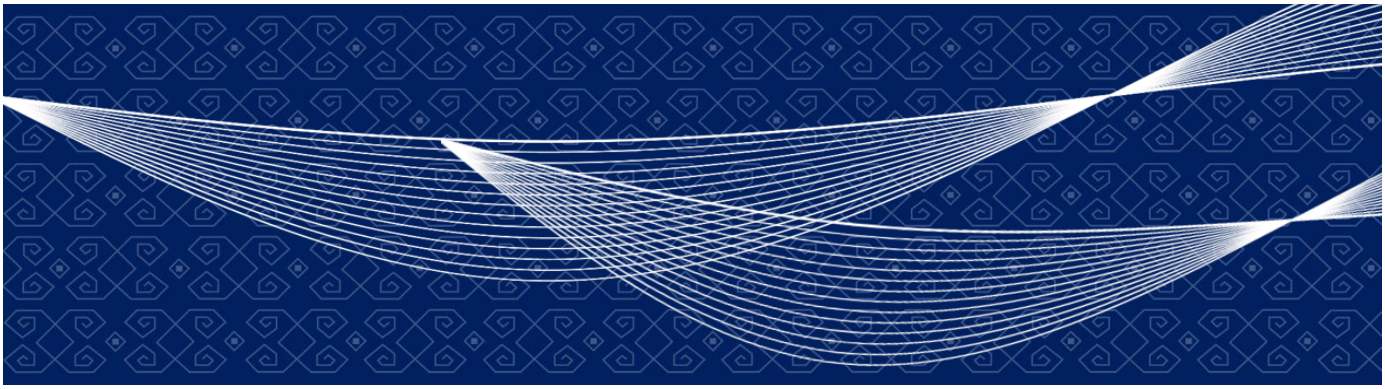
BANK INDONESIA
BANK SENTRAL REPUBLIK INDONESIA



WP/14/2025

WORKING PAPER

IDENTIFICATION OF ILLEGAL TRANSACTION PATTERNS IN PAYMENT SYSTEM DATA USING AI/ML: A CASE STUDY ON ONLINE GAMBLING

Renardi Ardiya Bimantoro, Rudy Hardiyanto, Irfan Sampe, Agung Bayu Purwoko, Imam Dwi Kuncoro, Irvan Fadjar R., Devima Christi M., Anugerah Mohamad Setiawan, Moh. Mashudi Arif, Mahanani Margani, Dwi Kartika Siregar, Ganang Suryo Anggoro, Melati Pramudyastuti, Farah Hilda Fuad Lubis, Rudy Marhastari, Nurkholisoh Ibnu Aman, Sintia Aurida

2025

Identification of Illegal Transaction Patterns in Payment System Data Using AI/ML: A Case Study on Online Gambling

Renardi Ardiya Bimantoro, Rudy Hardiyanto, Irfan Sampe, Agung Bayu Purwoko, Imam Dwi Kuncoro, Irvan Fadjar R, Devima Christi M, Anugerah Mohamad Setiawan, Moh. Mashudi Arif, Mahanani Margani, Dwi Kartika Siregar, Ganang Suryo Anggoro, Melati Pramudyastuti, Farah Hilda Fuad Lubis, Rudy Marhastari, Nurkholisoh Ibnu Aman, Sintia Aurida

Abstract

The transformation of Indonesia's payment system, driven by BSPI initiatives such as SNAP, QRIS, and BI-FAST, has made digital payments faster, more affordable, and more accessible. However, these advancements can also be misused for illegal activities, specifically online gambling. With transactions projected to grow rapidly from Rp327 trillion in 2023 to Rp900 trillion in 2024, this issue has become a major national financial concern. Beyond eroding public trust, this poses serious social and legal risks. Standard monitoring simply cannot keep up with these shifting threats. To address this, this study proposes an AI-driven Fraud Detection System (FDS). By using a hybrid machine learning approach, combining clustering, classification, and GraphML, we can map out criminal networks and how accounts interconnect. The results indicate that the system identified over 90% of syndicate accounts linked to gamblers. It also cut the time required to flag 1,000 fraudulent accounts from a week of manual work down to just 30 minutes, while catching three times the volume of fraud. These insights offer a strong basis for creating adaptive, risk-based policies that reinforce the integrity and resilience of Indonesia's payment ecosystem.

Keywords: AI/Machine Learning, Judi Daring, Sistem Pembayaran, Bank Indonesia, Pengawasan Keuangan, Deteksi Penipuan.

JEL Classification: C55 (Large Data Sets: Modeling and Analysis), G18 (Government Policy and Regulation), K42 (Illegal Behaviour and the Enforcement of Law)

Acknowledgement: The authors would like to express their appreciation to the subject matter experts and the technical team who contributed their insights during the Focus Group Discussions (FGD), which were instrumental in identifying the key features for the Fraud Detection System.

1. Introduction

1.1 Background

Indonesia's payment landscape has undergone a massive transformation recently, leaving traditional cash reliance behind in favor of real-time, interconnected systems. This shift is largely fueled by a regulatory drive for better efficiency and financial access. As noted by Hendrawan et al. (2023), these technological leaps have done more than just upgrade the infrastructure; they have fundamentally reshaped consumer habits, successfully steering the public toward efficient non-cash alternatives.

Bank Indonesia is driving this digitalization through its Indonesia Payment System Blueprint (BSPI) 2025. The blueprint envisions a payment system that supports the national digital economy by being integrated, interoperable, inclusive, and secure. We see these goals in action through specific innovations such as BI-FAST, which drastically lowered the cost of real-time transfers. Similarly, the implementation of the Quick Response Code Indonesian Standard (QRIS) has standardized the market, ensuring that various payment providers can work together without technical barriers.

The data leaves no doubt about the impact. National digital payment transactions grew rapidly, expanding from Rp10.2 trillion in 2022 to Rp70.3 trillion in 2024. QRIS transactions demonstrated even more rapid growth, climbing from Rp27.6 trillion in 2021 to Rp705.2 trillion in 2025, with the BI-FAST processing Rp8,892.8 trillion in 2024 (Bank Indonesia, 2025). However, this rapid digitization presents a double-edged sword. The financial ecosystem is increasingly vulnerable to cybercrime, such as phishing and investment fraud. In fact, the Indonesia Anti-Scam Center (IASC, 2025) received 225,281 reports of fraud resulting in Rp4.6 trillion in losses. Similarly, the PPATK (2025) noted that suspicious transactions tied to fraud nearly quadrupled, rising from 33,376 in 2021 to 132,289 in 2024.

One illegal activity exploiting this ease of transaction is online gambling. These platforms thrive on payment tech that allows for instant, anonymous cross-platform transfers. According to PPATK (2024), online gambling transactions hit Rp327 trillion in 2023 and are projected to reach Rp600 trillion in 2024. Most of this moves through digital channels: bank transfers account for 77%, followed by e-money (10%) and QRIS (3%). In response, the government established a Task Force for the Eradication of Online Gambling (Presidential Decree No. 21/2024) involving multiple ministries. This was followed by the creation of a specific "Desk" for the same purpose under the coordinating minister for Politics and Security (Decree No. 154 of 2024). As part of the prevention working group, Bank Indonesia is tasked with monitoring and evaluating the sector to ensure payment systems remain safe, well-governed, and free from illegal activities.

Payment Service Providers (PJP) and Payment Infrastructure Operators (PIP) are critical chokepoints in the online gambling transaction chain, but their effectiveness depends on tech readiness and strict regulation. Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 mandates that industry players implement effective risk management and secure information systems. Furthermore, PBI No. 23/6/PBI/2021 requires providers to adhere to prudence principles and actively detect and prevent illegal acts.

To meet these risk management standards, regulations require a fraud management system capable of detecting anomalies at the account, network, and transaction levels. Additionally, PBI No. 10 of 2024 regarding Anti-Money Laundering (AML) mandates strict Customer Due Diligence (CDD) to ensure compliance.

The problem is that traditional "rule-based" fraud detection systems struggle to keep up with the scale and complexity of modern digital transactions. This is where AI and Machine Learning (AI/ML) become essential. Developing an AI-driven Fraud Detection System (FDS) allows for not just detection, but the prediction of accounts likely to be used as shelters for illegal funds (mule accounts). Consequently, Bank Indonesia has initiated the development of FDS algorithms designed to proactively spot these risks.

The goal is for this FDS framework to serve as a reference for both regulators and the industry. It aims to identify accounts linked to gambling while still giving service providers the flexibility to develop their own models. Once identified, these accounts can be subjected to due diligence or enforcement actions. Ultimately, an AI/ML-based FDS should make the fight against online gambling more proactive, efficient, and measurable.

1.2 Research Question

Given the background outlined above, this study addresses the following research questions:

1. What are the specific characteristics of online gambling accounts and transaction patterns in Indonesia, particularly regarding their demographic and spatial distribution?
2. How can AI/ML methodologies be leveraged to analyze illegal transaction patterns, specifically online gambling, using data from the Bank Indonesia Payment System (SPBI)?

1.3 Research Purpose

Guided by the research questions above, the objectives of this study are:

1. To understand the characteristics of online gambling accounts, which will serve as a key input for selecting variables and features during AI/ML model development.
2. To build AI/ML models capable of identifying accounts or transactions linked to online gambling, utilizing data from the Bank Indonesia Payment System (SPBI).
3. To evaluate the models to determine which yields the highest accuracy, while also pinpointing the most significant variables and features.

2. Literature Review

2.1. Online Gambling: Triggers & Risks

The rapid evolution of digital technology has significantly lowered the barriers to online gambling in Indonesia. With 4G network coverage reaching 96.5% of the population in 2022 (Global SDG) and internet penetration hitting 69.2% in 2023 (World Bank), betting platforms are now instantly accessible, anytime and anywhere, on portable devices like smartphones (Fahrudin et al., 2024). This sheer accessibility has directly driven up public participation; research by McCormack et al. (2013) and Zhang et al. (2018) indicates that the ease of access to a wide variety of online games is a primary factor driving individuals toward online gambling. The COVID-19 pandemic acted as a further catalyst. Social restrictions and lockdown policies forced people to seek entertainment online, with a ripple effect that increased engagement in digital gambling (Håkansson, 2020). During difficult economic times, some individuals turned to online gambling for amusement or as a temporary source of income (Dwihayuni & Fauzi, 2021). Moreover, psychological struggles such as depression and anxiety often lead individuals to use gambling as a coping

mechanism, which ultimately cements the cycle of addiction (Gainsbury et al., 2015; Törrönen et al., 2020).

