Mitigating Financial Fraud in Indonesia: A Grounded Theory Approach to Fraud Detection in P2P Lending, Rural Banks, and Conventional Banks

Yasser Arafat Akhmad, Sudarso Kaderi Wiryono, Subiakto Sukarno

School of Business and Management, Bandung Institute of Technology (ITB), Indonesia

KEYWORDS
Fraud detection systems, Peer-to-Peer Lending, Rural Credit Banks, conventional banks, financial fraud, multi-subject perception, grounded theory, Indonesia, risk management, digital financial services, financial regulation.

ABSTRACT:
The rapid digitalization of Indonesia's financial sector, driven by the growth of Peer-to-Peer Lending (P2PL) platforms, Rural Credit Banks (BPR), and conventional banks, has expanded financial inclusion but also heightened the risk of fraud. This study investigates the fraud detection systems (FDS) employed by these diverse financial institutions using a grounded theory approach. By conducting semi-structured interviews with key stakeholders—including directors, compliance managers, and fraud control officers—the research identifies critical factors influencing fraud detection in Indonesia's financial ecosystem. The study reveals that while larger institutions leverage advanced machine learning models and real-time transaction monitoring, smaller entities like BPRs rely heavily on manual oversight due to resource constraints. Furthermore, the integration of multi-subject perception differences is highlighted as a novel and effective approach for fraud detection, particularly in P2PL platforms, by analyzing multiple data sources to reduce bias and increase accuracy. However, the study also uncovers significant challenges in implementing robust FDS, including high false-positive rates, regulatory complexities, and resource limitations, particularly in smaller institutions. The findings emphasize the need for a tailored fraud detection framework that addresses the unique needs of each sector, balancing technological advancements with operational feasibility.

1. Introduction

In recent years, the digital revolution has rapidly reshaped Indonesia's financial sector, encompassing both traditional financial institutions such as banks and rural credit banks (BPR), as well as fintech platforms like Peer-to-Peer Lending (P2PL). P2PL, in particular, has introduced a disruptive model of financial intermediation, connecting borrowers and lenders through online platforms without requiring them to meet in person. This has broadened financial access across the country, including for those traditionally excluded from formal financial systems. However, the growth of digital financial services has also expanded opportunities for fraud, raising significant concerns about financial security.

Fraud in the financial sector is not only a severe problem for investors, but it also disrupts the integrity of the market and undermines trust in digital platforms. According to the 2020 Global Study on Occupational Fraud and Abuse by the Association of Certified Fraud Examiners (ACFE), the median financial loss due to fraud is a staggering $950,000, and the typical duration before detection is around 24 months. As online transactions become more prevalent, the threat of fraud has escalated, making fraud detection systems (FDS) a critical component of any financial institution's risk management strategy. This is particularly urgent for the growing fintech industry, which, unlike traditional banking, operates within a less regulated environment and faces distinct risks (G. Li et al., 2024).

The challenge of financial fraud detection is compounded by the complex nature of fraudulent behaviors and the vast amount of transactional data generated in digital platforms. While many studies have focused on using financial indicators, such as abnormal transaction frequencies or suspicious account behaviors, to detect fraud, these approaches are often inadequate in capturing the nuances of fraud in digital financial ecosystems. In Indonesia's diverse financial landscape, where P2PL, rural banks, and traditional banks coexist, there is a need for a more robust, sector-specific approach to fraud detection.

This study employs a grounded theory approach to develop a comprehensive understanding of fraud detection systems within Indonesia's financial institutions. Grounded theory, as a qualitative research methodology, allows for the generation of theory directly from the data, making it an ideal approach for exploring the multifaceted and evolving nature of fraud in the financial sector. By focusing on the experiences and practices of key stakeholders—such as fraud control officers, compliance managers, and regulatory bodies—this research seeks to identify the critical factors that influence fraud detection across different financial institutions.

This paper aims to bridge the gap between existing fraud detection models and the specific requirements of Indonesia's financial institutions. By understanding the unique challenges faced by P2PL platforms, rural banks, and traditional banks, this study proposes a tailored fraud detection framework that considers the distinct characteristics of each sector. Furthermore, the grounded theory approach facilitates a deeper exploration of the socio-economic and regulatory factors that shape fraud detection practices, providing a more nuanced understanding of how financial institutions in Indonesia can enhance their fraud detection capabilities.

2. LITERATURE REVIEW

2.1 The Evolution of Financial Fraud Detection

The evolution of fraud detection systems (FDS) in the financial industry has been a response to the increasing sophistication of fraudulent activities, driven largely by technological advancements and the growing complexity of financial transactions. Early models of fraud detection, such as Beneish's financial fraud detection model, relied heavily on financial ratios to detect irregularities that might indicate fraudulent behavior. These traditional models focused on examining discrepancies in financial statements, which were often used to uncover financial misreporting, as seen in cases like the Enron scandal (Pettker et al., 2023; Shahana et al., 2023). However, while such models provided a foundational framework for detecting fraud, they were largely reactive, catching fraud only after it had occurred and been reported in financial disclosures.

Over time, fraud detection mechanisms have evolved to include more advanced techniques, leveraging technological tools such as machine learning, artificial intelligence, and big data analytics. The shift from static financial data to dynamic data streams has enabled financial institutions to detect fraud in real-time. This shift was essential in addressing the limitations of earlier models that primarily focused on historical financial data. Studies such as those by Charizanos et al. (2024) highlight the role of textual data mining from financial statements, news media, and social media as a way to uncover hidden signals of potential fraud. The use of such non-traditional data sources has expanded the scope of FDS, allowing institutions to respond to potential fraud before it results in significant financial losses.

