	No cross platform validation, lacks comparison with other methods.	Classifying fraudulent users in P2P environments using fuzzy logic.
	Wang Y.; Yang J.; Qi L.	This model imitates real P2P platforms by allowing sellers to be of different types with type information unavailable to buyers.	Sample size; how steady-state equilibria can be approximately reached in a finite time.	Modeling P2P platforms using game theory.
	Pereira R.H.; Gonçalves M.J.A.; Coelho M.A.G.M.	Comprehensive framework in classification of fraud, methods, and validation techniques.	Theoretical, needs empirical development.	Theoretical discussion on fraud classification.
	Musau F.; Wang G.; Abdullahi M.B.	Reduces malicious behaviors by comparing	Simulation - based, assumes honest peers, scallability and generalisibility concerns	Trust model based on neighbor similarity

 doi:10.20944/preprints202509.1144.v1

Table 3. Categories Table.

Category	Description
Basic Principles Covered	Includes Data-Driven Analysis, Behavioral Analysis, Text Analysis, Network Analysis, Trust and Reputation Analysis, Risk Assessment, Ensemble Methods, Feature Engineering, and Explainable AI (XAI).
Using ML (Yes)	k-means algorithm, logistic regression, Ego-network, Ad boost, random forest, meta-learning algorithm, decision trees, SVM, NN, text logistic regression, CNN LSTM, LIME model, type-2 fuzzy logic, Imbalance-XGBoost, XGBoost, NGBoost, AdaBoost GBDT, Graph Attentive Network model (FDNE), ensemble-based deviance detection model.
Using ML (No)	Analytic Hierarchy Process (AHP), game theory model, CFA and SEM analysis, trust mechanisms and simulation techniques, Cox Hazard Model, qualitative analysis, unsupervised learning and clustering, reputation models, collaborative filtering, auctions, social networking, rule-based detection (invariants).
Data-Driven Analysis	Wang Y.; Li F.; Hu J.; Zhuang D. (using k-means), Xu J.J.; Lu Y.; Chau M. (potential use of meta-learning), Tsuchiya T.; Cuevas A.; Christin N. (building ML models). Applications: Fraud detection in P2P lending, predicting account suspension, anti-fraud system design.
Behavioral Analysis	Liu F.; You Y. (using Random Forest), Islam M.M.; Sohag A.; Hasan M.; Islam M.K.; Sultan M.N. (using 10 ML algorithms), Lai W. (using Imbalance-XGBoost). Applications: Fraud detection based on consumption behavior, using behavioral data and explainable AI, using imbalanced data processing.
Text Analysis	Li L.; Zhao T.; Xie Y.; Feng Y. (using text logistic regression, SVM, CNN LSTM). Applications: Fraud detection using text analysis and behavioral theory.
Network Analysis	Li Y.; Bu H.; Wu J. (using logistic regression, Ego-network), Musau F.; Wang G.; Abdullahi M.B. (using trust mechanisms), Wang Q.; Liu Y. (using Graph Attentive Network model FDNE). Applications: Fraud detection using ego-network models, trust mechanisms, and graph attentive networks.
Trust and Reputation Analysis	Acampora G.; Alghazzawi D.; Hagras H.; Vitiello A. (using type-2 fuzzy logic), Wang Y.; Yang J.; Qi L. (using a game theory model), Li J.; Liu L.; Xu J. (using a Fuzzy-Rep model). Applications: Classifying fraudulent users using fuzzy logic, modeling P2P platforms using game theory, improving P2P e-commerce security.
Risk Assessment	Xie X.L. (using Analytic Hierarchy Process), Shen L.H.; Khan H.U.; Hammami H. (using CFA and SEM analysis), Li J.; Hsu S.; Chen Z.; Chen Y. (using Cox Hazard Model). Applications: Detecting fraud, understanding lenders' perceptions, analyzing the relation among survival, interest rate, and capital.

 doi:10.20944/preprints202509.1144.v1

Table 4. Summary of Authors and Their Model/Method Used.

Authors	Model/Method Used
Wang Y.; Li F.; Hu J.; Zhuang D.	k-means algorithm
Li Y.; Bu H.; Wu J.	logistic regression models, Ego-network, Ad boost, random forest
Xu J.J.; Lu Y.; Chau M.	meta-learning algorithm, decision trees, SVM, NN
Liu F.; You Y.	Random Forest
Li L.; Zhao T.; Xie Y.; Feng Y.	text logistic regression, SVM, CNN LSTM, decision tree, LIME model
Acampora G.; Alghazzawi D.; Hagras H.; Vitiello A.	type-2 fuzzy logic
Islam M.M.; Sohag A.; Hasan M.; Islam M.K.; Sultan M.N.	10 well-known ML algorithms, four XAI tools (Random Forest outperforms)
Tsuchiya T.; Cuevas A.; Christin N.	random forest, gradient boosting
Lai W.	Imbalance-XGBoost, XGBoost, NGBoost, AdaBoost GBDT
Chen Y.; Wang D.	Ad Boost algorithm
Fu X.; Zhang S.; Chen J.; Ouyang T.; Wu J.	CNN
Chengeta K.; Mabika E.R.	supervised learning techniques, deep convolution neural networks (CNN), XGBoost, Deep Learning, CatBoost
Xu J.; Chen D.; Chau M.	Blacklisting, Random Forest (RF), Support Vector Machines (SVM)
Li J.; Liu L.; Xu J.	Fuzzy-Rep model, fuzzy logic
Wang H.; Wang Z.; Zhang B.; Zhou J.	Bayesian Networks, Logistic Regression, other machine learning techniques
Wang Q.; Liu Y.	Graph Attentive Network model called FDNE
Folino F.; Folino G.; Pontieri L.	ensemble-based deviance detection model (AODE and other classification algorithms)
Wang H.	supervised ML methods based on feature engineering, random forest, gradient boosting decision tree
Xu J.J.; Chen D.; Chau M.; Li L.; Zheng H.	random forest (RF), XGBoost (XGB), deep neural network (DNN), Long Short Term Memory (LSTM) neural network
Kim H.-J.; Jung J.J.; Jo G.-S.	cosine similarity, Recommend-Feedback-Re-recommend (RFR) algorithm
Yadav A.S.; Kushwaha D.S	(No specific model listed)
Xie X.L.	Analytic Hierarchy Process (AHP)
Wang Y.; Yang J.; Qi L.	game theory model
Pereira R.H.; Gonçalves M.J.A.; Coelho M.A.G.M.	(Theoretical discussion on ML methods)
Shen L.H.; Khan H.U.; Hammami H.	CFA and SEM analysis
Musau F.; Wang G.; Abdullahi M.B.	trust mechanisms and simulation techniques
Li J.; Hsu S.; Chen Z.; Chen Y.	Cox Hazard Model
Cekerevac Z.; Dvorak Z.; Prigoda L.; Cekerevac P.	(No specific model listed)
Chen D.; Deakin S.; Johnston A.; Wang B.	(Qualitative analysis)
Lu S.; Xu X.; Wang H.; Zhao J.; Wu Z.	Unsupervised learning, Minimum spanning tree extraction
Zhong Q.-Q.; Wei W.-H.	(No specific model listed)
Sundaresan N.	reputation models, collaborative filtering, auctions, social networking
Yang B.; Garcia-Molina H.	rule-based detection (invariants)

4. The Role of AI in P2P Fraud Detection

AI has introduced a paradigm shift in fraud detection by enabling the analysis of vast amounts of data in real-time, identifying patterns and anomalies that may indicate fraudulent activity. Peer-to-peer (P2P) transactions, enabled by digital platforms, have revolutionized financial exchanges by facilitating direct interactions between individuals and entities. This model, which bypasses traditional intermediaries, offers efficiency and cost-effectiveness (Xu et al. 2015; Liu and You 2020). However, it also presents new challenges, particularly in terms of fraud detection (Xu et al. 2022, 2015; Chen and Wang 2020; Pereira et al. 2023; Wang 2019; Li et al. 2020). The anonymity (Teichmann et al. 2024), decentralization (Yadav et al. 2022), and speed inherent in P2P transactions create vulnerabilities that can be exploited by malicious actors (Acampora et al. 2016). As fraud schemes become increasingly sophisticated, there is a growing need for advanced detection mechanisms (Xu et al. 2022). Artificial Intelligence (AI) has emerged as a powerful tool in this domain, offering dynamic (Wang et al. 2017; Folino et al. 2018; Zhong and Wei 2011), scalable (Xu et al. 2015; Liu and You 2020), and accurate solutions to combat P2P fraud (Lai 2023). This chapter explores the role of AI in detecting P2P fraud, examining its methodologies and potential limitations.