While the specific reasons people engage in online gambling vary, the drive to secure substantial financial gains remains the primary motivation (Athallah et al., 2024). That study found that among 3,320 participants, 36% played with the intent of winning large sums of money, 18% to escape personal problems, 18% for entertainment, and 28% for other reasons. Alarmingly, 72% of the respondents were reported to have already exhibited signs of gambling addiction.

The fallout from online gambling addiction in Indonesia encompasses severe financial distress, such as mounting debt and job loss, alongside social consequences like strained family relationships and the emergence of criminal behaviour (Elie, 2023; Winarsih & Salsabila, 2022). This reality shows that online gambling is not merely a technological or economic phenomenon; it is a complex, multidimensional social issue that demands a cross-sector approach for effective prevention and rehabilitation.

2.2. National-Level Response to Online Gambling

The Government of Indonesia has established a dedicated task force to combat online gambling activities. Through Presidential Decree No. 21 of 2024 on the Task Force for the Eradication of Online Gambling (*Satuan Tugas Pemberantasan Perjudian Daring*), the Online Gambling Task Force is mandated to carry out several key responsibilities, including:

a. Optimizing the prevention and enforcement of online gambling in an effective and efficient manner;
b. Enhancing coordination among ministries and government institutions, as well as with international counterparts, in efforts to prevent and enforce laws against online gambling; and
c. Aligning and implementing strategic policies and formulating recommendations to strengthen the prevention and law enforcement of online gambling activities.

Various measures have been undertaken by ministries and agencies within the Task Force framework to address online gambling. During the period from January to July 2025, the Ministry of Communication and Digital Affairs (Komdigi) conducted enforcement actions and/or blocked approximately 1.2 million online gambling-related contents. This figure represents a decline compared to 2024, when approximately 3.8 million online gambling-related contents were blocked. In addition, the Financial Services Authority (OJK) has frozen 17,024 accounts identified as being associated with online gambling activities. These account freeze actions were carried out based on official requests from relevant ministries, particularly Komdigi.

Bank Indonesia's involvement in the Preemptive Working Group includes initiatives such as public outreach programs aimed at enhancing financial literacy and raising awareness of the risks and negative impacts associated with online gambling. On the preventive front, Bank Indonesia has also implemented several initiatives targeting Payment Service Providers (PSPs) that are potentially vulnerable to misuse in facilitating online gambling transactions. These initiatives include:

a. Strengthening the application of the prudential principle for PSPs engaging in partnerships with third parties;
b. Enhancing Fraud Detection Systems (FDS) and strengthening monitoring procedures for FDS implementation by PSPs; and

c. Conducting verification of user data, information, and/or transaction documents suspected of being linked to online gambling activities, including the termination of business relationships where necessary.

In addition to encouraging PSPs to implement preventive measures to mitigate online gambling transactions, Bank Indonesia has also undertaken initiatives such as cyber patrols targeting websites associated with online gambling activities. The results of these cyber patrols are subsequently reported to relevant ministries for blocking actions. Furthermore, payment instruments and channels used in online gambling transactions are communicated to PSPs for verification and account closure processes. As the payment system authority, Bank Indonesia has also updated the fraud detection system embedded within its payment system infrastructure by incorporating rule-based parameters to strengthen the integrity of payment services. In parallel, supervisory tools have been reinforced through the implementation of market intelligence and money mule detection mechanisms.

2.3. Fraud Detection Techniques and Parameters

As the dynamics of transactions in the digital financial economy grow more complex, conventional fraud detection methods are beginning to shown their limitations, specifically, their rigidity and the ease with which perpetrators can bypass them. The nature of fraud emerging within this digital ecosystem demands a more responsive and adaptive strategy. Consequently, this sub-chapter provides a detailed comparison between traditional, rule-based fraud detection and systems that leverage machine learning to identify fraudulent activity.

2.3.1 Traditional Method and Parameters of Fraud Detection

In practice, the landscape of fraud detection within many institutions remains heavily reliant on legacy methodologies. These typically center on rule-based systems and manual reviews, approaches that are inherently reactive and struggle to adapt to emerging modus operandi (Bagwe, 2024). Sudjianto et al. (2010) highlight that these traditional frameworks face significant structural limitations, including class imbalance, data drift, and difficulties in accurately verifying fraud labels. Furthermore, rule-based systems are often rigid and prone to bias, particularly when fraudulent tactics evolve at a pace that outstrips the static rules governing the system.

Despite these shortcomings, previous research has established a robust set of transaction parameters that function as effective fraud predictors. These parameters provide the essential groundwork for developing AI and Machine Learning-based Fraud Detection Systems (FDS). Broadly speaking, they can be categorized into:

- Transaction value and volume, such as transaction amount, daily spending amount, overdrafts, and amount/transaction limits (Panigrahi et al., 2009; Bolton & Hand, 2001);
- Frequency and intensity, including card frequency, hourly transaction counts, and the time gap between transactions (Agrawal et al., 2015; Bahnsen et al., 2015);
- Time dimensions, such as specific card usage times or transactions occurring during particular hours (Bahnsen et al., 2015; Renuga et al., 2014); and
- Location and channel, covering the country of origin, merchant location, channel type (ATM, online, POS), and the distance between the IP location and the billing address (Sánchez et al., 2009; Oracle FSS, 2014).

2.3.2 AI/ML Aprroaches for Fraud Detection

Various machine learning-based fraud detection techniques have been applied to enhance model accuracy, specifically by reducing the false positive rate in fraud detection. Table 1 illustrates the evolution of methodologies used for detecting fraudulent transactions over the years.

Table 1. Methodology/technique used for detecting online transaction fraud

No.	Methodology/technique	Authors (Year)
1	Line-Graph-Assisted Multi-View Graph Neural Networks	Poon et al. (2025)
2	Graph Neural Networks	Cheng et al. (2024)
3	Machine learning in Financial Fraud Detection	Rafi et al. (2024)
4	Deep Neural Networks	Konstantinidis, G. and Gegov, A. (2024)
5	Distributed tree-based model	Vorobyev and Krivitskaya (2022)
6	Hidden Markov model and genetic algorithm	Agrawal et al. (2015)
7	Semi-hidden Markov model	Prakash and Chandrasekar (2015)
8	Fuzzy clustering and neural network	Behera and Panigrahi (2015)
9	Neural network committee and clustering	Bekirev et al. (2015)
10	Artificial neural network	Carneiro et al. (2015)
11	Big data	Chen et al. (2015)
12	Naive Bayesian approach	Singh and Singh (2015)
13	Artificial neural network tuned by simulated annealing algorithm	Khan et al. (2014)
14	Genetic programming	Assis et al. (2014)
15	Naive Bayesian approach and random forest	Renuga et al. (2014)
16	Migrating bird's optimization	Duman et al. (2013)
17	Hidden Markov model	Prakash et al. (2012)
18	Artificial immune systems	Soltani et al. (2012)
19	Genetic algorithm and scatter search	Duman et al. (2011)
20	Association rule mining	Sanchez et al. (2009)

The various literature cited in Table 1 indicates that AI/ML is capable of delivering superior performance in fraud detection compared to rule-based methods. For instance, Rafi et al. (2024) compared rule-based methods with several ML models (Random Forest, Gradient Boosting, and Neural Networks) across more than one million financial transactions and found that these models were able to reduce false positives by approximately 30% while simultaneously increasing efficiency in fraud detection compared to traditional methods.

Furthermore, Vorobyev and Krivitskaya (2022) reported that their best model, Gradient Boosting, achieved a ROC-AUC score of 0.992 on training data and 0.547 on testing data, along with a recall of approximately 0.806 and a precision of 0.162. These values indicate that AI/ML is capable of effectively learning fraud patterns. However, the literature generally still utilizes a single specific algorithmic approach (single-model approach) and focuses on the individual transaction level, resulting in limitations in capturing criminal patterns or behaviours involving interconnections between accounts or those possessing dynamic modi operandi. To address this gap, this study employs a hybrid AI/ML approach by combining unsupervised learning,

supervised learning, and graph-based learning to analyze transactions as well as the account network structure. Through this approach, it is hoped that a more comprehensive identification of online gambling activities can be achieved, while still utilizing previous literature as the foundation for the methodological development in this study.

3. Methodology

This study employs an approach that combines qualitative and quantitative methods to obtain a comprehensive understanding of the characteristics, patterns, and detection potential of online gambling activities in Indonesia. The approach consists of three main stages: Focus Group Discussion (FGD), Descriptive Analysis, and an Artificial Intelligence/Machine Learning (AI/ML) approach.

3.1. Data

This study utilizes a transaction dataset spanning 4 months, from June 2024 to October 2024. This period was selected based on prior analysis indicating that it represents the highest transaction volume in the available fraud data. The entities included in the data are the sender (source node), recipient (target node), as a ground to build unsupervised and supervised model (incl. graph machine learning). In general, the dataset in this study is divided into two main categories: accounts associated with online gambling activities (fraud accounts) and unassociated accounts (non-fraud accounts). The associated accounts were collected based on scraping results, while the non-fraud accounts serve as a comparison to test the model's capability in distinguishing between normal and illegal transactions.

Table 2. Comparison of Fraud and Non-Fraud Data Proportions

Account Type	Number	Proportion
Fraud Accounts	+- 1600	$\frac{1}{45.625}$
Non-Fraud Accounts	+- 73 millions	

Given the significant imbalance between fraud and non-fraud accounts, this study adopts a staged modeling strategy to mitigate class imbalance, where data reduction and prioritization are applied before supervised learning. The technical details of the imbalance handling mechanisms are discussed in Section 3.4.