Nevertheless, the increasing complexity of financial ecosystems, particularly with the advent of digital finance, has exposed the inadequacies of traditional fraud detection models. Fraudsters have adapted their methods, exploiting the rapid expansion of internet-based financial platforms such as Peer-to-Peer Lending (P2PL) platforms, which do not fit neatly into the risk profiles built for conventional banking institutions (Charizanos et al., 2024; Suryono et al., 2021). As a result, fraud detection systems today must contend with more decentralized models of financial transactions, where borrower and lender interactions are largely online and often anonymous.

To address these challenges, there has been a growing focus on using hybrid models that combine both financial and non-financial data to detect fraudulent activity. While financial ratios remain a valuable tool, their limitations in detecting fraud in digital financial platforms necessitate the use of more sophisticated data-mining techniques. These include leveraging algorithms capable of identifying patterns across large datasets, many of which may not be directly related to financial performance but still signal potential fraudulent behavior. For example, the inclusion of behavioral data, such as login patterns or geolocation tracking, has proven crucial in identifying anomalies in user behavior that could indicate fraudulent activities (Zhao et al., 2024).

In conclusion, the evolution of financial fraud detection has shifted from simple financial ratio analysis to more comprehensive, technology-driven systems that integrate both financial and non-financial data. The increasing complexity of digital finance platforms, particularly P2PL, demands new approaches that can adapt to the decentralized and often anonymous nature of transactions. As such, modern fraud detection systems must be flexible, capable of analyzing diverse datasets, and responsive to the rapidly changing financial landscape.

2.2 Challenges of Fraud Detection in Digital Finance

The rapid digitization of financial services, particularly in the fintech and Peer-to-Peer Lending (P2PL) sectors, has introduced significant challenges for traditional fraud detection systems. As fintech platforms outpace regulatory frameworks (Akhmad et al., 2022a), new vulnerabilities emerge in the financial ecosystem. The increased reliance on online transactions, often without the stringent oversight of conventional banking systems, has created an environment where fraudsters can exploit these digital platforms using sophisticated techniques such as account takeovers, synthetic identity fraud, and transaction laundering (Lebichot et al., 2024; J. Li et al., 2020). These methods are not easily detected by conventional fraud detection systems that rely primarily on numerical data or simple rule-based approaches.

One of the major challenges in detecting fraud in digital finance is the complexity of the data generated by online transactions. While traditional financial fraud models focused on financial ratios and static transaction data, digital finance operates at a scale and speed that requires real-time detection mechanisms. Fraudsters often exploit this speed by carrying out high-volume, low-value transactions that bypass traditional red flags. Additionally, the rise of synthetic identity fraud, where fraudsters create false identities using real and fabricated data, has complicated fraud detection efforts in P2PL platforms. These synthetic identities are often indistinguishable from real users, making it difficult for conventional systems to flag them as fraudulent.

Furthermore, the subjective nature of textual data presents another layer of complexity in fraud detection. Many fraud detection systems today incorporate textual data from financial statements or customer communications to identify potential red flags. However, this data is often subject to manipulation by internal management or external actors. For instance, financial statements may present an overly positive view of a company’s financial health, leading to a false sense of security (Aftabi et al., 2023). The inherent bias in such data makes it difficult for fraud detection systems to rely solely on internal reports, emphasizing the need for cross-referencing with external sources, such as news reports, social media sentiment, or third-party audits.

Another challenge in the digital finance landscape is the regulatory gap between fintech platforms and traditional banks. While traditional financial institutions are subject to strict regulations, fintech platforms, particularly in developing markets like Indonesia, often operate in a gray area where regulations are either unclear or non-existent. This lack of regulatory oversight enables fraudsters to exploit loopholes, such as by opening multiple accounts under different identities or conducting fraudulent transactions across borders, where enforcement may be weaker (Cumming & Johan, 2020).

To address these challenges, there is a need for more robust fraud detection systems that integrate multiple data sources and perspectives. These systems must be able to process large volumes of data in real-time, detect complex patterns, and adapt to new forms of fraud as they emerge (Muthukannan et al., 2020). However, implementing such systems requires significant investment in technology, expertise, and regulatory cooperation, particularly in markets like Indonesia, where the financial landscape is rapidly evolving.

2.3 The Role of Multi-Source Perceptions in Fraud Detection

The integration of multi-source data has emerged as a critical development in the evolution of fraud detection systems. As financial institutions recognize the limitations of relying on single-source data, such as financial ratios or internal reports, there has been a shift toward incorporating external data to provide a more comprehensive view of potentially fraudulent activities. This multi-source approach is particularly valuable in detecting inconsistencies between different datasets, which can offer critical clues to uncovering fraud (Lebichot et al., 2024; Wu et al., 2024).

For example, discrepancies between a company’s financial statements and external sources, such as news reports or social media sentiment, may indicate potential fraud. Financial data alone often presents an incomplete picture, especially when internal reports are subject to management bias or manipulation (Ripamonti, 2020). By integrating external data sources, such as public sentiment on social media or third-party audits, fraud detection systems can cross-check internal financial reports against independent perspectives, providing a more accurate assessment of a company’s financial health (Gao & Sun, 2020).