P2P fraud encompasses a wide range of deceptive practices aimed at exploiting the vulnerabilities of decentralized transactions (Yadav et al. 2022). Common types of P2P fraud include identity theft

 doi:10.20944/preprints202509.1144.v1

(Pereira et al. 2023; Xu et al. 2016), transaction laundering (Teichmann et al. 2024), fake accounts (Tsuchiya et al. 2024), loan request fraud (Xu et al. 2015) or others (Cumming et al. 2021; Beekun et al. 2008). The lack of centralized oversight and the reliance on digital identities increase the complexity of fraud detection in P2P networks (Wang 2019; Li et al. 2010). Traditional fraud detection systems, which often depend on rule-based approaches, struggle to adapt to the evolving tactics used by fraudsters in P2P contexts (Lai 2023; Chengeta and Mabika 2021).

In P2P fraud detection, supervised learning models are commonly used, where the algorithm is trained on labeled data containing known instances of fraud (Wang 2019). ML algorithms can learn from historical transaction data to identify patterns associated with fraudulent activities. Decision trees, random forests, and support vector machines are frequently employed in P2P fraud detection due to their ability to handle large datasets and uncover complex relationships between variables (Liu and You 2020; Chen and Wang 2020). Deep Learning, a more advanced subset of ML, leverages neural networks with multiple layers to analyze complex data structures (Chengeta and Mabika 2021; Li et al. 2020). Natural Language Processing (NLP) is another AI methodology with significant implications for P2P fraud detection. NLP techniques can analyze textual data, such as transaction descriptions, communication between parties, or customer support interactions, to detect signs of fraud (Li et al. 2020).

AI in P2P fraud detection holds significant promise but faces several challenges, including the need for large, high-quality datasets, which can be difficult to obtain in certain markets or platforms, leading to inconsistencies that affect model performance (Xu et al. 2015; Liu and You 2020). The "black box" nature of AI, particularly in deep learning models, poses issues with transparency, making it difficult to explain decisions to stakeholders or regulatory bodies (Islam et al. 2024).

There are many dimensions in which this topic is analyzed. (Li et al. 2016) examine the risks of P2P lending platforms in China by applying a Cox Hazard Model to model platform failure. It identifies significant factors like platform age, interest rates, and loan types that impact the likelihood of failure. Different perspective is offered by Chen and Wang (2020) as they explore anti-financial fraud technology using machine learning, specifically the AdaBoost algorithm, to enhance credit fraud detection in P2P networks. It emphasizes the importance of data preprocessing and adaptive weight adjustments to improve model accuracy and minimize lending risks associated with fraudulent applicants. Moreover, Bitcoin emerged as an alternative payment method following the decline of the U.S. dollar's reputation, offering benefits like lower transaction costs, privacy, and inflation protection (Cekerevac et al. 2015). Risks associated with Bitcoin are discussed by Fu et al. (2019), including its volatility, regulatory uncertainty, and potential for facilitating illegal activities. The authors analyze these risks in the context of Bitcoin's adoption as a currency and its implications for financial stability and investor protection. Moreover, peer-to-peer (P2P) lending, a digital marketplace connecting borrowers and lenders, has grown during the COVID-19 pandemic but faces significant challenges, including information asymmetry and inadequate credit verification (Chengeta and Mabika 2021). Machine learning algorithms like deep learning convolutional neural networks and frameworks such as XGBoost and LightGBM are employed to predict loan defaults and fraudulent behavior, outperforming traditional classifiers. The study, using datasets from Prosper and Lending Club, identifies key predictors of loan defaults, including purpose, employment status, age, and credit grade (Chengeta and Mabika 2021; Wang et al. 2020; Chen et al. 2021).

Ethical and legal concerns also arise, particularly regarding data privacy and the potential for biased outcomes, necessitating compliance with varying data protection regulations (Pereira et al. 2023; Teichmann et al. 2024; Li et al. 2021). Overcoming these challenges while driving innovation is crucial, with future directions focusing on developing interpretable AI models, leveraging federated learning to enhance privacy while improving performance, and refining anomaly detection techniques to reduce false positives and better identify novel fraud patterns (Li et al. 2020,?; Islam et al. 2024).

 doi:10.20944/preprints202509.1144.v1

5. Predominant Themes in Literature

This subsection summarizes the content-related aspects of the papers collected in this systematic literature review. We categorize the content into settings, methods, and evaluation aspects of the empirical studies reviewed. Additionally, Table A1 presents a summary of all the papers collected, highlighting their main features. Fraud in P2P platforms extends beyond financial losses, having significant implications for consumer trust, platform sustainability, and service delivery Xu et al. (2022); Lo and Kan (2023). Fraudulent activities erode trust in digital platforms, reducing consumer willingness to engage with P2P services so that detecting and mitigating fraud ensures the operational sustainability of the platforms.

5.1. Defining Fraud in P2P Platforms

Fraud definitions in P2P literature vary based on the type of platform and context. Commonly addressed forms of fraud include: a) misrepresentation and identity theft: users providing false information to deceive lenders or sellers, often resulting in financial losses (Xu et al. 2016; Shen et al. 2021); b) reputation manipulation: fraudulent activities where users artificially inflate their reputations through fake reviews or ratings, especially problematic in e-commerce settings (Acampora et al. 2016); c) platform-level fraud: some platforms themselves engage in fraudulent activities, such as Ponzi schemes, where funds from new investors are used to pay returns to earlier investors without real profit generation (Chen et al. 2021); d) payment and loan default fraud: in the context of P2P lending, fraud can also involve defaulting on loans after receiving funds, often exacerbated by limited regulatory frameworks in certain regions (Lai 2023).

Fraud in the digital context of P2P platforms consists of deliberate acts of deception aimed at gaining financial or reputational advantage at the expense of others, facilitated by the unique characteristics and vulnerabilities of online environments (see Figure 7). These forms of fraud exploit the digital nature of peer-to-peer platforms, requiring robust detection and prevention mechanisms.

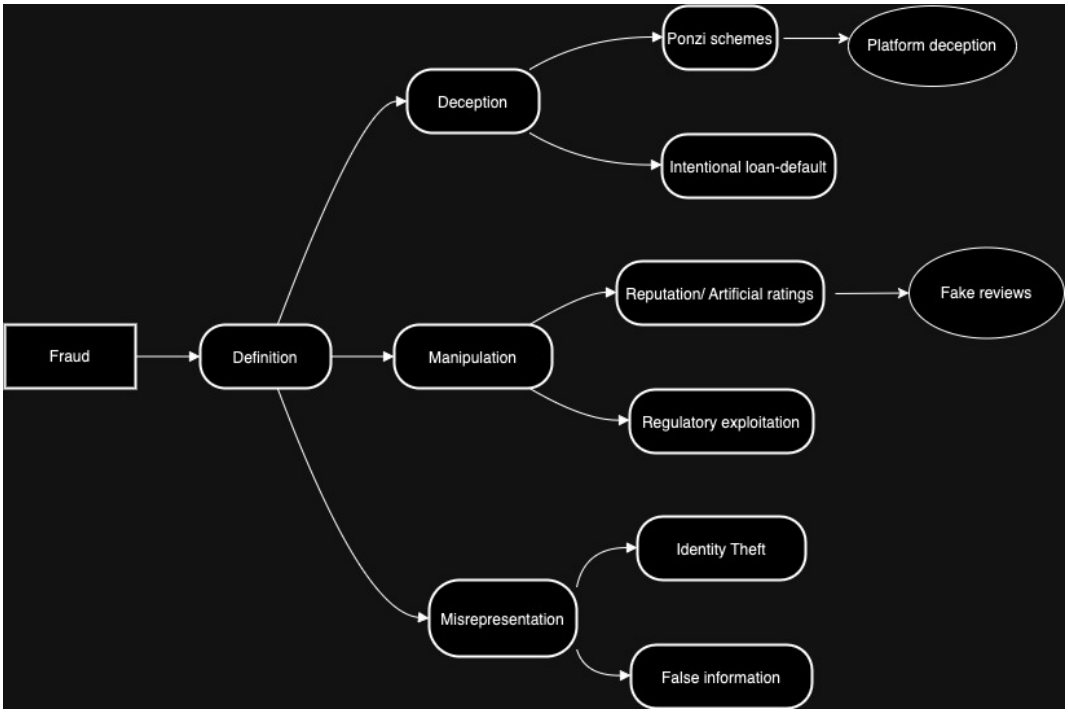

Figure 7. Fraud Definition.