3.2. Focus Group Discussion (FGD)

The first stage was conducted through Focus Group Discussions (FGDs) involving relevant industries and institutions to understand the patterns and modus operandi of online gambling activities in Indonesia. The FGDs aimed to obtain empirical perspectives on the challenges and transaction mechanisms used in these illegal activities. The discussion outcomes were subsequently validated against empirical data and relevant literature to ensure alignment between field findings and the existing theoretical context.

In practice, two FGDs were conducted. The first was held with Payment Service Providers (PSPs) and ASPI on 15 July 2025, followed by a subsequent FGD with government institutions (OJK and Komdigi) on 1 August 2025.

3.3. Descriptive Analysis

The second stage involved descriptive analysis of the characteristics of online gambling transactions based on the available data. This analysis was conducted to

identify patterns, trends, and key characteristics emerging from transactions related to online gambling. The results of the analysis were used to support the feature engineering process in the development of the detection model. By understanding transaction behaviour patterns, key indicators that can potentially be used to more accurately detect illegal activities can be identified.

Table 3. Illustration of Descriptive Analysis Process

Analysis Aspect	Descriptive Question	Key Indicator
Time	When are fraudsters most active?	Dominant activity between 01:00–04:00 a.m.
Nominal Value	What is the range of transaction values?	Average transaction value
Frequency	How frequently does a fraudster conduct transactions?	Total number of transactions within one month
Behaviour	What is the interaction pattern of online gambling transactions?	Multiple different senders to a single account
Demographics	What is the demographic distribution of gambling collection accounts?	Locations with the highest amount transaction values

3.4. AI/ML Approach

The third stage is an AI/ML approach to build a model to learn transaction patterns of illegal activities, specifically online gambling. The three approaches used are as follows:

3.4.1 Unsupervised Learning

As shown on Table 2, the data imbalance exists, potentially causing the model to predict all accounts as non-fraud, which results in a low recall rate and a failure to detect patterns within the minority data (fraud accounts). One method to address this is simple random sampling, which reduces the volume of non-fraud data by randomly selecting a small subset of samples to balance the proportion with the fraud data; however, while this approach is fast and simple, it often discards significant information from the majority class, potentially compromising the model's ability to distinguish between normal and fraudulent transactions. Therefore, we use the K-Nearest Neighbor (KNN) algorithm to cluster transaction data based on pattern similarity before we perform simple random sampling. The fundamental principle is to group based on nearest neighbors, relies on the calculation of the distance between transaction data feature vectors x and y, then we take sample of each cluster to represent the characteristics of each cluster for the training dataset. The most commonly used metric for the distance calculation is Euclidean Distance:

$$(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

Where:

- $d(x, y)$ is the distance between two transaction data points.
- x_i dan y_i are the values of the i^{th} feature of each respective data point.
- n is the total number of features (dimensions)

3.4.2 Supervised Learning

This study employs supervised learning to classify transactions using labeled historical examples. To address the challenges of complex and imbalanced fraud datasets, the Gradient Boosting algorithm is used. Described by Alothman et al. (2022), this ensemble technique enhances model robustness by sequentially aggregating weak learners. iteration introduces a new learner ($h_m(x)$) specifically weighted (γ_m) to correct the residuals of the previous prediction ($F_{m-1}(x)$), represented by the equation:

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x)$$

The methodology further enriched by adding GraphSAGE (Graph Sample and Aggregate) into accounts. Unlike traditional graph embedding methods that rely on matrix factorization and require the entire graph to be present during training (transductive learning), GraphSAGE is an inductive framework. As proposed by Hamilton et al. (2017), GraphSAGE learns aggregator functions that can generate embeddings for unseen nodes by sampling and aggregating features from a node's local neighborhood. This capability is critical for fraud detection, where new accounts (nodes) are constantly added to the transaction network.

The embedding generation process involves two main steps: aggregating information from neighbors and updating the node's current state. For a specific node v, the embedding at depth k is calculated using the following operations:

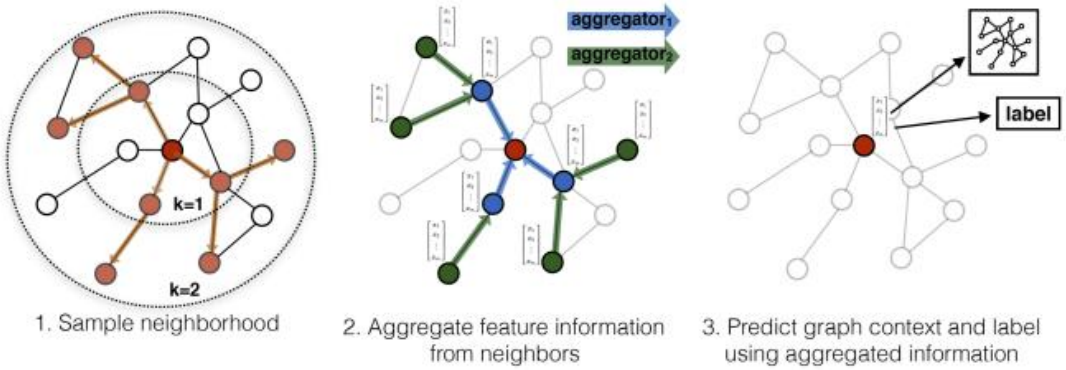


Figure 1. Visual illustration of the Graph Sample and Aggregate (GraphSAGE) approach (Hamilton et al., 2017).

a. Neighborhood Aggregation: The model aggregates the feature vectors from the sampled neighborhood $\mathcal{N}(v)$:

$$\mathbf{h}_{\mathcal{N}(v)}^{k} \leftarrow \text{AGGREGATE}_k\left(\{\mathbf{h}_u^{k-1}, \forall u \in \mathcal{N}(v)\}\right)$$

b. Update Step: The aggregated neighborhood vector is concatenated with the node's current representation and passed through a fully connected layer with a non-linear activation function σ:

$$\mathbf{h}_v^k \leftarrow \sigma\left(\mathbf{W}^k \cdot \text{CONCAT}\left(\mathbf{h}_v^{k-1}, \mathbf{h}_{\mathcal{N}(v)}^k\right)\right)$$

Where:

$\mathbf{h}_v^k$ is the embedding vector of node v at layer k.

$\mathcal{N}(v)$ represents the sampled neighbors of node v.

AGGREGATE_k is a differentiable aggregator function (e.g., Mean, LSTM, or Pooling).

$\mathbf{W}^k$ is the weight matrix learned during training.

σ is a non-linear activation function (e.g., ReLU).

4. Results / Analysis

4.1. Characteristics of Online Gambling

Based on the results of the Focus Group Discussions (FGDs) with industry stakeholders and relevant institutions, key insights were obtained regarding the main characteristics of online gambling activities in Indonesia. These insights encompass the demographic profile of participants, patterns of distribution and modus operandi, as well as the payment system ecosystem utilized in online gambling practices.

4.1.1 Demographic Profile of Online Gambling Players

Online gambling activities in Indonesia have attracted millions of participants from diverse demographic backgrounds. Recent data indicate an alarming trend, showing that throughout 2023 approximately 3.8 million Indonesians were detected as being involved in online gambling activities. By mid-2024, the number of online gambling players was estimated to have increased to around 4 million. Based on data from the Online Gambling Task Force, the distribution of participants spans various age groups, including children under the age of 10 (2%) and adolescents aged 10–20 years (11%), while the productive age group of 30–50 years dominates with the highest proportion at 40%.

In terms of gender, online gambling participants are predominantly male. Data from the Financial Transaction Reports and Analysis Center (PPATK) recorded that in 2023 there were approximately 3.2 million male participants and 500,000 female participants involved in online gambling. In other words, around 86% of players are male, while females account for approximately 14%. This indicates that online gambling is relatively more prevalent among men, although female participation remains non-negligible.

The majority of players, approximately 80%, originate from low-income groups, reflecting a correlation between economic instability and the tendency to seek instant income through gambling. These findings further reinforce indications of weak digital supervision and limited financial literacy within the community.

The socio-economic background of online gamblers is generally concentrated within the lower-middle class. PPATK reports that 80% of online gambling players come from low-income communities. They tend to place small bets, with typical deposit amounts ranging from IDR 10,000 to IDR 100,000 per transaction. Meanwhile, approximately 20% of players belong to the upper-middle class, with betting transactions reaching hundreds of millions to billions of rupiah. Online gambling participants are found across a wide range of occupations, including students, housewives, private-sector employees, laborers, farmers, and the unemployed. This indicates that the appeal of online gambling transcends occupational and economic boundaries.

Geographically, the distribution of online gambling participants spans nearly all provinces in Indonesia. However, data indicate higher concentrations in densely populated provinces and urban regions. Based on data from the Online Gambling Eradication Task Force (sources: PPATK and the Coordinating Ministry for Political, Legal, and Security Affairs), five provinces record the highest number of online gambling players:

1. West Java: Approximately 535,644 players, with transaction values of around IDR 3.8 trillion. West Java ranks first nationally, supported by factors such as the largest population in Indonesia, widespread internet access, and high urbanization in cities such as Bandung and Bekasi. These conditions create a large internet user base, while regulatory oversight remains limited.

2. DKI Jakarta: Approximately 238,568 players, with transaction values of around IDR 2.3 trillion. As the capital city with advanced internet infrastructure and relatively strong economic conditions, Jakarta represents the second-largest hub. High internet penetration and widespread gambling promotions (e.g., banners and illegal advertisements) in urban areas contribute significantly to this trend.
3. Central Java: Approximately 201,963 players, with transaction values of around IDR 1.3 trillion. Central Java, including major cities such as Semarang and Surakarta, benefits from a large population and increasingly widespread internet access.
4. Banten: Approximately 150,302 players, with transaction values of around IDR 1.02 trillion. Urban areas within the Greater Tangerang region contribute significantly, alongside a substantial population of internet-literate youth who are particularly vulnerable to online gambling advertisements.
5. Jawa Timur: Approximately 135,227 players, with transaction values of around IDR 1.05 trillion. The high prevalence of online gambling in this province is influenced by its large population (including cities such as Surabaya and Malang) and extensive internet access. In addition, pre-existing cultural practices related to conventional gambling have partially migrated to online platforms.