In Indonesia, where the financial sector is diverse and includes both traditional and fintech platforms, the multi-source approach is particularly relevant. The fragmented nature of the financial system, with P2PL platforms operating alongside conventional and rural banks, creates an environment where single-source fraud detection models may overlook sector-specific risks. For instance, a P2PL platform may face risks related to fraudulent borrowers that are not applicable to traditional banks, while rural banks may be more vulnerable to insider fraud. Multi-source perception differences—such as discrepancies between borrower-reported financial data and social media activity—can provide critical insights that single-source models may miss (Akhmad et al., 2022b).

The use of multi-source data is further enhanced by the integration of sentiment analysis. By analyzing public and private financial data alongside sentiment expressed in social media or news media, financial institutions can identify shifts in public perception that may signal potential fraud. For example, negative sentiment in news articles or social media posts, when cross-referenced with positive internal reports, may indicate an attempt to conceal fraud or manipulate public opinion. This approach allows for a more nuanced understanding of a company's financial behavior, particularly in rapidly changing markets like fintech (Sun et al., 2023).

The adoption of multi-source perceptions in fraud detection has proven particularly effective in identifying sophisticated fraud schemes. By broadening the range of data sources used in fraud detection, institutions can reduce the risk of bias inherent in single-source data and improve the overall accuracy of fraud detection systems. This approach has been shown to improve fraud detection accuracy by approximately 10%, particularly in fintech platforms where transparency is limited (Patil et al., 2024).

2.4 The Grounded Theory Approach to Fraud Detection

Grounded theory, as a methodological framework, provides a flexible and dynamic approach to understanding the complexities of fraud detection in the financial sector (Villalba et al., 2023). By allowing theories to emerge directly from data, grounded theory enables researchers to explore the evolving nature of fraud and the contextual factors that influence fraud detection practices. This approach is particularly valuable in fraud detection research, where technological advancements, regulatory changes, and new fraud techniques continuously reshape the landscape.

Grounded theory has been effectively used in previous studies to explore the relationship between fraud detection systems and external regulatory frameworks. For example, Abdallah et al. (2016) applied grounded theory to uncover the nuanced relationships between various fraud indicators, such as transaction frequency, abnormal timing, and high-risk user profiles. By focusing on the real-world experiences of fraud control officers, compliance managers, and regulatory bodies, the grounded theory allows researchers to gain insights into how fraud detection systems can be tailored to specific sectors.

In the Indonesian context, grounded theory is particularly useful in understanding how fraud detection systems must adapt to the diverse financial landscape (Nikkel, 2020). The coexistence of traditional banks, rural credit banks, and fintech platforms creates a complex environment where different sectors face distinct fraud risks and regulatory challenges. By collecting data from stakeholders across these sectors, grounded theory provides a framework for developing fraud detection models that are responsive to the specific needs of each sector.

Moreover, grounded theory enables researchers to explore the human factors that influence fraud detection practices. Fraud detection is not solely a technological issue; it is also shaped by the attitudes, perceptions, and actions of individuals within financial institutions. By examining the experiences of fraud control officers and compliance managers, grounded theory reveals the practical challenges faced by those tasked with implementing fraud detection systems, such as balancing regulatory compliance with operational efficiency (McKillop et al., 2020).

In summary, grounded theory offers a valuable methodological approach for fraud detection research (Abdallah et al., 2016), providing insights into the evolving nature of fraud and the contextual factors that shape detection practices. This approach is particularly relevant in the Indonesian financial sector, where diverse financial institutions require tailored fraud detection models that can adapt to the specific risks and challenges of each sector.

2.5 Sector-Specific Fraud Detection in Indonesia

Indonesia's financial landscape is characterized by the coexistence of traditional banks, rural credit banks (BPR), and fintech platforms, each facing unique fraud risks and regulatory challenges. Traditional banks, which are subject to stringent regulatory oversight, have developed comprehensive fraud detection systems that rely on real-time monitoring, machine learning algorithms, and anomaly detection. These systems are designed to flag suspicious activities, such as large cross-border transfers or sudden changes in account behavior, which may indicate fraud (Akhmad et al., 2023).

In contrast, rural credit banks (BPR) operate in a less regulated environment and are often constrained by limited financial and technological resources. As a result, BPRs typically rely on simpler, rule-based fraud detection systems that focus on flagging abnormal transactions, such as sudden surges in deposits or frequent small withdrawals. However, these systems are often insufficient for detecting more sophisticated forms of fraud, such as identity theft or insider fraud, which can be more difficult to identify in smaller institutions (Chatterjee et al., 2024).

P2PL platforms, which operate in a largely unregulated space, face distinct challenges in fraud detection. The decentralized nature of P2PL platforms, where borrowers and lenders interact directly through digital platforms, makes it difficult to apply traditional fraud detection models. Fraudsters often exploit loopholes in the system, such as by creating multiple accounts under false identities or engaging in transaction laundering. As a result, P2PL platforms require fraud detection models that are tailored to the specific risks of digital finance, including synthetic identity fraud and account takeovers (Duan et al., 2024).

This study seeks to address these sector-specific challenges by using a grounded theory approach to explore how fraud detection systems can be adapted to Indonesia's unique financial environment. By analyzing the experiences of stakeholders across different sectors, this research will develop a comprehensive fraud detection framework that accounts for the distinct characteristics of P2PL platforms, rural banks, and traditional banks. This framework will provide practical recommendations for improving fraud detection systems in each sector, ensuring that they are responsive to the specific risks and regulatory challenges faced by different financial institutions.