5.2. P2P Lending Platform and Fraud Divtersity

The settings in which fraud detection and management in Peer-to-Peer (P2P) lending and e-commerce platforms have been explored demonstrate a wide range of environments, reflecting the diversity of these platforms and the geographic regions where they operate. Several studies have

 doi:10.20944/preprints202509.1144.v1

concentrated on the Chinese P2P lending market, which has garnered significant attention due to its rapid expansion and the subsequent regulatory challenges it faces (Wang 2019; Li et al. 2016; Chen et al. 2021; Wan 2018). These studies highlight the unique risks associated with the Chinese market, such as the prevalence of fraud and liquidity issues that have plagued the sector. Moreover, the focus on emerging markets is evident in studies that examine P2P platforms within broader international settings (Teichmann et al. 2024; Musau et al. 2011). These studies often address the challenges posed by evolving regulatory frameworks and the need for robust fraud detection mechanisms in markets where financial systems are still developing.

The platforms under study vary from specific P2P lending sites to broader e-commerce platforms that utilize reputation management systems. For instance, research has focused on Chinese P2P lending platforms (Xu et al. 2015; Li et al. 2020,?) as well as on platforms that manage trust and reputation in decentralized e-commerce environments (Acampora et al. 2016; Wang et al. 2017). The diversity of these platforms underscores the varying levels of risk and the different approaches required for fraud detection and prevention. Additionally, some studies have explored cryptocurrency P2P marketplaces (Tsuchiya et al. 2024), which present unique challenges due to their decentralized nature and the increased risk of scams and fraud that comes with disintermediation.

From a technological perspective, the environments studied range from platforms leveraging big data analytics to those implementing machine learning algorithms and blockchain technologies. Big data approaches are particularly highlighted in studies that focus on the management and analysis of large datasets, which is crucial for real-time fraud detection in large-scale P2P lending platforms (Xu et al. 2015; Liu and You 2020). Blockchain technology, on the other hand, is explored as a means to enhance transaction transparency and security, particularly in the context of digitizing land records and mitigating document forgery in property transactions (Yadav et al. 2022). These technological settings illustrate the critical role that advanced data processing and secure transaction systems play in maintaining the integrity of P2P lending and e-commerce platforms.

5.3. Big Data and ML/AI Solutions for P2P Fraud Detection

Datasets play a central role in fraud detection, but data availability and labeling are major challenges. Many studies use data from P2P platforms such as Lending Club and EasyLoans, which provide transaction histories, user profiles, and rating data. These datasets often include labeled fraud cases, typically based on user behavior such as defaults or negative ratings (Wang 2019). Data from social media or business registration databases, such as Qichacha in China, are also used to supplement platform data, especially in cases where internal data is unavailable (Li et al. 2020,?). In the absence of real-world data, researchers sometimes use simulated datasets to model fraud detection, though these are limited in terms of real-world applicability (Pereira et al. 2023; Musau et al. 2014).

Various methods are employed to detect fraud in P2P lending and e-commerce platforms, utilizing approaches that range from traditional rule-based systems to complex machine learning (ML) models. Traditional fraud detection relies on predefined rules, such as flagging users with a high number of negative ratings or identifying unusual transaction patterns; however, these methods often lack flexibility and can lead to false positives (Wang 2019; Wang et al. 2017; Wang and Liu 2015). Another approach is the use of reputation systems, which assess trustworthiness based on user feedback and transaction history, making them particularly useful in e-commerce settings. Techniques like collaborative filtering and reputation-based clustering are employed in these systems to help detect anomalies in user behavior (Acampora et al. 2016; Sundaresan 2007). Additionally, some studies have focused on creating specific features that capture fraudulent behavior, such as indicators of social connections, transaction sequences, and spending patterns, which enhance model performance by targeting key behavioral attributes linked to fraud (Xu et al. 2016; Li et al. 2010, 2020).

Machine learning models have become increasingly popular for fraud detection in P2P platforms, offering greater predictive accuracy and adaptability than traditional methods.The techniques employed in fraud detection across P2P lending and e-commerce platforms are as varied as the settings in

 doi:10.20944/preprints202509.1144.v1

which they are applied, with a strong emphasis on machine learning, big data analytics, and other computational methods.

Machine learning and artificial intelligence (AI) techniques have emerged as the dominant tools for detecting fraudulent activities. Supervised Learning Models like logistic regression, random forests, and support vector machines (SVMs) are widely used to classify users as fraudulent or non-fraudulent based on labeled datasets (Xu et al. 2015; Li et al. 2020).

Ensemble methods, including XGBoost and deep learning models like convolutional neural networks (CNNs), are often applied to high-dimensional datasets for better fraud detection. Deep learning models, in particular, are effective in capturing complex fraud patterns, though they require large datasets and significant computational resources (Chengeta and Mabika 2021; Islam et al. 2024).

Many studies employ algorithms such as Random Forest, XGBoost, and Neural Networks, which have proven effective in identifying patterns of fraud in large datasets (Wang et al. 2020; Chen et al. 2021). The integration of Explainable AI (XAI) tools further enhances these models by providing transparency in decision-making processes, which is critical for gaining user trust and regulatory approval (Islam et al. 2024).

Graph attentive networks (GATs) and ego-network models represent user relationships as nodes and edges, allowing detection of fraud through network analysis and clustering of suspicious behaviors (Wang et al. 2020; Musau et al. 2014).

Big data analytics is another significant technique utilized across several studies. This approach is essential for handling the vast amounts of data generated by P2P lending platforms, allowing for the real-time processing and analysis necessary for effective fraud detection (Xu et al. 2015; Liu and You 2020). The ability to process and analyze large datasets quickly and accurately is particularly important in the context of P2P lending, where transaction volumes can be immense and the potential for fraudulent activity is high.

Blockchain and consensus algorithms have also been explored as innovative techniques to improve the security and transparency of P2P transactions. For example, Yadav et al. (2022) propose a blockchain-based framework for digitizing property transactions, which significantly reduces the risk of document forgery and other fraudulent activities. This approach leverages the decentralized nature of blockchain technology to create a secure, distributed ledger system that is less vulnerable to tampering and fraud.

Reputation and trust management systems are critical in maintaining the integrity of P2P networks, especially in the absence of traditional intermediaries. Techniques such as fuzzy logic and game-theoretic models are used to assess and manage trust among users on these platforms (Acampora et al. 2016; Wang et al. 2017). These systems are designed to evaluate the trustworthiness of participants based on their past behaviors and interactions, helping to prevent fraud by identifying potentially malicious actors before they can cause harm.

5.4. Evaluation Methods Analysis

The evaluation methods employed in the studies reviewed are diverse, reflecting the complexity of fraud detection in P2P lending and e-commerce platforms. Empirical validation is a common approach, with many studies using real-world data from P2P platforms to test and refine their models. For example, Li et al. (2016) utilize datasets from the Lending Club, a well-known P2P lending platform, to validate their machine learning models. This empirical approach ensures that the models are not only theoretically sound but also practically applicable in real-world scenarios.