These data indicate that the top five provinces with the highest number of online gambling participants are all located on Java Island, reflecting high population density and extensive internet access in this region. Nevertheless, other provinces are not immune to online gambling exposure. Based on the analysis of gambling distribution across Indonesia, Java Island dominates with 53.52% of total participants, followed by Sumatra (26.89%), Kalimantan (9.46%), Bali–Nusa Tenggara (3.96%), Sulawesi (3.77%), and the Maluku & Papua regions (2.41%). Provinces with smaller populations are not entirely free from exposure; however, several newly established provinces in Papua (e.g., Highland Papua, South Papua) report nearly zero cases, primarily due to limited internet access. With large populations and continuously increasing internet penetration, urban and densely populated areas have become primary targets for online gambling operators in recruiting new players.

4.1.2 Factual Conditions: Distribution and Modus Operandi

The Ministry of Communication and Informatics (Kominfo) reported that from 2018 to mid-2024, access to more than 2.6 million online gambling-related contents had been blocked. These contents include websites, social media pages, and applications identified as offering online gambling services.

From a geographical distribution perspective, online gambling activities are present in nearly all provinces across Indonesia. At a more granular level, the Financial Transaction Reports and Analysis Center (PPATK) identified the Greater Jakarta metropolitan area (Jakarta and surrounding regions) as the largest hub for online gambling fund circulation. Several cities and regencies recorded the highest transaction values, including West Jakarta (IDR 792 billion), Bogor City (IDR 612 billion), Bogor Regency (IDR 567 billion), East Jakarta (IDR 480 billion), and North Jakarta (IDR 430 billion). At the sub-district level, South Bogor District recorded 3,720 participants with transaction values amounting to IDR 349 billion, while Tambora District (Jakarta) recorded 7,916 participants with transaction values of IDR 196 billion. These granular data indicate that online gambling networks penetrate down to the local level, particularly in densely populated areas.

The modus operandi employed by online gambling operators and syndicates are highly diverse and continuously evolving, as follows:

a. Social Media and Digital Advertising

Online gambling operators promote their services through advertisements on social media platforms, video-sharing platforms, and even by infiltrating legitimate websites. Kominfo has reported the widespread presence of online gambling advertisements on platforms such as YouTube and Facebook, which are often designed to resemble ordinary content advertisements. In some cases, phishing techniques are used to deceive users into clicking gambling-related links or advertisements. In response, the government has coordinated with platform providers such as Google, YouTube, and Meta (Facebook/Instagram) to block keywords associated with online gambling. As of July 2024, Kominfo had submitted 20,595 keywords to Google and approximately 3,961 keywords to Meta for filtering and enforcement. Conversely, online gambling operators continue to exploit loopholes by frequently changing website or account names, using coded language, or collaborating with influencers and social media personalities to covertly promote gambling links.

b. Infiltration of Legitimate Websites

Another modus operandi involves embedding online gambling pages within official government or educational websites that are vulnerable to exploitation. Kominfo identified tens of thousands of concealed gambling pages, with records showing that by July 2024, approximately 23,616 gambling pages had been embedded within government websites and 22,205 pages within educational institution websites. Online gambling operators exploit high-authority domains such as *gov* and *ac.id* by hacking into these sites and embedding gambling links, making them difficult to distinguish and allowing them to evade blocking due to the use of legitimate domains. This reflects an evolution in gambling operators' strategies from previously hosting standalone websites to now piggybacking on popular and trusted platforms to enhance reach and credibility.

c. Bonus-Based Deceptive Schemes

In terms of player recruitment, online gambling operators frequently offer registration bonuses, free credits, or instant winnings to attract new users. These "bait" strategies exploit players' expectations of quick profits and serve as a mechanism to foster gambling addiction. Operators leverage psychological manipulation by providing easy rewards at the initial stage, ultimately trapping players in a cycle of continued participation in pursuit of illusory gains.

d. Domain and Application Switching

To evade blocking measures, online gambling operators rapidly change their website domains. Once a domain is blocked by Kominfo, operators reappear using new domain addresses or mirror sites. In addition, many operators distribute illegal mobile applications or APK files outside official app stores. These applications are often disguised as ordinary games or unrelated applications, allowing them to bypass moderation processes. Players are also frequently encouraged to use VPN services to access blocked gambling sites. These tactics significantly complicate law enforcement efforts, as operators continuously re-emerge with new digital identities after each enforcement action.

e. Mule Accounts and Borrowed Identities

Financial transaction operations in online gambling commonly involve the use of bank accounts or e-wallets owned by third parties, commonly referred to as mule accounts. PPATK reports that operators frequently exploit accounts registered under the names of students or low-income individuals as fund collection accounts. Such accounts are perceived as less suspicious due to their typically small transaction volumes. Additionally, the illicit trade of bank accounts and national identity cards (ID cards) in underground markets has been identified, enabling gambling syndicates to use legitimate banking or e-wallet accounts while obscuring the identities of the actual operators.

f. Collaboration with Illegal Online Lending Platforms

Another modus operandi reported by the Financial Services Authority (OJK) is the similarity between online gambling operations and illegal online lending platforms (*pinjaman online ilegal*). Both operate through mobile applications, and there are indications that some illegal lending platforms are used as channels to finance online gambling activities. For example, players borrowing from illegal lenders to gamble, or lending platforms being used as a façade for gambling-related transactions. This overlap further complicates enforcement efforts, as online gambling networks intersect with other forms of cybercrime.

g. Money Laundering Practices

PPATK has identified money laundering patterns involving the use of money changers and fictitious export–import transactions to disguise proceeds from online gambling. Under this scheme, gambling proceeds are converted through money changers to appear as legitimate business transactions or transferred abroad via fictitious export–import companies under the guise of trade payments. As a result, gambling proceeds appear as legitimate cross-border transactions and evade conventional monitoring mechanisms. Additionally, operators have been found to store funds in crypto-assets or move money outside the formal banking system to avoid detection. Collectively, these laundering practices demonstrate that online gambling activities are conducted in a highly organized and systematic manner.

4.1.3 Online Gambling Ecosystem within the Payment System

Online gambling transactions generally involve the deposit of funds by players into online gambling accounts, the circulation of bets within the platform, and the withdrawal of funds by winners or gambling participants. To deposit funds, players are offered several payment method options, such as transfers to designated bank accounts, electronic money (e-money) accounts, or payments through third-party agents. The deposit and withdrawal stages are the phases most closely associated with the payment system. The transaction patterns commonly observed in online gambling payments are described as follows:

a. Bank Accounts and Fund Transfers

Many online gambling websites utilize local bank accounts as repositories for player deposits. Online gambling operators typically control hundreds of bank accounts across multiple banks, registered under different names, to receive player transfers. Once funds are received, the amounts are converted into balances within players' gambling accounts. Transfer patterns are often deliberately structured into small and fragmented amounts to avoid suspicion. On the operators' side, fund circulation occurs rapidly, with funds from collection accounts being quickly transferred to other accounts (layering) to obscure transaction trails. PPATK reported that by 2023, approximately 5,000 bank accounts suspected of being linked to online

gambling had been blocked. Similarly, as of August 2024, the Financial Services Authority (OJK) had instructed banks to freeze more than 6,000 accounts associated with online gambling. These figures indicate that thousands of bank accounts within the banking system have been misused as channels for online gambling transactions.

b. Electronic Money (E-Money)

The growth of financial technology has also been exploited by online gambling operators to facilitate transactions, including deposits for gambling activities and withdrawals of gambling proceeds to electronic money accounts. Data from the Financial Transaction Reports and Analysis Center (PPATK) indicate that several electronic money providers have been misused to facilitate online gambling transactions, with total values ranging from billions to trillions of rupiah. The data suggest that a small number of large platforms account for a substantial share of the detected transaction value and frequency.

The high transaction volume associated with certain platforms indicates that widely adopted electronic money services can be attractive channels for illicit actors due to their broad user base and transaction convenience. In some cases, electronic money accounts can be created with relatively minimal verification requirements, typically requiring only a mobile phone number and a username for basic registration. Online gambling operators frequently exploit such mechanisms by using false or borrowed identities to create multiple accounts.

Funds generated from online gambling activities are typically moved out of collection accounts as quickly as possible. Money laundering is conducted through various mechanisms, including money changers, fictitious export–import transactions, and online lending platforms. Common schemes include transferring funds from domestic accounts to overseas accounts registered under fictitious companies, or converting funds into foreign currency before transferring them abroad under the guise of "trade payments." These international transactions exploit regulatory gaps across jurisdictions. In addition, money laundering through online lending platforms has also been observed, whereby gambling operators obtain large online loans and repay installments using proceeds derived from online gambling activities.

The widespread proliferation of online gambling represents a leakage of funds from the productive economy into the illegal sector. Large amounts of financial resources flow into the hands of gambling operators, many of whom operate from overseas jurisdictions, resulting in minimal domestic economic benefit from the circulation of these funds. Moreover, funds used for online gambling often originate from loans or the diversion of productive assets, leading to significant negative multiplier effects, particularly when players incur financial losses.

Based on the above discussion, it is evident that online gambling transaction patterns are closely intertwined with Indonesia's payment system infrastructure, including both the banking system and digital payment systems (such as electronic money and QRIS), which may be vulnerable to misuse as channels for financing illegal gambling activities. Therefore, the role of payment system regulators is crucial in disrupting the financial supply chain that sustains these illicit activities while ensuring that legitimate payment service providers continue to operate within a robust regulatory and supervisory framework.

4.2. Descriptive Analysis

4.2.1. Distribution and Profile of Hub Accounts

Based on the web scraping results on April 29, 2025, a total of around 1,600 accounts were confirmed as being online gambling hub accounts, with potentially involving more than 56,000 player. The geographical distribution indicates that the largest concentration of these collection accounts is located in DKI Jakarta, West Java, and North Sumatra. These findings suggest that online gambling activities are predominantly concentrated in regions with high internet penetration and dense economic activity. This result is also consistent with the findings of the Focus Group Discussions (FGDs), which confirmed that Java Island represents the region with the highest concentration of online gambling participants, driven by high population density and broader internet access compared to other regions.