In conclusion, the sector-specific approach to fraud detection recognizes the diverse nature of Indonesia's financial sector and the need for tailored fraud detection systems. By using grounded theory to explore the experiences of key stakeholders, this research will provide valuable insights into how fraud detection systems can be adapted to meet the specific needs of P2PL platforms, rural banks, and traditional banks.

3. METHODOLOGY/MATERIALS

This study employs a qualitative research approach using grounded theory to explore fraud detection systems (FDS) within Indonesia's financial institutions, specifically focusing on Peer-to-Peer Lending (P2PL), rural banks, and traditional banks. Grounded theory, a systematic methodology in social sciences (Guerrero Puerta & Lorente García, 2023), allows for the generation of theory based on the data collected during the research process (Strauss & Corbin, 1998). It is particularly suited for this research as fraud detection within the Indonesian financial context is a multifaceted and evolving issue, requiring insights from industry experts.

3.1 Research Design

Grounded theory was selected as the methodological approach to enable the development of a conceptual framework that emerges directly from the data, particularly from the perspectives of senior professionals working within financial institutions. This approach emphasizes the importance of inductively generating theory from real-world experiences, which is crucial in understanding how fraud detection systems (FDS) operate across different sectors, including P2PL, rural banks, and traditional banks.

To collect the necessary data, semi-structured in-depth interviews were conducted with twelve experienced professionals, each with over 15 years of work experience in various senior roles within the financial sector. These professionals were selected from conventional banks, Sharia banks, fintech P2PL, and rural banks, providing a broad perspective on fraud detection across different types of financial institutions (Akhmad et al., 2024).

3.2 Sampling and Participant Selection

A purposive sampling technique was used to select the participants for this study, ensuring that each individual had substantial experience and direct involvement in fraud detection or management within their respective organizations. The sample consists of professionals holding senior positions such as Chief Operating Officers (COOs), Vice Presidents, Directors, Senior Managers, and General Managers from different financial sectors (Akhmad et al., 2023), as detailed in the table below:

Table 1. List of respondents

No.	Position Level	Organization	Data Collection Type	Total Work Experience (in Years)	Meeting Type
1	COO (Director)	Conventional Bank	Semi-Structure In-Depth Interview	≥ 15	Online
2	Vice President (Director)	Conventional Bank	Semi-Structure In-Depth Interview	≥ 15	Online
3	Vice President (Director)	Conventional Bank	Semi-Structure In-Depth Interview	≥ 15	Online
4	Senior-Manager	Conventional Bank	Semi-Structure In-Depth Interview	≥ 15	Online
5	Director	Sharia Bank	Semi-Structure In-Depth Interview	≥ 15	Online
6	Senior-Manager	Sharia Bank	Semi-Structure In-Depth Interview	≥ 15	Online
7	Director	Fintech P2PL	Semi-Structure In-Depth Interview	≥ 15	Online
8	Director	Fintech P2PL	Semi-Structure In-Depth Interview	≥ 15	Online
9	Director	Fintech P2PL	Semi-Structure In-Depth Interview	≥ 15	Online
10	Senior-Manager	Fintech P2PL	Semi-Structure In-Depth Interview	≥ 15	Online
11	General Manager (Director)	Rural Bank	Semi-Structure In-Depth Interview	≥ 15	Offline

3.3 Data Collection Methods

The primary data collection method for this study was semi-structured in-depth interviews. Semi-structured interviews were chosen for their flexibility, allowing for a balance between guiding the conversation and allowing participants to share their insights and experiences freely. This approach enabled the researchers to capture detailed narratives and personal perspectives on how fraud detection systems are implemented and managed across different financial sectors.

Each interview followed a pre-determined guide with open-ended questions designed to elicit in-depth responses about the participant's experiences with fraud detection systems, the challenges they face, the effectiveness of the systems, and their recommendations for improving fraud detection processes. The use of open-ended questions also allowed the participants to explore topics they considered important, providing a richer data set that is reflective of real-world scenarios.

The interviews were conducted over a period of two months, primarily using online meeting platforms for participants from conventional banks, Sharia banks, and fintech P2PL. The face-to-face interview with the General Manager from the rural bank provided an opportunity for deeper engagement and contextual observation, which helped in understanding the specific challenges faced by rural credit banks in detecting fraud.

3.4 Data Analysis

Data analysis followed the grounded theory approach, which involves three stages of coding: open coding, axial coding, and selective coding (Strauss & Corbin, 1998).

1. Open Coding: In this first stage, the interview transcripts were thoroughly reviewed, and the data was broken down into discrete parts. Codes were assigned to identify recurring themes, phrases, and patterns related to fraud detection practices across the different types of financial institutions. The key concepts that emerged from the interviews were fraud indicators, the use of technology in fraud detection, sector-specific challenges, and regulatory gaps.

2. Axial Coding: The second stage of analysis involved identifying relationships between the concepts discovered during open coding. This process helped in grouping the codes into broader categories and finding links between different fraud detection practices across sectors. For example, the use of automated systems in fintech P2PL fraud detection was compared to manual review processes in rural banks.

3. Selective Coding: In the final stage, the core themes were refined into a central theory about fraud detection systems in Indonesia. This theory integrates the experiences of participants and offers a conceptual framework for understanding how fraud detection is managed, the factors that influence its effectiveness, and the sector-specific needs for improving fraud detection systems.