Simulation studies are another frequently used method, particularly when empirical data is either unavailable or insufficient. Simulations allow researchers to create controlled environments in which they can test the performance of their models under various conditions before applying them to actual data (Chengeta and Mabika 2021). This approach is valuable for understanding how different variables and factors influence the effectiveness of fraud detection techniques.

Some studies also incorporate cross-platform comparisons to evaluate the generalizability of their models. For instance, Tsuchiya et al. (2024) compare data from multiple cryptocurrency marketplaces

 doi:10.20944/preprints202509.1144.v1

to assess the performance of their fraud detection models across different platforms. This method highlights the importance of developing models that are adaptable and can perform well in diverse environments, which is crucial for the global applicability of fraud detection tools.

6. Managerial Implications

The findings from these studies offer significant insights for managers overseeing P2P lending platforms and other decentralized marketplaces. One of the primary managerial implications is the necessity for advanced risk management tools. The reviewed literature strongly suggests that implementing machine learning models capable of detecting fraud patterns early can mitigate financial losses and enhance platform integrity (Liu and You 2020; Wang 2019). For managers, investing in these technologies is not just an option but a critical requirement for maintaining a competitive edge and ensuring long-term platform sustainability.

Regulatory compliance is another crucial area where managerial attention is needed. The studies reviewed emphasize the importance of aligning platform operations with evolving legal frameworks, particularly in regions with less developed regulatory environments (Chen et al. 2021; Li et al. 2021). Managers must stay informed about regulatory changes and proactively adjust their practices to comply with new laws and guidelines. This is particularly important in markets like China, where regulatory responses to the rapid growth of P2P lending have been both swift and significant.

Enhancing trust and reputation systems is also vital for maintaining user confidence in P2P platforms. The literature highlights the effectiveness of employing fuzzy logic and game-theoretic models to manage trust in decentralized environments (Acampora et al. 2016; Wang et al. 2017). For managers, this means prioritizing the development and implementation of sophisticated reputation management systems that can accurately assess and predict user behavior, thereby preventing fraudulent activities and maintaining a secure trading environment.

Finally, the adoption of emerging technologies such as blockchain is recommended for improving transaction transparency and reducing the risk of fraud. As illustrated by Yadav et al. (2022), blockchain can play a transformative role in markets where traditional systems of record-keeping and transaction verification are prone to fraud. Managers in high-risk markets, particularly in sectors like real estate or large-scale P2P lending, should consider integrating blockchain technology into their operations to safeguard against fraud and enhance the overall security of their platforms.

In conclusion, the systematic literature review underscores the importance of advanced technological solutions, regulatory compliance, and robust trust management systems in managing the risks associated with P2P lending and decentralized e-commerce platforms. For managers, these findings provide a clear road map for developing strategies that not only mitigate fraud risks but also promote the sustainable growth and long-term success of their platforms.

Automation of fraud detection processes supports the operational efficiency through decreasing the manual workload, in the same time improving the platform's scalability and potential for handling increased volumes of data and transactions. This operational efficiency reflects further on the strategic planing and decision making processes based on big data and game theory models. Managerial behavioral insights and decisions are in line with the developed reputation feedback systems, enabling enhanced user engagement strategies and platform sustainability.

7. Conclusion

This study has conducted a comprehensive review of the current state of fraud detection in Peer-to-Peer (P2P) lending and decentralized e-commerce platforms, focusing on the intersection of advanced technologies, regulatory challenges, and managerial implications. The findings demonstrate the critical role of machine learning, big data analytics, blockchain, and reputation management systems in identifying and preventing fraudulent activities within these platforms. As P2P lending continues to grow and evolve, the adoption of these technologies is not only essential for mitigating risks but also for ensuring the sustainability and trustworthiness of these financial systems.

 doi:10.20944/preprints202509.1144.v1

The literature review highlights that while significant progress has been made in developing sophisticated fraud detection models, the effectiveness of these models relies heavily on continuous refinement and the integration of new data points. This dynamic process requires a deep understanding of both technological advancements and the behavioral patterns of fraudsters. The reviewed studies also emphasize the importance of regulatory compliance and the need for platforms to adapt to evolving legal frameworks, particularly in regions where financial systems are still developing. Moreover, the integration of blockchain technology offers a promising avenue for enhancing transaction transparency and reducing the risk of fraud in high-risk markets.

Fraud detection in P2P lending and e-commerce remains a dynamic and challenging field. While machine learning has introduced powerful tools for detecting and predicting fraud, issues of generalizability, scalability, and ethical compliance continue to shape research and practice. Future work should focus on developing adaptable models that can operate across diverse contexts and platforms, integrating explainability as a standard feature, and addressing regulatory and ethical considerations to safeguard user trust and platform integrity.

One of the main ethical challenges requiring the implementation of explainable solutions is the tendency of ML models to incur false negatives (FN) in the context of fraud detection (Raghavan and El Gayar 2019; Al-dahasi et al. 2024). To address the ethical challenge of false negatives in ML-based fraud detection, several solutions can be implemented. Explainable AI (XAI) techniques, such as SHAP values, LIME, and decision tree visualizations, allow for greater transparency, enabling stakeholders to understand model decisions and adjust for more accurate fraud detection. (Cirqueira et al. 2021; Gade et al. 2019) Hybrid models, which combine rule-based systems with ML algorithms, offer a balanced approach that leverages both precision and human intuition to reduce false negatives Malik et al. (2022). Anomaly detection algorithms, like autoencoders and isolation forests, capture unusual behaviors that traditional models might overlook, thus enhancing fraud detection accuracy (Pourhabibi et al. 2020). Regular model retraining and real-time monitoring further ensure models adapt to evolving fraud patterns, while threshold optimization helps balance the trade-off between precision and recall to minimize both false positives and false negatives. Ensemble methods, such as bagging, boosting, and stacking, aggregate multiple model outputs to capture complex patterns that individual models might miss Esenogho et al. (2022). Additionally, human-in-the-loop systems provide an extra layer of scrutiny for high-stakes cases, allowing human analysts to review ambiguous cases and ensure more reliable fraud detection (Chai et al. 2020). Collectively, these solutions work to improve explainability, flexibility, and accuracy, reducing the ethical risks associated with false negatives in fraud detection.

7.1. Limitations and Future Recommendations

While this study provides valuable insights into the current landscape of fraud detection in P2P lending, several limitations must be acknowledged. First, the review primarily focuses on studies published in journals and conference proceedings, which may limit the inclusion of emerging research from less traditional sources such as industry reports or unpublished studies. Additionally, the reliance on data from specific regions, particularly China, may limit the generalizability of the findings to other markets with different regulatory environments and user behaviors.

Another limitation is the inherent challenge of evaluating the effectiveness of fraud detection models in real-world settings. Many of the studies reviewed rely on simulation or historical data, which may not fully capture the complexities of live, real-time fraud detection in a rapidly evolving technological landscape. Furthermore, the "black box" nature of many AI and machine learning models poses a challenge in terms of transparency and explainability, particularly in highly regulated industries where understanding the decision-making process is crucial.

Future research should address these limitations by expanding the scope of the review to include a broader range of sources and geographic regions. Models trained on data from specific platforms or regions may not perform well across different contexts due to variations in user behavior and regulatory environments.

 doi:10.20944/preprints202509.1144.v1

A useful analogy to understand the potential of a unified fraud definition in P2P lending is the Linux Foundation's Hyperledger Fabric project. Hyperledger Fabric is an open-source blockchain framework that provides modular and adaptable infrastructure, enabling different businesses to collaborate and share data securely. Despite diverse use cases, Hyperledger Fabric ensures all participants adhere to the same fundamental standards, allowing companies from various sectors to build applications with shared protocols and data interoperability. Moreover, much like the Hyperledger Fabric community benefits from collective governance and shared technical resources, a standardized fraud framework would foster a more collaborative ecosystem among P2P platforms, academic researchers, and regulators. It would encourage the development of open-access fraud datasets and enable platforms to benchmark their fraud detection systems against industry-wide standards. This collaboration would drive innovation, ensure faster responses to emerging fraud patterns, and ultimately enhance the security and credibility of the entire P2P lending industry.