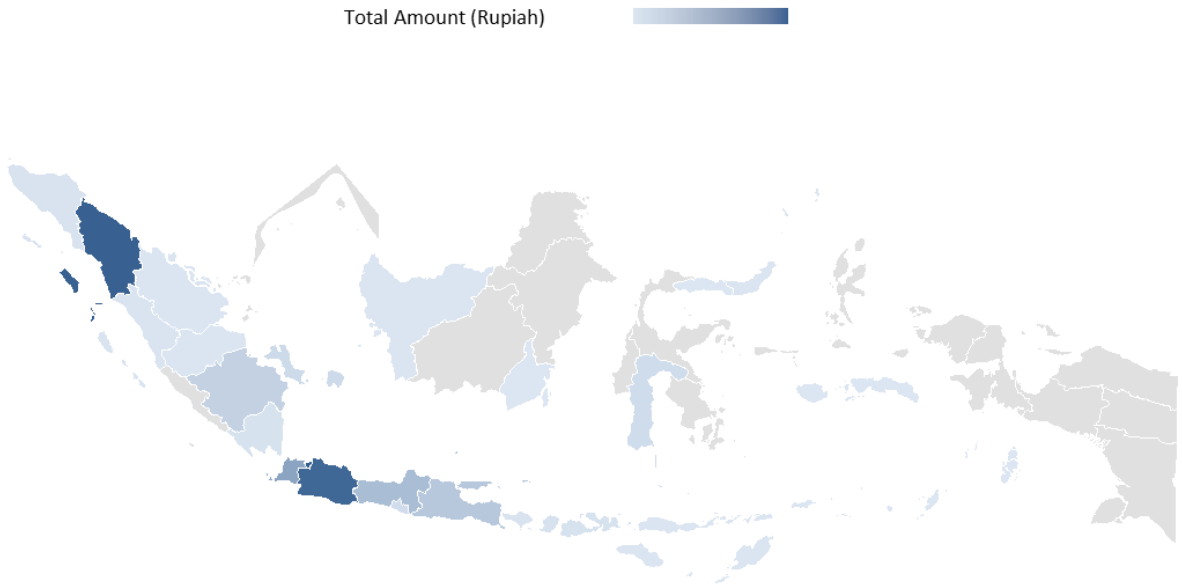


Figure 2. Geographic Distribution of Online Gambling Hub Account Domiciles

In addition, demographic analysis reveals that the majority of collection accounts belong to younger age groups, particularly Generation Z (aged 15–28 years), followed by Generation Y. These findings further corroborate the FGD results, which indicated that, in practice, gambling operators frequently exploit accounts owned by students or low-income individuals, who are generally within the productive age group, as hub accounts for online gambling transactions.

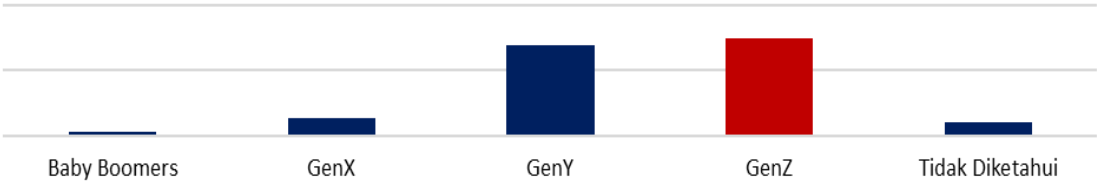


Figure 3. Age Group Distribution of Online Gambling Hub Accounts

4.2.2. Transaction Patterns and Intensity

Based on the analysis results, transaction patterns between accounts identified as online gambling hub accounts (fraud accounts) and non-fraud accounts exhibit substantial differences. These differences are particularly evident in transaction timing. Accounts identified as hub accounts tend to be significantly more active

during the early morning hours, whereas transactions in non-fraud accounts predominantly occur during regular daytime business hours.

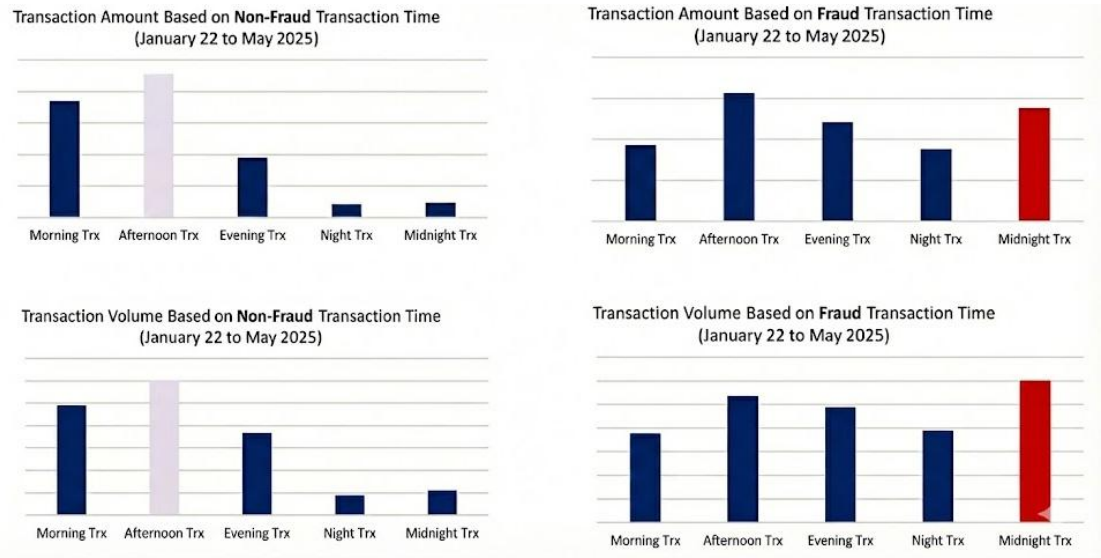


Figure 4. Distribution of Transaction Values and Volumes by Transaction Time

This pattern indicates that online gambling activities are largely conducted outside normal banking operational hours and reflect repetitive transaction behaviours that are temporally anomalous and inconsistent with typical consumer or business activity.

Furthermore, analysis of monthly transaction values and volumes reveals marked disparities between the two account groups. Online gambling hub accounts record an average monthly inbound transaction value that are higher than the baseline figures observed in normal accounts. This gap is even more obvious at night, while regular transaction values drop to a trickle, these hubs continue processing significant sums, even matching their afternoon transaction levels.

4.2.3. *Feature Engineering*

Based on the results of Focus Group Discussions (FGD), literature reviews, and descriptive analysis, several variables have been identified as key features for the development of the AI/ML-based Fraud Detection System (FDS) model. For instance, aggregate transaction & demographical feature (vol_trx, indegree, snd_avg_age), time-based feature (amt_late_night, trx_weekend, sndr_late_night), and basic statistical feature (avg_amt, med_amt, std_amt). These variables were selected due to their ability to represent the transaction behaviours most relevant to online gambling activities.

4.3. AI/ML Approach For Fraud Detection

4.3.1. Account Clustering

The unsupervised learning approach was implemented using the K-Nearest Neighbor (KNN) algorithm to identify accounts with similar transaction patterns based on their behavioural characteristics. Based on Figure 5, the decrease in WSSE values indicates an optimal point at four clusters, where adding subsequent clusters does not yield a significant reduction in error. Consequently, the formation of four groups is considered the most efficient for capturing variations in transaction behaviour without increasing model complexity.

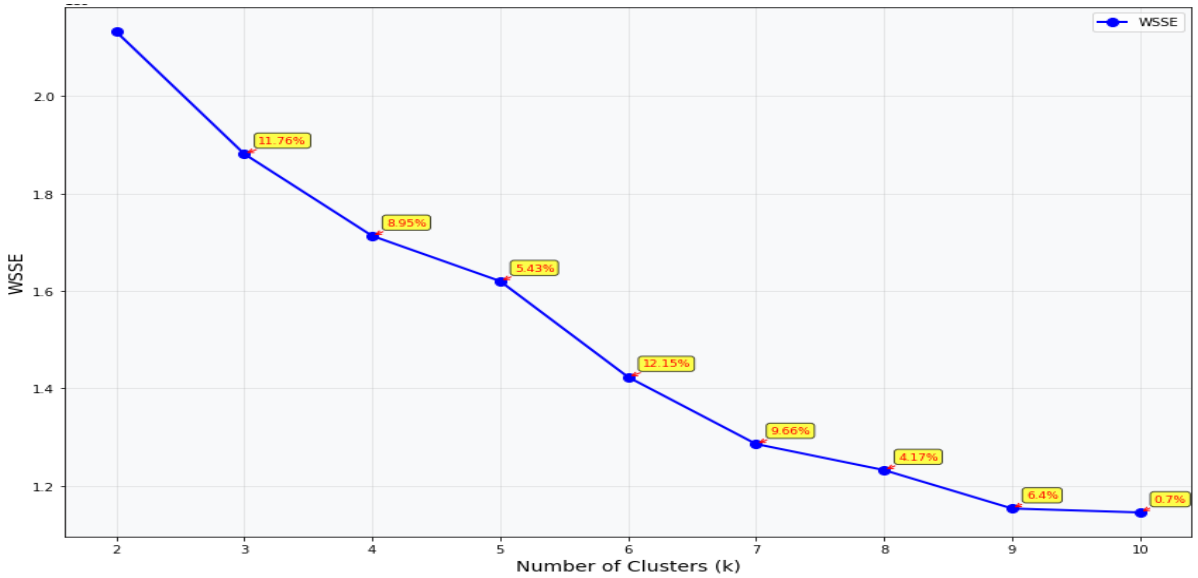


Figure 5. Weighted Sum of Squared Error (WSSE) vs. Number of Clusters

The resulting four clusters from the KNN analysis possess the following distinct characteristics:

a. Cluster 0: Personal accounts with low transaction volume and normal activity.
b. Cluster 1: Accounts with large transaction values but low frequency, likely representing business entities.
c. Cluster 2: Accounts with high transaction values and frequency, as well as dense interconnectivity, indicating potential as hub accounts or business entities playing a role in online gambling networks.
d. Cluster 3: Accounts with very high transaction values and frequency, likely representing Payment Service Provider (PSP) book-transfer intermediary entities.