3.5 Validation and Reliability

To ensure the validity of the findings, multiple strategies were employed, including triangulation of data sources and member checking. Triangulation was achieved by comparing insights from participants across different sectors (e.g., conventional banks, P2PL, rural banks) to identify commonalities and differences in fraud detection practices. Member checking was used to validate the findings by sharing the preliminary results with participants to ensure that their experiences and views were accurately represented.

The reliability of the research process was maintained by following consistent procedures for conducting interviews, coding, and analyzing the data. Detailed records were kept for each interview, including transcripts and field notes, allowing for transparency and replicability.

4. RESULTS AND DISCUSSIONS

4.1 Overview of Fraud Detection Mechanisms in Indonesia’s Financial Sector

The rapid digitization of Indonesia’s financial sector, encompassing conventional banks, Rural Credit Banks (BPR), and fintech platforms, has opened the door to new and sophisticated methods of fraud. These institutions face the constant challenge of maintaining fraud detection systems (FDS) that are capable of monitoring increasingly complex and high-frequency transactions. Each sector implements fraud detection mechanisms specific to their operational and regulatory environments, with varied levels of technological sophistication and internal control structures.

Fraud detection in Indonesia's financial institutions typically revolves around real-time transaction monitoring, anomaly detection, and rule-based systems. As revealed through interviews with directors, risk management heads, and fraud control officers across various financial institutions, the design and application of fraud detection systems rely on predefined fraud indicators, both at the account level (such as login patterns, device IDs, and IP changes) and transaction level (unusual transaction volumes, geolocation discrepancies). However, the effectiveness of these systems largely depends on the resources available and the institution's capacity to handle false positives, regulatory compliance, and overall risk management strategies.

4.2 Fraud Detection in P2PL Platforms

Peer-to-peer lending (P2PL) platforms in Indonesia, being among the most rapidly growing segments, are especially vulnerable to fraud due to the high volume of digital transactions and the relatively low level of personal interaction between lenders and borrowers. The interview data suggests that P2PL platforms typically implement a combination of fraud detection techniques, including identity verification, transaction monitoring, and credit risk assessments, to combat fraud at both the user and transaction levels.

One of the critical strategies employed by P2PL platforms is the use of multi-subject perception differences, where multiple sources of data are analyzed to identify discrepancies between borrower claims and their actual financial behavior. For instance, fraudulent borrowers often provide misleading information about their income, which can be detected by comparing data from credit bureaus, bank statements, and social media. This method, as pointed out by directors of fintech companies, helps mitigate bias that may occur when relying on a single data source. Additionally, P2PL platforms use advanced machine learning models to flag transactions that deviate from normal user behavior, especially transactions involving high-risk profiles such as users with prior fraud history or those conducting transactions at odd hours (midnight to early morning).

The reliance on automated fraud detection systems like Fraud Labs, which evaluates factors such as device validation, IP address validation, and behavioral patterns, ensures a scalable solution. However, challenges remain in reducing false positives and ensuring the system's adaptability to emerging fraud patterns.

4.3 Fraud Detection in Rural Credit Banks (BPR)

Rural credit banks (BPR) face unique challenges in fraud detection due to their limited technological infrastructure and resources compared to larger institutions. Interviews with general managers and directors from rural credit banks reveal that while these institutions are committed to adhering to regulatory standards for fraud detection, they often lack the sophisticated, real-time monitoring tools employed by conventional banks and fintech platforms.

BPRs primarily rely on manual oversight and periodic transaction reviews, which increases the potential for fraud detection delays. Fraud detection in these institutions tends to focus on transactional inconsistencies such as abnormal withdrawals, irregular patterns of deposit, and unusual cash flows that are flagged by internal audits or risk management teams. However, fraud in rural credit banks often manifests in more subtle forms, such as identity fraud and manipulation of financial records by insiders. The introduction of more automated and real-time systems has been slow due to cost constraints, making BPRs more reliant on employee vigilance and customer complaints to identify suspicious activities.

Despite these limitations, BPRs have made strides in aligning their fraud detection protocols with larger banks by adopting basic fraud detection systems. For instance, a simple rule-based monitoring system flags unusual transaction behaviors, such as frequent withdrawals in small amounts or sudden surges in deposits, which may indicate fraudulent activity.

4.4 Fraud Detection in Conventional Banks and Sharia Banks

Conventional banks and Sharia banks in Indonesia deploy more comprehensive fraud detection systems compared to BPRs and P2PL platforms. These institutions often leverage sophisticated FDS platforms that incorporate machine learning algorithms, rule-based detection, anomaly detection, and geolocation tracking to monitor transactions in real-time. According to senior managers from conventional and Sharia banks, the focus is on flagging transactions that deviate from the customer’s normal behavior patterns, such as large cross-border transfers, frequent account logins from different IP addresses, or sudden changes in account activity.

Sharia banks, in particular, face the additional complexity of ensuring that their fraud detection mechanisms comply with Islamic principles while maintaining a high level of financial scrutiny. As such, fraud detection systems in these banks not only flag financial irregularities but also monitor compliance with Sharia principles, such as prohibitions against transactions involving alcohol, gambling, or other non-compliant sectors.

Both conventional and Sharia banks have invested heavily in internal controls, with fraud control officers conducting regular reviews of flagged transactions. The role of the internal auditor is critical in these institutions, providing an additional layer of oversight through periodic evaluations of the fraud detection systems’ performance.