There is also a need for more empirical studies that evaluate fraud detection models in real-world settings, providing insights into their practical applicability and effectiveness. Additionally, future research should focus on developing more transparent and interpretable AI models that can be easily understood by both regulatory bodies and platform users.

Supervised models depend on accurate labeling, which can be challenging to obtain, particularly when distinguishing between legitimate users and those who engage in fraud without obvious indicators. Unfortunately, for the platforms, publishing labeled data on individual users could result in a breach of data protection requirements, therefore platforms are only required to publish aggregated loan performance data (Louisse 2022).

Finally, as blockchain technology continues to evolve, further research is needed to explore its potential in enhancing fraud detection and prevention in decentralized financial systems. This includes investigating the integration of blockchain with existing fraud detection models and exploring its application in new and emerging markets. By addressing these areas, future research can contribute to the development of more robust, effective, and transparent fraud detection systems that support the continued growth and sustainability of P2P lending and decentralized e-commerce platforms.

Fraud prevention strategies that incorporate behavioral dynamics can also be leveraged to personalize consumer services, but this aspects were not tackled in the current paper.

These findings provide actionable insights for platform managers, policymakers, and researchers, promoting secure and sustainable P2P lending environments.

Acknowledgments: This work has been made possible with the support of several key institutions, funding sources and collaboration networks: COST Actions CA19130, (FinClusion_ FEBA_2023) Leveraging alternative data sources for building a sustainable and unbiased credit scoring tool National Scientific Program "Petar Beron i NIE", BG-175467353-2023-14-0004 - 2023, (WiseCredit) Integrating Personality Traits and Open Banking Data for Sustainable and Ethical Creditworthiness Assessments, 09I03-03-V04-00502- 2023, (DIGITAL) project (No. 101119635) (Marie Skłodowska-Curie Actions).

 doi:10.20944/preprints202509.1144.v1

Appendix A

Table A1. Table reporting all the articles that have been examined to conduct the research and highlighting their main features

Study Authors	Fraud definition?	Datasets sources	Label fraud? If so, how?	Fraud detection methods	ML methods used in the study	Validation methods used	Main contributions	Main limitations
(Wan 2018)	Defined as users with negative ratings.	Bitcoin Exchange (https://www.bitcoin-otc.com), 35,592 obs., 5,881 users.	Based on negative ratings.	Rating-based method.	k-means.	N/A	Combines different detection algorithms; accurate in identifying fraud.	Sample size limited to one website; may not generalize well.
(Li et al. 2020)	Fraud risk linked to failed companies.	Qichacha business database, WDZJ.com (2,107 platforms).	Based on company failure.	Logistic regression, Ego-networks.	Adaboost, Random Forest.	10-fold cross-validation.	Regulatory tool for fraud detection in P2P lending firms.	Limited to Chinese data; difficult to apply globally.
(Xu et al. 2015)	Dictionary definition of fraud.	PPDai.com dataset.	Not yet labeled.	Meta-learning, decision trees, SVM, NN.	N/A	N/A	Proposes diverse methods; unique dataset.	Work-in-progress; more features needed for improvement.
(Liu and You 2020)	Differentiated by consumption behavior.	Consumption, social, and status datasets (346,920 obs.).	Based on consumption ratings (0-3).	Based on consumption types.	Random Forest.	Cross-validation.	Predicts fraud using social network and consumption data.	High-dimensional sample issues; more ML methods needed.
(Li et al. 2020)	Psychological fraud intentions more likely for companies with low-quality executive profiles	4,554 P2P companies from the Home of Network Loan (https://www.wdzj.com).	Yes, based on the size of the extracted text.	Text models (NLP).	Logistic regression, SVM, CNN, LSTM.	Decision tree and LIME model.	Combines ML and behavioural theory to both detect and explain why companies are fraudulent.	Lacks depth on the validation methods. Only applicable when text describing the company is abundant.
(Acampora et al. 2016)	Reputation of buyers/sellers.	eBay-like datasets.	Based on eBay labels.	Type-2 fuzzy logic.	N/A	Comparison statistical procedures (e.g., Friedman test).	Proposes new method to evaluate reputation and detect fraud.	Needs testing on non-Ebay platforms; compare with other methods.
(Xie 2017)	Not explicitly defined.	N/A (theoretical model).	Based on features defined in the model.	Analytic Hierarchy Process (AHP).	N/A	N/A	Proposes features to consider for future fraud detection.	Theoretical; needs testing with real data.
(Wang et al. 2017)	Not directly defined; feedback system between sellers and buyers.	N/A (theoretical model).	Proportion of cheating sellers.	Reputation feedback systems.	Game theory model (non-atomic game setup).	Proof of lemma.	Models real P2P platforms with diverse seller types.	Needs realistic modeling of trader entries/exits.
(Pereira et al. 2023)	Deceptive practices undermining reputation systems.	Simulated data.	Based on various fraud types (e.g., Sybil attacks).	Systematic review.	Theoretical discussion on ML methods.	N/A	Classifies fraud, methods, and validation techniques.	Framework needs development.
(Shen et al. 2021)	Misrepresentation, Ponzi schemes, identity theft, platform misconduct.	Questionnaire survey.	Based on perceptions of trust and risk.	CFA, SEM analysis.	N/A	Identifies factors influencing P2P lending intentions.	Sample bias, limited scope, self-reporting data.	
(Musau et al. 2011)	Various deceptive practices in P2P e-commerce.	Simulated data.	Based on risk management techniques.	Trust model based on neighbor similarity.	N/A	Simulation experiments.	Reduces malicious behavior via neighbor similarity.	Simulated validation; scalability and generalizability concerns.
(Islam et al. 2024)	Behavioral fraud in P2P lending.	Online data on customer behavior.	Based on enterprise credit, residential status.	10 ML algorithms with XAI tools.	Random Forest, SHAP, LIME.	Cross-validation (accuracy, precision, recall, F1).	Random Forest outperforms; highlights explainability.	Generalizability, transparency, explainability tool limitations.
(Tsuchiya et al. 2024)	Vendor deceptive practices.	Paxful, LocalCoinSwap platforms.	Based on scams, payment reversals, etc.	Various ML methods.	Random Forest, Gradient Boosting.	Cross-validation, confusion matrix, ROC, AUC.	High accuracy in predicting account suspension.	Limited transferability across markets.
(Lai 2023)	Deliberate actions deceiving lenders.	Lending Club platform dataset.	Based on false information, identity theft, payment evasion.	Imbalance-XGBoost, real-time monitoring.	XGBoost, NGBoost, AdaBoost, GBDT.	Cross-validation, confusion matrix, ROC, AUC.	Combines feature extraction with imbalanced data processing.	Robustness and applicability of models.