Of the four groups, Cluster 2 exhibits behaviour most consistent with the characteristics of pooling accounts. Accounts in this cluster have a high number of senders (up to more than 488 accounts), as well as significantly increased activity during late night hours. This pattern signals transactions occurring outside normal operational hours and is potentially linked to illegal activities.

Once the account behaviour profiles were mapped into four clusters, the next step involved data resampling to construct a training set for the development of the supervised learning model. Given the data population reaches 73 million accounts, this resampling strategy was executed systematically through the following approach:

a. Conducting random sampling on the cluster with the largest population to balance the data distribution. This ensures the dataset size becomes more balanced without eliminating the variations in customer behaviour identified by the clustering algorithm.
b. Ensuring that each cluster contributes a representative sample to the model, so the classification model is not biased toward the majority group and remains sensitive to high-risk minority groups such as Cluster 2.

4.3.2. ML Classification Results

A supervised learning approach was applied to develop an automated detection model capable of distinguishing between normal accounts and accounts identified as online gambling hub accounts. The model was trained using monthly transaction

data under a rolling-period training scheme and subsequently tested on the following period. This adaptive approach accounts for the dynamic nature of hub account modus operandi, which may evolve over time, as previously identified through the Focus Group Discussions (FGDs).

To obtain the optimal model configuration, hyperparameter tuning was conducted using GridSearchCV with 10-fold cross-validation. As summarized in Table 4, the best-performing models were XGBoost and Gradient Boosting, both of which consistently achieved ROC–AUC values above 0.921. These results indicate a strong capability of the models to discriminate between gambling-related and non-gambling-related accounts with high accuracy.

Table 4. Performance Summary of Adaptive Supervised Learning Models

Train Period	Test Period	Best Model	Search Type	Recall	Precision	F2 Score	ROC AUC
2024-06	2024-07	Gradient Boosting	GridSearchCV	0.940	0.256	0.613	0.991
2024-07	2024-08	XGBoost	GridSearchCV	0.969	0.107	0.371	0.969
2024-08	2024-09	Gradient Boosting	GridSearchCV	0.901	0.242	0.583	0.985
2024-09	2024-10	XGBoost	GridSearchCV	0.961	0.036	0.157	0.921

These findings are consistent with the Precision–Recall curve analysis, where XGBoost and Gradient Boosting consistently demonstrated superior performance compared to other models across all evaluation periods. The optimal operating points were located around the elbow region of the Precision–Recall curve, corresponding to precision values of approximately 0.65–0.80 and recall values of approximately 0.70–0.80. This indicates a better balance between precision and recall for the minority class and further supports the selection of Gradient Boosting and XGBoost as the most effective models.

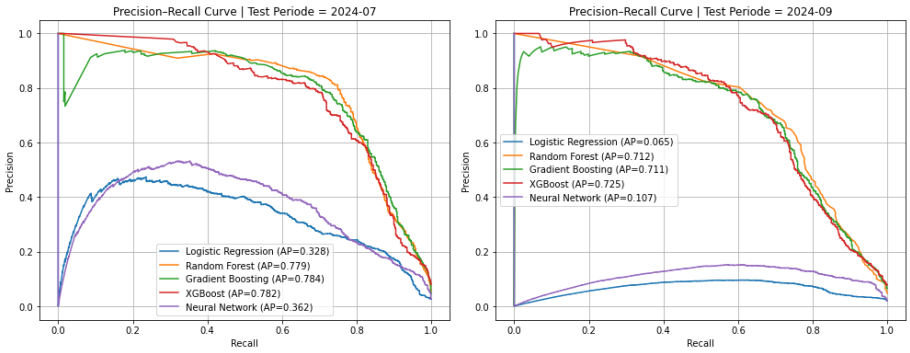


Figure 6. Precision-Recall Curve

Based on feature contribution analysis using SHAP (SHapley Additive exPlanations), several variables were identified as having a significant influence on the model's predictions, including:

1. Number of unique senders (*in-degree*), reflecting a high level of connectivity across accounts.
2. Transaction frequency during anomalous hours, such as late night and early morning periods (*trx_late_night, sndr_late_night, amt_late_night*).

3. Transaction magnitude and distribution features, including *max_amt, total_amount, med_amt,* and *std_amt*, which capture the scale and variability of transactional activity.

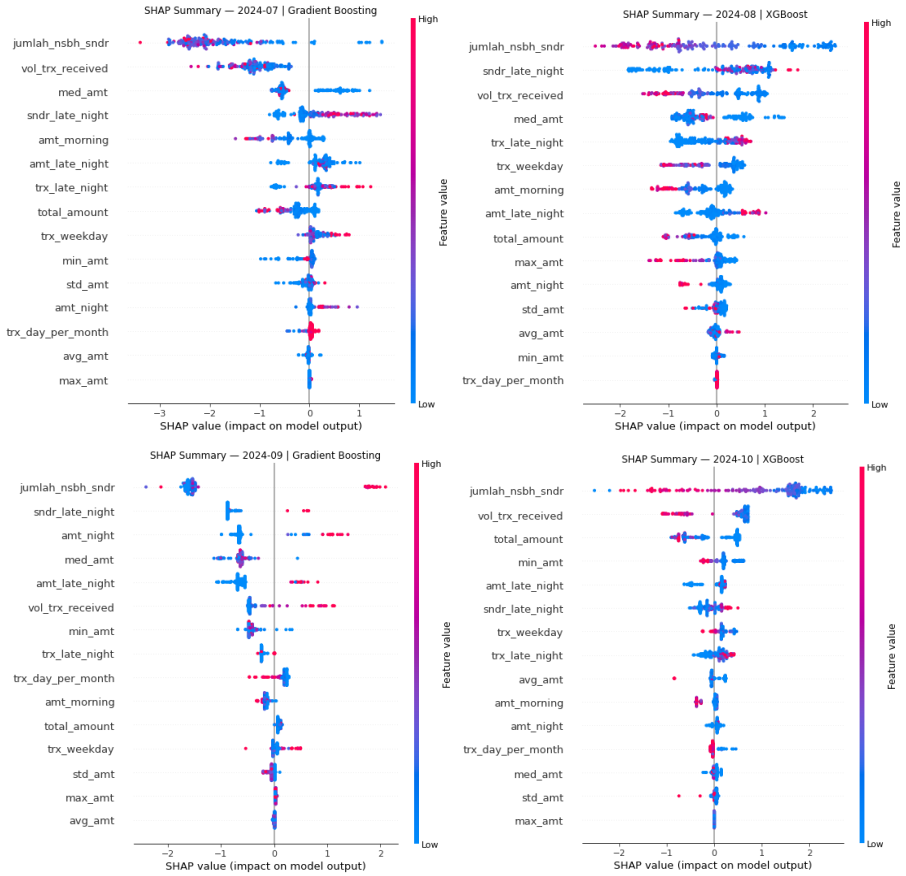


Figure 7. SHAP Summary Plot

The SHAP values indicates that transaction patterns occurring outside normal working hours consistently increase the probability of an account being classified as an online gambling-related account. In addition, greater variability in transaction values, as reflected by higher standard deviations, contributes significantly to improving the model's ability to detect anomalous behaviour.

Furthermore, evaluation results across different testing periods reveal that the best-performing model may vary over time. This variation suggests temporal changes in transaction characteristics, potentially driven by shifts in player behaviour or adaptive strategies employed by online gambling operators, as highlighted in the FGD findings. SHAP visualizations also demonstrate that while certain core features consistently appear across periods, their relative contributions and rankings may change over time. These conditions indicate that no single model remains consistently dominant across all periods, rendering a static modeling approach suboptimal. Consequently, the implementation of an adaptive supervised learning strategy through periodic model retraining, particularly under a monthly retraining scheme, is essential to ensure that the model remains responsive to evolving data patterns and maintains optimal detection performance.

4.3.3. Graph Machine Learning

Prior to applying Graph Machine Learning, a preliminary filtering stage is conducted using the Louvain Method. Fraud syndicates tend to form dense clusters,

characterized by a high volume of internal transactions among fraudster accounts, while rarely interacting with legitimate accounts outside their group. The Louvain method is highly effective in isolating such dense structures.

Additionally, this step ensures computational resources are concentrated on communities with the highest risk. The algorithm condenses a massive, unstructured population into distinct, manageable communities based on behavioral patterns and relationships. Specifically, 1,000 communities were found to account for 41% of the total transaction value, 31% of the total transaction volume, and 71% of the total fraudster samples. By focusing detection efforts on these priority clusters, the model can capture the majority of fraudulent activity without the need to process the entire millions communities that possess a low concentration of risk.

Once the priority communities were identified, the data was processed using Graph Machine Learning (GraphML). Within this GraphML framework, two fundamental data types are processed:

a. Node Data: Represents customer entities (accounts) along with their attribute features (such as in_degree, out_degree, nominal value, and volume).
b. Edge Data: Represents interactions or financial transaction relationships between customers.

The primary focus of this experiment is Node Classification . Unlike Link Prediction (which predicts the existence of relationships) or Graph Classification (which categorizes the entire network), Node Classification aims to predict the class label (Fraud vs. Normal) for each individual entity. The model utilizes topological information (edges) to enrich the representation of each node prior to classification.

In this experiment, the comparative analysis involves three GraphML algorithms: GraphSAGE, GCN, and GNN. Based on Table 5, the GraphSAGE model successfully detected 60% of fraudulent accounts (28 out of 47). Conversely, the other models (GCN & GNN) failed to identify more than half of the existing fraud cases. Although the Recall stands at 0.60, this performance is deemed acceptable given the challenge of extreme data imbalance (only 47 fraud accounts versus over 120,000 normal accounts). The model demonstrated effective identification of highly rare minority anomaly patterns (0.03% of the population) while minimizing the false positive rate to below 10% of the total population.