4.5 Role of Multi-Subject Perception Differences in Fraud Detection

The introduction of multi-subject perception differences as a fraud detection strategy marks a significant advancement in detecting financial fraud, particularly in P2PL platforms. By evaluating a transaction or user across multiple sources—such as financial statements, social media behavior, and credit bureau data—multi-subject perception helps identify discrepancies that might otherwise go unnoticed in a single-subject analysis. This technique minimizes the risk of bias, especially in financial institutions where management or customer reports may present overly positive assessments.

The interviews revealed that directors and managers view this approach as especially useful in detecting early signs of fraud. In practice, this means triangulating data from various sources, such as customer interactions, third-party databases, and transactional histories, to generate a comprehensive fraud risk profile. The use of sentiment analysis on public and private financial data, cross-referenced with internal reports, provides a more nuanced understanding of a company's financial behavior.

This technique has proven particularly effective in detecting sophisticated fraud schemes that might evade traditional financial audits or transaction monitoring systems. The study highlighted that the application of multi-subject perception differences has boosted fraud detection accuracy by approximately 10%, as reported by directors in the fintech industry.

4.6 Challenges in Implementing Fraud Detection Systems

Despite advancements in fraud detection, significant challenges remain in implementing robust FDS across Indonesia’s financial sector. One of the primary issues identified through the interviews is the difficulty of maintaining a balance between thorough fraud detection and customer experience. High false-positive rates, especially in P2PL platforms and BPRs, often lead to unnecessary account freezes or transaction rejections, which can frustrate legitimate customers.

Despite the advancements in fraud detection, significant challenges remain in implementing effective FDS across Indonesia’s financial institutions. One of the primary challenges identified is the high false-positive rates generated by these systems, particularly in P2PL platforms and BPRs. False positives can lead to unnecessary account freezes or transaction rejections, causing frustration among legitimate customers.

Another major challenge is the disparity in resource availability between larger financial institutions and smaller entities like BPRs. While conventional and Sharia banks can afford to invest in cutting-edge technologies, smaller banks struggle to allocate sufficient resources for implementing advanced FDS. Regulatory compliance adds another layer of complexity, particularly with anti-money laundering (AML) and counter-terrorism financing (CFT) requirements, which demand a high level of scrutiny in fraud detection processes.

Human resource limitations also play a role in hindering fraud detection efforts. While automated systems provide significant support, many institutions still rely on manual oversight, particularly in the investigation of flagged transactions. The shortage of specialized fraud detection professionals, especially in smaller institutions, limits their capacity to respond swiftly and effectively to potential fraud.

Finally, the dynamic nature of fraud itself presents an ongoing challenge. Fraudsters continuously adapt to existing detection methods, necessitating regular updates to FDS and ongoing training for fraud detection teams. The rapid evolution of fraud techniques means that financial institutions must remain vigilant and invest in both technological and human resources to stay ahead of emerging threats.

Table 2: Key Fraud Indicators for Financial Institutions

Category	Indicators	Criteria
Transaction Frequency	High frequency of transactions exceeding normal limits	Daily or monthly transactions exceeding predefined limits
Transaction Timing	Transactions conducted at unusual times (e.g., midnight to early morning)	Transactions between 00:00 - 05:00
Geolocation Discrepancies	Transactions conducted in high-risk areas based on geographical risk assessments	Users located in regions identified as high-risk for fraud (based on AML guidelines)
Profile Risk	Users or merchants involved in high-risk profiles, such as prior fraud history or regulatory risks	Users or merchants flagged by fraud detection systems for unusual behavior or high-risk regions
Transaction Amounts	Unusually high or low transaction amounts relative to normal user behavior	Transactions exceeding predefined limits based on user profiles

This table provides a summary of key indicators that financial institutions use to detect potential fraud based on transaction frequency, timing, geolocation discrepancies, and user profiles. These indicators are critical in guiding the design and implementation of FDS across various sectors of Indonesia’s financial industry.

5. CONCLUSION

This journal explores the landscape of fraud detection mechanisms within Indonesia's financial sector, with a particular focus on Peer-to-Peer Lending (P2PL) platforms, Rural Credit Banks (BPR), conventional banks, and Sharia banks. It presents a detailed analysis of fraud detection systems (FDS), including the use of multi-subject perception differences, and the challenges of implementing effective fraud detection mechanisms across these institutions.

5.1 Overview of Fraud Detection Mechanisms in Indonesia’s Financial Sector

The rapid expansion of digital financial services in Indonesia has significantly increased the risk of fraud across all financial sectors. This chapter outlines the varying levels of technological adoption in fraud detection among conventional banks, rural banks, and fintech P2PL platforms. Larger institutions are more advanced in their use of real-time monitoring and machine learning-driven systems, while smaller entities, such as BPRs, often rely on manual oversight and periodic transaction reviews due to resource limitations.

5.2 Fraud Detection in P2PL Platforms

P2PL platforms face heightened exposure to fraud due to their online nature and high transaction volumes. This section emphasizes the use of multi-subject perception differences as a key method for improving fraud detection accuracy. By comparing diverse data sources—ranging from financial records to social media behavior—P2PL platforms can detect inconsistencies that would be missed by single-source analysis. Despite its benefits, the implementation of such systems remains resource-intensive, often causing friction between ensuring security and maintaining a seamless user experience.