 doi:10.20944/preprints202509.1144.v1

(Li et al. 2016)	Based on survival, interest rate, capital.	WDZJ.com platform data.	Not labeled as fraud.	Cox Hazard Model.	N/A	Log Likelihood.	Links capital increase with reduced fraud risk.	Limited access to national credit system data.
(Cekerevac et al. 2015)	Risks and benefits of Bitcoin use.	blockchain.info, Measuring-Worth.com.	Not labeled as fraud.	Not in scope.	N/A	N/A	Discusses Bitcoin's risks and benefits.	Uncertainty about Bitcoin.
(Chen and Wang 2020)	Perceived from a mathematical perspective.	Multiple data sources (discrete/continuous data).	Based on individual characteristics.	AdaBoost algorithm.	N/A	System performance.	Designs a prototype anti-fraud system.	More classifiers needed for AdaBoost algorithm.
(Fu et al. 2019)	Misrepresentation or blind expansion by operators.	Sina Weibo, Baidu Post Bar, P2P info websites.	Based on positive/negative sentiment.	Text engineering.	CNN.	Precision, Recall, F1.	Uses investor sentiment for market prediction.	Precision and recall need improvement.
(Chengeta and Mabika 2021)	Based on loan status (defaulting/non-defaulting).	Prosper and Lending Club datasets.	Based on loan status.	Supervised learning (loan specifics).	XGBoost, Deep Learning, CatBoost.	TPR, ROC, FPR, MAE, F-measure, MCC, Recall, PRC.	Identifies key parameters for loan defaults.	Recommends quantum ML and cloud computing for future studies.
(Musau et al. 2014)	Dishonest negotiation, exploiting advantages.	Peer group data.	Based on risk management technique.	Trust mechanisms, neighborhood graph.	Various graph models.	Eigen Group Trust model comparison.	Efficiently handles malicious attacks.	Needs more research on social communities and game theory.
(Xu et al. 2016)	Misleading ratings, loan description, wrong info.	MyLending platform.	Based on learning, past performance, social networking, manipulation.	Blacklisting.	Random Forest, SVM.	Precision, F-measure.	Outperforms baseline features in detecting fraud.	Needs more features for borrower behavior and credibility.
(Li et al. 2010)	Vicious trust recommendation within P2P e-commerce	Simulated data, no external sources	No explicit labeling of data as "fraud" or "non-fraud"; trust is evaluated through the Fuzzy-Rep model.	Fuzzy-Rep model using direct trust, indirect reputation, fuzzy logic, and penalty mechanisms.	Fuzzy logic is the primary method used.	Validation through simulation experiments	Introduces a fuzzy logic-based reputation model to improve P2P e-commerce security.	Reliance on simulations; real-world applicability and scalability need further validation.
(Wang 2019)	Not directly mentioned, allusion to high fraud rate in Chinese P2P markets.	Data from various Chinese websites (e.g., People's Bank of China, China Mobile) via web crawling.	No explicit fraud labels; data is used as input for anti-fraud processes.	Anti-fraud methods include feature engineering on collected data and applying machine learning-based prediction methods.	Bayesian Networks, Logistic Regression, etc.	Robustness and efficiency metrics for the data collection system.	Data collection system for anti-fraud in P2P financial markets, addressing challenges such as encryption.	Security measures on websites, complexity of maintaining up-to-date crawlers, technical limitations of current tools.
(Li et al. 2021)	"Runaway" platforms: shutting down, losing contact, or being involved in economic crimes.	Scraped data on Chinese P2P-lending platforms (2007-2016): company information, news, announcements, etc.	Platforms are labeled as "runaways" based on conditions such as stopping business, website shutdown, fraud, etc.	Regression analysis on the relationship between business friendliness, law enforcement, and P2P platform runaways.	Statistical regression models.	Statistical relation between predictive variables and incidence of P2P runaways.	Established link between business-friendly policies, weak law enforcement and higher rates of P2P platform failures.	Potential measurement biases in the business friendliness index and the generalizability of the results to other contexts.
(Teichmann et al. 2024)	Fake loans or identity theft.	Data scraped from various P2P platforms, primarily focused on Chinese markets.	Fraudulent loans are labeled based on government reports and news announcements.	Logistic regression and support vector machines (SVM).	Logistic regression, SVM.	ROC curves, confusion matrices for validation.	Combines financial and textual data to predict fraudulent behavior in platforms.	Focus on the Chinese market limits global applicability.
(Wang and Liu 2015)	Fraudulent transactions or failures of P2P platforms.	Data collected through web scraping and official records from several platforms.	Platforms are labeled based on transaction anomalies and failures.	Decision trees, support vector machines (SVM), and random forests.	Decision trees, SVM, random forests.	Cross-validation, precision, recall, F1-scores.	Proposes new decision tree approaches for fraud detection.	Lack of scalability and complexity in global markets.

 doi:10.20944/preprints202509.1144.v1

(Wang et al. 2020)	Identity theft and false reporting.	Data from various Chinese platforms using scraped information on user activities.	Labels based on false user identities and reports.	Supervised learning approaches with a focus on detecting behavioral anomalies.	Random Forest, XGBoost.	Precision, recall, F1-scores, ROC curves.	Identifies key behavioral patterns leading to fraudulent activities.	Relies on Chinese datasets; needs validation in broader markets.
(Chen et al. 2021)	False reporting and loan defaults.	Data scraped from Chinese P2P platforms, focusing on loan requests and repayment histories.	Labeled based on loan defaults and repayment fraud.	Supervised learning models for fraud detection in loan data.	XGBoost, Random Forest.	Cross-validation, ROC curves, AUC scores.	High accuracy in predicting fraudulent behavior in loan requests.	Limited to the Chinese market; may not be applicable elsewhere.
(Folino et al. 2018)	False reporting and loan defaults.	Data from LendingClub and Prosper, focused on default patterns.	Labels based on loan defaults.	Supervised ML approaches, decision trees, ensemble methods.	Decision trees, Random Forest.	Precision, recall, F1-scores, AUC curves.	Highlights the role of ensemble methods in improving fraud detection accuracy.	Needs further exploration in non-lending platforms.
(Lu et al. 2018)	Not directly defined; Ponzi scheme mentioned.	WDZJ.com platform data (March 2016-February 2017).	No advanced labels; clustering method.	Unsupervised learning.	Minimum spanning tree extraction.	Distance metric.	Clusters applicants for potential fraudulent behavior.	No explicit fraud labels; systemic metrics not used.
(Zhong and Wei 2011)	Misrepresentation of creditworthiness.	N/A (theoretical work).	Misrepresentation of creditworthiness.	N/A	N/A	Authenticity, robustness, efficiency.	Efficient communication protocol; prevents fraud.	Theoretical work, needs real-world application.
(Wang 2019)	Identity theft and overdue payments.	HC Financial Group, 60K overdue payments, 50K fraud users.	Fraudulent/overdue users labeled, unclear how.	Supervised ML methods.	Random Forest, Gradient Boosting.	AUC.	Good predictions (AUC > 0.780).	Feature engineering needed; no deep learning.
(Xu et al. 2022)	Deliberate creation of fraudulent loan requests.	EasyLoans dataset (June 2007-December 2014).	Blacklisted in EasyLoans database.	Based on borrower features.	Random Forest, XGBoost, DNN, LSTM.	F1 Measure, AUC.	Identifies key features predicting P2P loan fraud.	Limited to Chinese market data.
(Sundaresan 2007)	Proxied through trust/reputation.	N/A	Trust and reputation as proxies.	Reputation models, collaborative filtering.	Collaborative filtering.	Circles of trust, degrees of freedom.	Overview of trust/reputation as fraud proxies.	Introductory tutorial; lacks real content.
(Kim et al. 2004)	Fraudulent ratings.	MovieLens dataset.	Fraudulent ratings based on collaborative filtering.	RFR algorithm (recommendation-based).	Cosine similarity clustering.	F1 Measure, MAE.	Enhances robustness with collaborative filtering.	Poor performance at higher fraud rates.
(Yang and Garcia-Molina 2003)	Coin fraud: replication, denial of assignment, double spending.	N/A (theoretical instance).	Coin fraud defined as per description.	Rule-based detection (invariants).	N/A	Credit loss.	Robust scheme against fraudulent behavior.	Theoretical work; needs real-world application.

 doi:10.20944/preprints202509.1144.v1

References

Morse, A. Peer-to-peer crowdfunding: Information and the potential for disruption in consumer lending. *Annual Review of Financial Economics* **2015**, *7*, 463–482.

Xu, J.J.; Chen, D.; Chau, M.; Li, L.; Zheng, H. Peer-to-Peer Loan Fraud Detection: Constructing Features from Transaction Data. *MIS Quarterly: Management Information Systems* **2022**, *46*, 1777 – 1792. Cited by: 6, https://doi.org/10.25300/MISQ/2022/16103.

Bello, H.O.; Idemudia, C.; Iyelolu, T.V. Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. *World Journal of Advanced Research and Reviews* **2024**, *23*, 056–068.

Hassan, M.; Aziz, L.A.R.; Andriansyah, Y. The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics* **2023**, *6*, 110–132.