Table 5. Graph ML Results

Algorithm	Recall	Precision	F2 Score	ROC AUC
GraphSAGE	0.6	0.4	0.02	0.77
GCN	0.5	0.24	0.01	0.70
GNN	0.4	0.18	0.01	0.68

In contrast to legitimate customer networks, which are typically widely dispersed and randomly connected, accounts implicated in fraud tend to form long, relay-like chains. In legitimate transactions, funds move in various directions without rigid patterns. However, fraudsters tend to transfer funds sequentially and rapidly from Account A to B, then to C, and subsequently to D. The objective is to perform transaction layering to obfuscate the origin of the funds.

Figure 8. Illustration of Node Classification in GraphSAGE using FNA

Furthermore, fraud networks exhibit a high degree of connection density. These networks rely heavily on specific accounts (nodes) acting as hubs or mini-hubs to facilitate and direct the flow of illicit transactions. Typically, one or two hub accounts receive funds from multiple victim accounts simultaneously, or conversely, a single account disperses or bridges funds to subsequent fraudulent accounts.

5. Policy Recommendation

5.1. Establishing Minimum Industry Standards for Fraud Detection Systems

Drawing from the empirical findings of this research, Bank Indonesia could consider establishing minimum FDS standards for PJPs/PIPs through technical provisions (such as PADG or Technical Guidelines). These standards should encompass, at a minimum:

a. Near real-time monitoring capabilities at the account, transaction, and network levels.
b. The application of behavioural analytics that goes beyond simple blacklists to include indicators of suspicious patterns or behaviours, such as high-frequency nighttime transactions, repetitive transaction values, and dense in-degree connections.
c. The implementation of adaptive account scoring mechanisms that are updated periodically. This scoring system could eventually be developed into an early warning system to protect consumers at the point of transaction.
d. A "human-in-the-loop" procedure requiring PSP to conduct due diligence when the system flags an account or transaction pattern as high-risk.
e. Information sharing mechanisms among PSP regarding high-risk accounts, merchants, or transaction patterns. Bank Indonesia could initiate the development of an inter-regulator sharing protocol that prioritizes the principle of purpose limitation, specifically targeting financial crimes and fraud detection.

However, adopting these standards implicitly demands adequate infrastructure readiness and robust analytics engines. In practice, this requires significant investment; therefore, determining the necessary infrastructure reinforcements should ideally be risk-based and proportional to the business scale, service complexity, and risk profile of each PJP/PIP. The provisions could include a clarification that PJPs/PIPs must ensure sufficient data processing and storage capacity, as well as the capability to implement AI/ML models (whether in-house or through technology partnerships), while maintaining strict data security and protection. It is important to underscore that this research does not cover an analysis of the infrastructure investment requirements for individual providers; consequently, further studies mapping infrastructure readiness and financing schemes remain an area for future development.

5.2. Leveraging Hybrid AI/ML Models to Enhance Fraud Detection within Bank Indonesia's Payment System

We recommend developing AI/ML models through a hybrid strategy that combines three distinct approaches: unsupervised learning, supervised learning, and Graph Machine Learning (GraphML). This strategy is designed to support privacy-preserving principles and computational efficiency, eliminating the need for the system to perform a "deep scan" on the entire population of customer transactions. Instead, the system employs a prioritization mechanism before conducting in-depth analysis, as detailed below:

a. Clustering: Prior to feeding data into the supervised learning model, customer accounts are first segmented into distinct groups using clustering algorithms. Once the optimal number of clusters is determined via Silhouette Score and WSSE, we interpret the clusters to identify high-risk groups. These are characterized by specific traits such as high interconnectedness, high volumes of incoming transactions, low outgoing volumes, and significant late-night activity.
b. Targeted Sampling: To ensure a focused analysis, we perform transaction sampling within each cluster to construct the Supervised Learning and GraphML models. This strategy effectively addresses the "class imbalance" issue often encountered in FDS development, where the volume of normal transactions vastly outnumbers fraudulent ones.
c. Adaptive Rules: The outputs from Supervised Learning (e.g., XGBoost or Neural Networks) can be utilized to make the rules within the on-transaction system adaptive. For instance, if the XGBoost model detects that gambling transaction patterns have shifted this week from 01:00–03:00 to 04:00–06:00, the "High-Risk Hours" parameter in the Rule-Based system can be updated automatically (or pending supervisor approval) to reflect the latest data findings.
d. Explainability: To ensure that AI-driven identifications are accountable to customers, an "Explainable AI" policy must be applied to every account flagged for fraud. For example, a notification might read: "Your account has been blocked because it was identified as being closely linked to a fraud network (GraphML) and your nighttime transaction frequency exceeds normal limits (XGBoost)."
e. Federated Learning: To address data sensitivity and privacy constraints within Bank Indonesia's payment ecosystem, federated learning can be adopted as an alternative model enhancement mechanism. Under this approach, AI/ML models are trained collaboratively across multiple Payment Service Providers (PSPs) without requiring raw transaction data to be centralized. Each PSP performs local model training on its own data, and only encrypted model updates (e.g., gradients or parameters) are shared with the central system for aggregation.

By employing this tiered approach, integrating clustering, supervised learning, and GraphML, Bank Indonesia can implement stricter yet more efficient off-transaction oversight, minimize false positives to reduce complaints from legitimate customers, and adhere to data minimization principles. Moreover, this method shifts the surveillance paradigm from "looking for a needle in a haystack" to "separating the hay first, then finding the needle." This directly addresses the need for a surveillance system where fraud identification is both defensible and dynamic enough to keep pace with the ever-evolving modus operandi of fraudsters.

5.3. Strengthening Payment System Oversight and Consumer Protection

Subsequently, these research findings provide a fundamental basis for reinforcing the integrity of the Payment System through strengthened supervision, encompassing both indirect (off-site) and direct (on-site) methods. To that end, the recommendations for Payment System Supervision include:

a. Strengthening off-site supervision operations by utilizing the developed FDS algorithms to analyze provider transactions that indicate involvement in online gambling services. Supervisors can conduct this analysis by testing transactional data within Bank Indonesia's Payment System. The results serve as feedback for the providers, prompting them to conduct deeper verification and investigation. This approach allows off-site supervision to become more effective without the immediate need for further physical inspections.
b. Enhancing on-site examination operations by leveraging the research algorithms to develop surveillance tools capable of pinpointing accounts used for online gambling. This ensures that the examination process is efficient, effective, and strictly focused on transactional data, thereby optimizing the time required for procedures while delivering high-quality results.
c. Knowledge sharing with the industry: The developed FDS algorithms should be communicated to payment system industry players and associations. This allows them to study, further develop, and replicate the models according to their specific needs, serving as a complement to their existing FDS tools and rules. Industry players can also adapt these models to create new use cases based on evolving trends in fraud, scams, and other financial crimes.
d. Consumer Protection and Legal Framework: From a consumer protection perspective, the algorithmic outputs and supervision analysis can inform the formulation of consumer education strategies. Online gamblers, or individuals victimized by account trading schemes (mule accounts), can be the subjects of targeted education. Meanwhile, the analysis provides input for providers to refine their own education strategies. Furthermore, this research provides a basis for implementing proportional, data-driven transaction delays (blocking online gambling accounts). It establishes digital evidence with legal standing for dispute resolution mechanisms and offers legal protection for fraud analysts within the industry and at Bank Indonesia.
e. Governance and Ethics: The utilization of these research findings must be accompanied by robust and ethical governance. This includes strengthening model validation and conducting periodic audits to minimize potential false positives and other biases that could infringe on consumer rights. Implementing an appeal mechanism is also crucial, ensuring that consumers harmed by tagging errors have the opportunity to request clarification and restore their accounts.
f. Cross-Sector Collaboration: Strengthening Payment System supervision and consumer protection requires cross-sector collaboration. This is essential to

enhance supervisory effectiveness and constrict the operating space for cross-platform syndicates, thereby fortifying overall consumer protection.

6. Conclusion

This study demonstrates that online gambling activities in Indonesia exhibit account characteristics and transaction patterns that are distinctly different from normal financial transactions. Accounts identified as online gambling *hub accounts* typically display intensive transaction activity during late-night and early-morning hours, high-frequency transactions with relatively small but repetitive amounts, and dense connectivity as reflected in high in-degree values. Geographically, these activities are concentrated in regions with high internet penetration and intense economic activity, such as DKI Jakarta, West Java, and North Sumatra. Moreover, the modus operandi of online gambling operators is highly adaptive and organized, involving the use of mule accounts, rapid domain switching, and integration with digital payment systems and illegal online lending platforms to obscure financial flows.

From a methodological perspective, this research confirms that a hybrid AI/ML approach, combining unsupervised learning, supervised classification, and Graph Machine Learning, is effective in identifying and detecting online gambling transaction patterns under conditions of data imbalance. The clustering stage successfully isolates high-risk account groups, supervised learning models, particularly XGBoost and Gradient Boosting exhibit strong classification performance in distinguishing gambling-related and non-gambling-related accounts, and GraphML effectively uncovers organized transactional networks with acceptable performance. Model interpretability using SHAP further ensures explainability, with key features such as late-night transaction behaviour, the number of unique senders, and transaction value variability consistently contributing to detection outcomes. These findings highlight the superiority of adaptive, data-driven models over static approaches in responding to the evolving behaviour of online gambling activities.

Based on these findings, this study suggests policy recommendation to strengthening payment system oversight and consumer protection. Payment system regulators, particularly Bank Indonesia, are encouraged to promote the adoption of adaptive AI/ML-based Fraud Detection Systems (FDS) that are standardized yet proportionate to the risk profiles of payment service providers. Supervisory frameworks that integrate behavioural analytics, transaction network analysis, and human-in-the-loop mechanisms can enhance detection effectiveness while mitigating false positives. Overall, this research offers an empirical and technical foundation for developing more responsive, accountable, and sustainable policy interventions to combat online gambling within the payment system ecosystem.

References

Agrawal, S., Agrawal, J., & Jain, S. (2015). A survey on credit card fraud detection. *International Journal of Computer Applications, 98*(3), 1–9.

Alamri, M., & Ykhlef, M. (2024). Hybrid Feature Engineering Based on Customer Spending Behaviour for Credit Card Anomaly and Fraud Detection. *Electronics, 13*(20), 3978.