5.3 Fraud Detection in Rural Credit Banks (BPR)

The fraud detection capabilities of rural credit banks are constrained by limited technological and financial resources. This chapter discusses how these banks rely on simpler, rule-based systems to flag abnormal transactions but face delays in real-time monitoring and investigation. The challenges of implementing advanced FDS in BPRs highlight the need for scalable, cost-effective solutions to protect against fraud without overwhelming the institution's operational capacity.

5.4 Fraud Detection in Conventional Banks and Sharia Banks

Conventional and Sharia banks in Indonesia are comparatively better equipped to combat fraud due to their substantial investments in real-time fraud detection systems and advanced algorithms. These banks integrate anomaly detection, geolocation tracking, and rule-based monitoring to detect suspicious activities. Sharia banks, in particular, must also ensure their fraud detection systems comply with Islamic financial principles, which introduces additional complexity to the detection process. Internal auditors play a crucial role in maintaining the integrity of these systems, and ensuring compliance with evolving regulatory standards. This robust internal control framework has enabled both conventional and Sharia banks to stay ahead of increasingly sophisticated fraud schemes.

5.5 Role of Multi-Subject Perception Differences in Fraud Detection

Multi-subject perception differences provide a breakthrough in fraud detection by comparing various data points from both internal and external sources. This method significantly reduces bias and improves fraud detection accuracy by approximately 10%, according to fintech directors interviewed. The chapter highlights how this approach is particularly effective in identifying sophisticated fraud schemes that evade traditional transaction monitoring. This section also delves into the technical process of implementing sentiment analysis and multi-source data triangulation, which has proven especially effective in the P2PL sector.

5.6 Challenges in Implementing Fraud Detection Systems

Despite technological advancements, implementing effective FDS remains fraught with challenges, particularly in balancing detection accuracy with customer experience. High false-positive rates, resource constraints, and regulatory complexities are recurring issues across all sectors. This chapter details the operational and financial hurdles faced by smaller institutions, such as BPRs, which lack the expertise and technological infrastructure to implement advanced FDS. The dynamic nature of fraud also poses a challenge, requiring continuous system updates and employee training to stay ahead of emerging threats. The chapter concludes with recommendations for strengthening fraud detection systems, particularly through the integration of automated and manual oversight mechanisms tailored to the institution's size and scope.

LIST OF ABBREVIATIONS

BPR: Rural Credit Bank (Bank Perkreditan Rakyat), AML-CFT: Anti-Money Laundering and Countering the Financing of Terrorism, FDS: Fraud Detection System, P2PL: Peer-to-Peer Lending, SOP: Standard Operating Procedure.

DECLARATIONS

Ethical Considerations

Ethical approval was obtained prior to data collection, and all participants were informed about the purpose of the study. They were assured of confidentiality and anonymity, with personal identifiers being removed from the transcripts to protect their identities. Informed consent was obtained from each participant before the interviews, ensuring that they understood the research objectives and their right to withdraw from the study at any time.

Competing interest

The authors state that they have no business or financial interests associated with the research described in this paper.

Funding

Not applicable.

Authors' contributions

YAA: he contributed to the conceptualization, methodology, software, curation, data writing, and original draft preparation; SKW: he contributed to supervision, review writing, and approved the manuscript; SS: he contributed to supervision, review writing, and approved the manuscript.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the useful input, suggestions, and comments from the journal's anonymous referrer that contributed to the value of this paper.

References:

[1] Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90–113. https://doi.org/https://doi.org/10.1016/j.jnca.2016.04.007

[2] Aftabi, S. Z., Ahmadi, A., & Farzi, S. (2023). Fraud detection in financial statements using data mining and GAN models. Expert Systems with Applications, 227, 120144. https://doi.org/https://doi.org/10.1016/j.eswa.2023.120144

[3] Akhmad, Y. A., Wiryono, S. K., & Sukarno, S. (2022a). Lending Banking And Financial Technology Peer-to-Peer Lending Between Disrupt or Creativity. Central Asia and the Caucasus, 23(1), 3439–3453. https://doi.org/https://doi.org/10.37178/ca-c.23.1.245

[4] Akhmad, Y. A., Wiryono, S. K., & Sukarno, S. (2022b). The Potential Way Forward for Bank Lending and Peer-to-Peer Lending, and What Should They Do? Baltic Journal Of Law & Politics A Journal of Vytautas Magnus University, 15(1), 944–956. https://doi.org/10.2478/bjlp-2022-00061

[5] Akhmad, Y. A., Wiryono, S. K., & Sukarno, S. (2023). After The Emergence Of Peer-To-Peer Lending , Will Peer-To-Peer Lending Be Disrupted By The Transformation Of Other Lending Financial Institutions ? Journal of Namibian Studies, 35, 1480–1513. https://namibian-studies.com/index.php/JNS/article/view/3703

[6] Akhmad, Y. A., Wiryono, S. K., & Sukarno, S. (2024). Mitigating Default Risks In Peer-To-Peer Lending Platforms : The Role Of Information Asymmetry In Indonesia. 27(3), 1201–1218. https://doi.org/10.53555/AJBR.v27i3S.2256

[7] Charizanos, G., Demirhan, H., & İçen, D. (2024). An online fuzzy fraud detection framework for credit card transactions. Expert Systems with Applications, 252, 124127. https://doi.org/https://doi.org/10.1016/j.eswa.2024.124127