Wu, Y.; Xie, Z.; Ji, S.; Liu, Z.; Zhang, X.; Lin, C.; Deng, S.; Zhou, J.; Wang, T.; Beyah, R. Fraud-agents detection in online microfinance: a large-scale empirical study. *IEEE Transactions on Dependable and Secure Computing* **2022**, *20*, 1169–1185.

Jayathilaka, H.; Krintz, C.; Wolski, R. Detecting performance anomalies in cloud platform applications. *IEEE Transactions on Cloud Computing* **2018**, *8*, 764–777.

Xu, J.J.; Lu, Y.; Chau, M. P2P lending fraud detection: A big data approach. In Proceedings of the Intelligence and Security Informatics: Pacific Asia Workshop, PAISI 2015, Ho Chi Minh City, Vietnam, May 19, 2015. Proceedings. Springer, 2015, pp. 71–81.

Xu, J.; Chen, D.; Chau, M. Identifying features for detecting fraudulent loan requests on P2P platforms. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI). IEEE, 2016, pp. 79–84.

Wenzlaff, K.; Odorović, A.; Riethmüller, T.; Wambold, P. On the merits of the Key Investment Information Sheet in the ECSPR. In *Regulation on European Crowdfunding Service Providers for Business*; Elgar commentaries in financial law series, Edward Elgar Publishing: Northampton, 2022; p. 310.

Alibrandi, A.S.; Grossule, E. Crowdfunding and consumer credit protection in the EU. In *Regulation on European Crowdfunding Service Providers for Business*; Edward Elgar Publishing, 2022; pp. 591–606. Section: Regulation on European Crowdfunding Service Providers for Business.

Louisse, M. Due diligence of project owners (Art 5). In *Regulation on European Crowdfunding Service Providers for Business*; Edward Elgar Publishing, 2022; pp. 105–112. Section: Regulation on European Crowdfunding Service Providers for Business.

Ferretti, R. Individual portfolio management of loans (Art 6). In *Regulation on European Crowdfunding Service Providers for Business*; Edward Elgar Publishing, 2022; pp. 113–129. Section: Regulation on European Crowdfunding Service Providers for Business.

Cumming, D.; Hornuf, L.; Karami, M.; Schweizer, D. Disentangling crowdfunding from fraudfunding. *Journal of Business Ethics* **2021**, pp. 1–26.

Machado, M.; Coita, I.F.; Bolesta, K.; Filipovska, O.; van Heeswijk, W.; Muñiz, J.A.; Bernard, F.S.; Osterrieder, J. What do we Know About Fraud Detection in Peer-to-Peer Lending? A Systematic Literature Review. *A Systematic Literature Review (September 06, 2024)* **2024**.

Liu, Y.; Baals, L.J.; Osterrieder, J.; Hadji-Misheva, B. Network centrality and credit risk: A comprehensive analysis of peer-to-peer lending dynamics. *Finance Research Letters* **2024**, *63*, 105308.

Agarwal, S.; Zhang, J. FinTech, lending and payment innovation: A review. *Asia-Pacific Journal of Financial Studies* **2020**, *49*, 353–367.

Varsha, P.; Chakraborty, A.; Kar, A.K. How to undertake an impactful literature review: Understanding review approaches and guidelines for high-impact systematic literature reviews. *South Asian Journal of Business and Management Cases* **2024**, *13*, 18–35.

Amato, A.; Osterrieder, J.R.; Machado, M.R. How can artificial intelligence help customer intelligence for credit portfolio management? A systematic literature review. *International Journal of Information Management Data Insights* **2024**, *4*, 100234.

Kushwaha, A.K.; Kar, A.K.; Dwivedi, Y.K. Applications of big data in emerging management disciplines: A literature review using text mining. *International Journal of Information Management Data Insights* **2021**, *1*, 100017.

Ngai, E.W.; Xiu, L.; Chau, D.C. Application of data mining techniques in customer relationship management: A literature review and classification. *Expert systems with applications* **2009**, *36*, 2592–2602.

Xu, J.J.; Lu, Y.; Chau, M. P2P lending fraud detection: A big data approach. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* **2015**, *9074*, 71 – 81. Cited by: 18, https://doi.org/10.1007/978-3-319-18455-5_5.

Liu, F.; You, Y. A big data-based anti-fraud model for internet finance. *Revue d'Intelligence Artificielle* **2020**, *34*, 501 – 506. Cited by: 2; All Open Access, Bronze Open Access, https://doi.org/10.18280/ria.340416.

Chen, Y.; Wang, D. Research on anti-Financial fraud Technology based on Machine learning. *Proceedings - 2020 2nd International Conference on Information Technology and Computer Application, ITCA 2020* **2020**, p. 105 – 108. Cited by: 0, https://doi.org/10.1109/ITCA52113.2020.00029.

Pereira, R.H.; Gonçalves, M.J.A.; Coelho, M.A.G.M. Reputation Systems: A framework for attacks and frauds classification. *Journal of Information Systems Engineering and Management* **2023**, *8*. Cited by: 2; All Open Access, Gold Open Access, https://doi.org/10.55267/iadt.07.12830.

Wang, H. Detection of fraudulent users in P2P financial market. *arXiv preprint arXiv:1910.02010* **2019**.

Li, Y.; Bu, H.; Wu, J. Identifying P2P Lending Frauds Based on Ownership Structure. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS* **2020**, *2020-October*, 250 – 253. Cited by: 2, https://doi.org/10.1109/ICSESS49938.2020.9237736.

Teichmann, F.M.J.; Boticiu, S.R.; Sergi, B.S. Compliance concerns in sustainable finance: an analysis of peer-to-peer (P2P) lending platforms and sustainability. *Journal of Financial Crime* **2024**, *31*, 993 – 1001. https://doi.org/10.1108/JFC-11-2022-0281.

Yadav, P.; Bhosale, R.; Sahoo, R.; Khanzode, V.; Tiwari, M.K. Advances in Air Cargo Financing Using a Consortium Blockchain. *IFAC-PapersOnLine* **2022**, *55*, 737–742.

Acampora, G.; Alghazzawi, D.; Hagras, H.; Vitiello, A. An interval type-2 fuzzy logic based framework for reputation management in Peer-to-Peer e-commerce. *Information Sciences* **2016**, *333*, 88 – 107. Cited by: 37; All Open Access, Green Open Access, https://doi.org/10.1016/j.ins.2015.11.015.

Wang, Y.; Yang, J.; Qi, L. A game-theoretic model for the role of reputation feedback systems in peer-to-peer commerce. *International Journal of Production Economics* **2017**, *191*, 178 – 193. Cited by: 9, https://doi.org/10.1016/j.ijpe.2017.06.012.

Folino, F.; Folino, G.; Pontieri, L. An ensemble-based P2P framework for the detection of deviant business process instances. *Proceedings - 2018 International Conference on High Performance Computing and Simulation, HPCS 2018* **2018**, p. 122 – 129. Cited by: 5, https://doi.org/10.1109/HPCS.2018.00034.

Zhong, Q.Q.; Wei, W.H. A credit model on P2P network based on comments group. *Proceedings - International Conference on Machine Learning and Cybernetics* **2011**, *1*, 344 – 347. Cited by: 0, https://doi.org/10.1109/ICMLC.2011.6016742.

Lai, W. Default Prediction of Internet Finance Users Based on Imbalance-XGBoost. *Tehnicki Vjesnik* **2023**, *30*, 779 – 786. Cited by: 2; All Open Access, Gold Open Access, https://doi.org/10.17559/TV-20230302000395.

Xu, J.; Chen, D.; Chau, M. Identifying features for detecting fraudulent loan requests on P2P platforms. *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016* **2016**, p. 79 – 84. Cited by: 15, https://doi.org/10.1109/ISI.2016.7745447.

Tsuchiya, T.; Cuevas, A.; Christin, N. Identifying Risky Vendors in Cryptocurrency P2P Marketplaces. *WWW 2024 - Proceedings of the ACM Web Conference* **2024**, p. 99 – 110. Cited by: 0, https://doi.org/10.1145/3589334.3645475.