Alothman, R., Talib, H. A., & Mohammed, M. S. (2022). Fraud detection under the unbalanced class based on gradient boosting. Eastern-European Journal of Enterprise Technologies, 2(2 (116)), 6–12.

Assis, C. A., Pereira, A. C., Pereira, M. A., & Carrano, E. G. (2014). A genetic programming approach for fraud detection in electronic transactions. In *2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)* (pp. 1–8). IEEE.

Athallah, N. H., & Isnani, A. R. (2024). Factors that cause many people to play gambling. *SINATTI, Universitas Semarang*.

Authorize.Net. (2012). *Fighting online fraud* (White paper No. WP-FRAUD-0712). CyberSource Corporation.

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2015). Detecting credit card fraud using periodic features. *In 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)* (pp. 208–213). IEEE.

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. Expert Systems with Applications, 51, 134–142.

Bank Indonesia. (2025). *Statistik Sistem Pembayaran dan Infrastruktur Pasar Keuangan (SPIP)*. Bank Indonesia.

Behera, R., & Panigrahi, S. (2015). Fuzzy clustering and neural network approach for fraud detection. *International Journal of Computer Applications, 111*(11), 1–7.

Bekirev, A. S., Klimov, V. V., Kuzin, M. V., & Shchukin, B. A. (2015). Payment card fraud detection using neural network committee and clustering. *Optical Memory and Neural Networks, 24*(3), 193–200.

Bhatla, T. P., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. *Cards Business Review, 1*(6).

Bhusari, V., & Patil, S. (2011). Study of Hidden Markov Model in credit card fraudulent detection. *International Journal of Computer Applications, 20*(5), 33–36.

Bolton, R. J., & Hand, D. J. (2001). Unsupervised profiling methods for fraud detection. *Credit Scoring and Credit Control VII*, 235–255.

Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2014). BankSealer: An online banking fraud analysis and decision support system. In *IFIP International Information Security Conference* (pp. 380–394). Springer.

Carneiro, E. M., Dias, L. A. V., da Cunha, A. M., & Mialaret, L. F. S. (2015). Cluster analysis and artificial neural networks: A case study in credit card fraud detection. In *2015 12th International Conference on Information Technology–New Generations (ITNG)* (pp. 122–126). IEEE.

Chen, J., Tao, Y., Wang, H. and Chen, T. (2015). Big data based fraud risk management at Alibaba. *The Journal of Finance and Data Scienece*. 1(1), 1-10.

Cheng, D., Zou, Y., Xiang, S., & Jiang, C. (2024). Graph neural networks for financial fraud detection: A review. *Frontiers of Computer Science, 0*(0), 1–17.

Correia, I., Fournier, F., & Skarbovsky, I. (2015). The uncertain case of credit card fraud detection. In *Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems* (pp. 181–192). ACM.

Duman, E., & Elikucuk, I. (2013). Applying migrating birds optimization to credit card fraud detection. In *PAKDD 2013 – Knowledge Discovery and Data Mining* (pp. 416–427).

Duman, E., & Ozcelik, M. H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications, 38*(10), 13057–13063.

Dwihayuni, Y. P., & Fauzi, A. M. (2021). The motive for the action of online gambling as an additional livelihood during social restrictions due to the Covid-19 pandemic. *Jurnal Sosiologi Dialektika, 16*(2), 108–116.

Elie, A. I. N., et al. (2023). Online gambling addiction in Parakou (Benin, 2022). *Open Journal of Psychiatry, 13*(5), 421–437.

Fahrudin, A., et al. (2024). Online gambling addiction: Problems and solutions for policymakers and stakeholders in Indonesia. *Journal of Infrastructure, Policy and Development, 8*(11), 9077.

Gainsbury, S. M. (2015). Online gambling addiction: The relationship between internet gambling and disordered gambling. *Current Addiction Reports, 2*(2), 185–193.

Hamilton, W. L., Ying, R., & Leskovec, J. (2017). Inductive representation learning on large graphs. Advances in Neural Information Processing Systems, 30, 1024–1034.

Håkansson, A. (2020). Impact of COVID-19 on online gambling—A general population survey during the pandemic. *Frontiers in Psychology, 11*, 568543.

Hendrawan, M. R. N. A., Marits, S. A., & Herman, S. (2023). Development of digital payment systems in Indonesia. *Jurnal Ilmiah Manajemen Kesatuan, 11*(3), 1335–1344.

IASC. (2025). *Marak penipuan keuangan, OJK bersama Pemerintah luncurkan Kampanye Nasional Berantas Scam dan Aktivitas Keuangan Ilegal* [Siaran pers].

Khan, A. U. S., Akhtar, N., & Qureshi, M. N. (2014). Real-time credit-card fraud detection using artificial neural network tuned by simulated annealing algorithm. In *Proceedings of the International Conference on Recent Trends in Information, Telecommunication and Computing (ITC)* (pp. 113–121).

Khan, M. Z., Pathan, J. D., & Ahmed, A. H. E. (2014). Credit card fraud detection system using Hidden Markov Model and K-clustering. *International Journal of Advanced Research in Computer and Communication Engineering, 3*(2), 5458–5461.

Konstantinidis, G., & Gegov, A. (2024). Deep neural networks for anti-money laundering using explainable artificial intelligence. In *2024 IEEE 12th International Conference on Intelligent Systems (IS)*. https://doi.org/10.1109/IS-2024-93893711

Matsumura, E. M., & Tucker, R. R. (1992). Fraud detection: A theoretical foundation. *The Accounting Review, 67*(4), 753–782.

Oracle Financial Services Software. (2014). *Oracle Financial Services Fraud Detection and Monitoring*. Oracle Corporation.

Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A. (2009). Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. *Information Fusion, 10*(4), 354–363.

Patel, R. D., & Singh, D. K. (2013). Credit card fraud detection and prevention of fraud using genetic algorithm. *International Journal of Soft Computing and Engineering, 2*(6),

Pemerintah Republik Indonesia. (2024). *Keputusan Presiden Republik Indonesia Nomor 21 Tahun 2024 tentang Satuan Tugas Pemberantasan Perjudian Daring*. Sekretariat Negara.

Perdana, R. B., et al. (2024). Detecting online gambling promotions on Indonesian Twitter using text mining algorithm. *International Journal of Advanced Computer Science and Applications, 15*(8), 942–949.

Poon, C.-H., Kwok, J., Chow, C., & Choi, J.-H. (2025). LineMVGNN: Anti-money laundering with line-graph-assisted multi-view graph neural networks. *AI, 6*(4), 69. https://doi.org/10.3390/ai6040069

Prakash, A., & Chandrasekar, C. (2012). A novel Hidden Markov Model for credit card fraud detection. *International Journal of Computer Applications, 59*(3), 1–6.

Prakash, A., & Chandrasekar, C. (2015). An optimized multiple semi-hidden Markov model for credit card fraud detection. *Indian Journal of Science and Technology, 8*(2), 165–171.

Pusat Pelaporan dan Analisis Transaksi Keuangan. (2024). *Laporan Tahunan PPATK Tahun 2023*. PPATK.

Pusat Pelaporan dan Analisis Transaksi Keuangan. (2025). *Laporan Tahunan PPATK Tahun 2024*. PPATK.

Rafi, S. M. S., et al. (2024). Machine learning in financial fraud detection: New models for predictive analysis and mitigating business risks. *Advanced International Journal of Multidisciplinary Research, 2*(6), 1–23.

RamaKalyani, K., & UmaDevi, D. (2012). Fraud detection of credit card payment system by genetic algorithm. *International Journal of Scientific & Engineering Research, 3*(7), 1–6.

Renuga, T. D., Rabiyathul, A. B., & Kamaladevi, M. (2014). Fraud detection in card-not-present transactions based on behavioural pattern. *Journal of Theoretical and Applied Information Technology, 61*(3), 1–9.

Sánchez, D., Vila, M. A., Cerda, L., & Serrano, J. M. (2009). Association rules applied to credit card fraud detection. *Expert Systems with Applications, 36*(2), 3630–3640.

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science, 2*(3), 1–21.

Singh, P., & Singh, M. (2015). Fraud detection by monitoring customer behaviour and activities. *International Journal of Computer Applications, 111*(11), 15–22.

Soltani, N., Akbari, M. K., & Javan, M. S. (2012). A new user-based model for credit card fraud detection based on artificial immune system. In *AISP 2012 – 16th CSI International Symposium on Artificial Intelligence and Signal Processing* (pp. 29–33).

Sudjianto, A., Yuan, M., Kern, D., Nair, S., Zhang, A., & Cela-Díaz, F. (2010). Statistical methods for fighting financial crimes. *Technometrics, 52*(1), 5–19.

Törrönen, J., Samuelsson, E., & Gunnarsson, M. (2020). Online gambling venues as relational actors in addiction: Applying the actor-network approach to life stories of online gamblers. *International Journal of Drug Policy, 85*, 102928.

Vorobyev, A., & Krivitskaya, L. (2022). Financial fraud detection using hybrid machine learning models. *Journal of Financial Crime, 29*(4), 1231–1248.

Winarsih, N., & Salsabila, S. (2022). The phenomenon of internet addiction disorder online gambling in Probolinggo. *Entita, 4*(2), 183–196.

World Bank. (2023). *Individuals using the internet (% of population) – Indonesia* [Data set]. World Development Indicators.

Xinwei Zhang, Han, Y., Xu, W., & Wang, Q. (2021). HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. *Information Sciences, 557*, 302–316.

Yen-Wu Ti, Hsin, Y.-Y., Dai, T.-S., Huang, M.-C., & Liu, L.-C. (2022). Feature generation and contribution comparison for electronic fraud detection. *Scientific Reports, 12*, 18042.

Yvan Lucas, Portier, P.-E., Laporte, L., He-Guelton, L., Caelen, O., Granitzer, M., & Calabretto, S. (2020). Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Future Generation Computer Systems, 102*, 393–402.

Zhang, M., Yang, Y., Guo, S., Cheok, C., Wong, K. E., & Kandasami, G. (2018). Online gambling among treatment-seeking patients in Singapore: A cross-sectional study. *International Journal of Environmental Research and Public Health, 15*(4), 832.