[8] Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems, 158, 410–426. https://doi.org/https://doi.org/10.1016/j.future.2024.04.057

[9] Cumming, D. J., & Johan, S. A. (2020). Regulation and investment in fintech ventures. In Crowdfunding (pp. 405–431). Elsevier. https://doi.org/10.1016/b978-0-12-814637-8.00018-4

[10] Duan, W., Hu, N., & Xue, F. (2024). The information content of financial statement fraud risk: An ensemble learning approach. Decision Support Systems, 182, 114231. https://doi.org/https://doi.org/10.1016/j.dss.2024.114231

[11] Gao, X., & Sun, L. (2020). Modeling Retirees' Investment Behaviors in the Presence of Health Expenditure Risk and Financial Crisis Risk. Economic Modelling. https://doi.org/10.1016/j.econmod.2020.10.013

[12] Guerrero Puerta, L., & Lorente García, R. (2023). Illuminating the path: a methodological exploration of grounded theory in doctoral theses. Qualitative Research Journal, 24(4), 384–393. https://doi.org/https://doi.org/10.1108/QRJ-07-2023-0119

[13] Lebichot, B., Siblini, W., Paldino, G. M., Le Borgne, Y.-A., Oblé, F., & Bontempi, G. (2024). Assessment of catastrophic forgetting in continual credit card fraud detection. Expert Systems with Applications, 249, 123445. https://doi.org/https://doi.org/10.1016/j.eswa.2024.123445

[14] Li, G., Wang, S., & Feng, Y. (2024). Making differences work: Financial fraud detection based on multi-subject

perceptions. Emerging Markets Review, 60, 101134. https://doi.org/https://doi.org/10.1016/j.ememar.2024.101134

[15] Li, J., Li, J., Zhu, X., Yao, Y., & Casu, B. (2020). Risk spillovers between FinTech and traditional financial institutions: Evidence from the U.S. International Review of Financial Analysis, 71. https://doi.org/10.1016/j.irfa.2020.101544

[16] McKillop, D., French, D., Quinn, B., Sobiech, A. L., & Wilson, J. O. S. (2020). Cooperative financial institutions: A review of the literature. International Review of Financial Analysis, 71, 101520. https://doi.org/https://doi.org/10.1016/j.irfa.2020.101520

[17] Muthukannan, P., Tan, B., Gozman, D., & Johnson, L. (2020). The emergence of a Fintech Ecosystem: A case study of the Vizag Fintech Valley in India. Information & Management, 57(8), 103385. https://doi.org/https://doi.org/10.1016/j.im.2020.103385

[18] Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. Forensic Science International: Digital Investigation, 33, 200908. https://doi.org/10.1016/j.fsidi.2020.200908

[19] Patil, A., Mahajan, S., Menpara, J., Wagle, S., Pareek, P., & Kotecha, K. (2024). Enhancing fraud detection in banking by integration of graph databases with machine learning. MethodsX, 12, 102683. https://doi.org/https://doi.org/10.1016/j.mex.2024.102683

[20] Pettker, C. M., Cambell, K. H., Aghababaei Jazi, O., Barach, P., Wiggin, H., Risner, P., Johnson, J. J., Patrishkoff, D., Kurra, S., Southern, B., Popovich, E., Gatti, S., Wang, X. X. X. X. X. X., Lu, Y., Chen, C. C., Yi, X., Cui, H., Mannaa, M., Mansour, A., … Armand, S. (2023). Credit rating downgrades and stock price crash risk: International evidence. Expert Systems with Applications, 64(1), A3. https://doi.org/https://doi.org/10.1016/j.iref.2023.03.027

[21] Ripamonti, A. (2020). Financial institutions, asymmetric information and capital structure adjustments. The Quarterly Review of Economics and Finance, 77, 75–83. https://doi.org/https://doi.org/10.1016/j.qref.2020.01.010

[22] Shahana, T., Lavanya, V., & Bhat, A. R. (2023). State of the art in financial statement fraud detection: A systematic review. Technological Forecasting and Social Change, 192, 122527. https://doi.org/https://doi.org/10.1016/j.techfore.2023.122527

[23] Strauss, A. L., & Corbin, J. M. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. In Management Learning (Vol. 31, Issue 4). Sage Publications, Inc. https://doi.org/10.1177/1350507600314007

[24] Sun, H., Li, J., & Zhu, X. (2023). Financial fraud detection based on the part-of-speech features of textual risk disclosures in financial reports. Procedia Computer Science, 221, 57–64. https://doi.org/https://doi.org/10.1016/j.procs.2023.07.009

[25] Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. Heliyon, 7(4), e06782. https://doi.org/https://doi.org/10.1016/j.heliyon.2021.e06782

[26] Villalba, R., Venus, T. E., & Sauer, J. (2023). The ecosystem approach to agricultural value chain finance: A framework for rural credit. World Development, 164, 106177. https://doi.org/https://doi.org/10.1016/j.worlddev.2022.106177

[27] Wu, B., Chao, K.-M., & Li, Y. (2024). Heterogeneous graph neural networks for fraud detection and explanation in supply chain finance. Information Systems, 121, 102335. https://doi.org/https://doi.org/10.1016/j.is.2023.102335

[28] Zhao, C., Sun, X., Wu, M., & Kang, L. (2024). Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification. Finance Research Letters, 60, 104843. https://doi.org/https://doi.org/10.1016/j.frl.2023.104843