Beekun, R.; Hamdy, R.; Westerman, J.; Hassabelnaby, H. An Exploration of Ethical Decision-making Processes in the United States and Egypt. *Journal of Business Ethics* **2008**, *82*, 587–605. https://doi.org/10.1007/s10551-007-9578-y.

Li, J.; Liu, L.; Xu, J. A P2P e-commerce reputation model based on fuzzy logic. *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010* **2010**, p. 1275 – 1279. Cited by: 7, https://doi.org/10.1109/CIT.2010.230.

Chengeta, K.; Mabika, E.R. Peer to Peer Social Lending Default Prediction with Convolutional Neural Networks. *icABCD 2021 - 4th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, Proceedings* **2021**. Cited by: 3, https://doi.org/10.1109/icABCD51485.2021.9519309.

Li, L.; Zhao, T.; Xie, Y.; Feng, Y. Interpretable Machine Learning Based on Integration of NLP and Psychology in Peer-to-Peer Lending Risk Evaluation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* **2020**, *12431 LNAI*, 429 – 441. Cited by: 2, https://doi.org/10.1007/978-3-030-60457-8_35.

Islam, M.M.; Sohag, A.; Hasan, M.; Islam, M.K.; Sultan, M.N. XAI-Driven Model Explainability and Prediction of P2P Bank Loan Default Network. *Lecture Notes in Networks and Systems* **2024**, *867 LNNS*, 109 – 121. Cited by: 0, https://doi.org/10.1007/978-981-99-8937-9_8.

Li, J.; Hsu, S.; Chen, Z.; Chen, Y. Risks of P2P Lending Platforms in China: Modeling Failure Using a Cox Hazard Model. *Chinese Economy* **2016**, *49*, 161 – 172. Cited by: 27, https://doi.org/10.1080/10971475.2016.1159904.

Cekerevac, Z.; Dvorak, Z.; Prigoda, L.; Cekerevac, P. Risks of bitcoin virtual currency. *Communications - Scientific Letters of the University of Žilina* **2015**, *17*, 93 – 98. Cited by: 1.

Fu, X.; Zhang, S.; Chen, J.; Ouyang, T.; Wu, J. A Sentiment-Aware Trading Volume Prediction Model for P2P Market Using LSTM. *IEEE Access* **2019**, *7*, 81934 – 81944. Cited by: 16; All Open Access, Gold Open Access, https://doi.org/10.1109/ACCESS.2019.2923637.

Wang, Q.; Liu, H.; He, J.; Du, X. A graph attentive network model for P2P lending fraud detection. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* **2020**, *12274 LNAI*, 316 – 327. Cited by: 2, https://doi.org/10.1007/978-3-030-55130-8_28.

Chen, D.; Deakin, S.; Johnston, A.; Wang, B. Too Much Technology and Too Little Regulation? The Spectacular Demise of P2P Lending in China. *Accounting, Economics and Law: A Convivium* **2021**. Cited by: 7; All Open Access, Green Open Access, Hybrid Gold Open Access, https://doi.org/10.1515/ael-2021-0056.

Li, M.; Phan, P.H.; Sun, X. Business friendliness: A double-edged sword. *Sustainability (Switzerland)* **2021**, *13*, 1 – 22. Cited by: 0; All Open Access, Gold Open Access, https://doi.org/10.3390/su13041819.

Xu, J.J.; Chen, D.; Chau, M.; Li, L.; Zheng, H. PEER-TO-PEER LOAN FRAUD DETECTION: CONSTRUCTING FEATURES FROM TRANSACTION DATA. *MIS quarterly* **2022**, *46*.

Lo, T.W.; Kan, W.S. How to win trust: The case of P2P financial fraud in China. *Journal of Criminology* **2023**, *56*, 116–135.

Shen, L.H.; Khan, H.U.; Hammami, H. An empirical study of lenders' perception of Chinese online peer-to-peer (P2P) lending platforms. *Journal of Alternative Investments* **2021**, *23*, 152 – 175. Cited by: 7, https://doi.org/10.3905/JAI.2021.1.128.

K-means algorithm for recognizing fraud users on a bitcoin exchange platform, Vol. 2018-December, 2018. Cited by: 2.

Musau, F.; Wang, G.; Abdullahi, M.B. Group formation with neighbor similarity trust in P2P E-commerce. *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011* **2011**, p. 835 – 840. Cited by: 7, https://doi.org/10.1109/TrustCom.2011.111.

Musau, F.; Wang, G.; Abdullahi, M.B. Group formation with neighbor similarity trust in P2P E-commerce. *Peer-to-Peer Networking and Applications* **2014**, *7*, 295 – 310. Cited by: 6, https://doi.org/10.1007/s12083-011-0116-4.

Wang, Q.; Liu, Y. The research on the peer-to-peer trust model under the internet financial environment. *Computing, Control, Information and Education Engineering - Proceedings of the 2015 2nd International Conference on Computer, Intelligent and Education Technology, CICET 2015* **2015**, p. 745 – 748. Cited by: 0, https://doi.org/10.1201/b18828-171.

Sundaresan, N. Online trust and reputation systems. *EC'07 - Proceedings of the Eighth Annual Conference on Electronic Commerce* **2007**, p. 366 – 367. Cited by: 19, https://doi.org/10.1145/1250910.1250969.

Raghavan, P.; El Gayar, N. Fraud detection using machine learning and deep learning. In Proceedings of the 2019 international conference on computational intelligence and knowledge economy (ICCIKE). IEEE, 2019, pp. 334–339.

Al-dahasi, E.M.; Alsheikh, R.K.; Khan, F.A.; Jeon, G. Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation. *Expert Systems* **2024**, p. e13682.

Cirqueira, D.; Helfert, M.; Bezbradica, M. Towards design principles for user-centric explainable AI in fraud detection. In Proceedings of the International Conference on Human-Computer Interaction. Springer, 2021, pp. 21–40.

Gade, K.; Geyik, S.C.; Kenthapadi, K.; Mithal, V.; Taly, A. Explainable AI in industry. In Proceedings of the Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining, 2019, pp. 3203–3204.

Malik, E.F.; Khaw, K.W.; Belaton, B.; Wong, W.P.; Chew, X. Credit card fraud detection using a new hybrid machine learning architecture. *Mathematics* **2022**, *10*, 1480.

Pourhabibi, T.; Ong, K.L.; Kam, B.H.; Boo, Y.L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems* **2020**, *133*, 113303.

Esenogho, E.; Mienye, I.D.; Swart, T.G.; Aruleba, K.; Obaido, G. A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access* **2022**, *10*, 16400–16407.

 doi:10.20944/preprints202509.1144.v1

Chai, C.; Cao, L.; Li, G.; Li, J.; Luo, Y.; Madden, S. Human-in-the-loop outlier detection. In Proceedings of the Proceedings of the 2020 ACM SIGMOD international conference on management of data, 2020, pp. 19–33.

Xie, X.L. Creditability assessment of dealers in P2P e-commerce. *Proceedings of 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2016* **2017**, p. 1326 – 1333. Cited by: 1, https://doi.org/10.1109/IMCEC.2016.7867428.

Lu, S.; Xu, X.; Wang, H.; Zhao, J.; Wu, Z. Detecting Systemically Important Platforms in P2P Market of China. *2018 15th International Conference on Service Systems and Service Management, ICSSSM 2018* **2018**. Cited by: 0, https://doi.org/10.1109/ICSSSM.2018.8465119.

Kim, H.J.; Jung, J.J.; Jo, G.S. Conceptual framework for recommendation system based on distributed user ratings. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* **2004**, *3032*, 115 – 122. Cited by: 9, https://doi.org/10.1007/978-3-540-24679-4_24.

Yang, B.; Garcia-Molina, H. PPay: Micropayments for peer-to-peer systems. *Proceedings of the ACM Conference on Computer and Communications Security* **2003**, p. 300 – 310. Cited by: 174.