Fraud Detection in Mobile Phone Recharge Transactions Using K-Means and T-SNE Visualization

Irwin Sakti[1)*], Arvin Mareta[2)], Ito Wasito[3)]
[1,2,3)] Information Technology, Science and Technology Faculty, Pradita University, Indonesia
[1)]irwin.sakti@student.pradita.ac.id, [2)]arvin.mareta@student.pradita.ac.id, [3)]ito.wasito@pradita.ac.id

Submitted :Dec 12, 2024 | **Accepted** : Dec 20, 2024 | **Published** : Jan 12, 2025

Abstract: The rapid expansion of digital transactions has heightened vulnerabilities in mobile recharge systems, exposing them to sophisticated fraudulent activities. This study introduces a robust framework for fraud detection that integrates K-Means clustering with t-Distributed Stochastic Neighbor Embedding (t-SNE) visualization. Using a dataset comprising over 200,000 mobile recharge transactions, this approach systematically identifies anomalies by analyzing transaction patterns, processing times, error frequencies, and geographic attributes. The methodology emphasizes data preprocessing, applying K-Means clustering to segregate transaction records into meaningful clusters. t-SNE visualization further enhances interpretability, offering a clear representation of high-dimensional data. Compared to Autoencoders, the framework demonstrates superior performance, achieving a Silhouette Score of 0.6215 and a Davies-Bouldin Index of 0.7074, underscoring its computational efficiency, interpretability, and clustering quality. Distinct cluster characteristics, such as prolonged processing times, high nominal values, and frequent errors, were effectively flagged as potential fraud indicators. These findings validate the proposed framework's adaptability to large-scale transactional data and its practicality in real-world scenarios. By bridging the gap between advanced machine learning techniques and actionable insights, this study empowers service providers to mitigate financial risks and enhance system integrity. Future research can explore hybrid models and refined feature engineering to address evolving fraud patterns. This work sets a foundation for scalable, interpretable, and precise fraud detection strategies across digital transaction ecosystems.

Keywords: Anomaly Detection; Fraud Detection; K-Means Clustering; Mobile Recharge Systems; t-SNE Visualization.

INTRODUCTION

The rapid growth of digital transactions has revolutionized the use of mobile recharge vouchers, offering consumers unmatched convenience and efficiency. However, this transformation has brought new challenges, as fraudulent activities such as voucher reuse, transaction manipulation, and system exploitation have become increasingly sophisticated. These fraudulent practices pose significant financial and reputational risks to service providers. Traditional methods, such as rule-based heuristics and manual audits, are no longer effective in addressing the dynamic and complex nature of fraud patterns. This highlights an urgent need for advanced and scalable solutions capable of detecting fraud swiftly and with high accuracy (Hanae et al., n.d.; Zhou et al., 2019). This study aims to address these challenges by identifying potential fraudulent activities in mobile recharge transactions through the application of machine learning techniques. By focusing on enhancing fraud detection systems, this research seeks to mitigate financial risks, improve operational efficiency, and strengthen the trust between service providers and their users.

To achieve this, the study conducts a comparative analysis of two methodologies: K-Means clustering and Autoencoders. K-Means is a widely adopted algorithm for partitioning datasets into meaningful clusters based on similarity, making it particularly effective for detecting anomalies in mobile recharge systems. Its computational efficiency, simplicity, and ability to highlight outliers that may indicate fraudulent behaviour make it a preferred choice in many fraud detection scenarios (Dwi Aulia & Nurahman, 2023; Sari & Suharjito, 2022). When combined with t-Distributed Stochastic Neighbour Embedding (t-SNE), a powerful data visualization technique, K-Means

*name of corresponding author

enhances interpretability by revealing complex data patterns and outliers, enabling service providers to quickly identify and respond to suspicious activities (Goh et al., 2022).

Recent studies have explored the potential of machine learning techniques for fraud detection, particularly Autoencoders. Autoencoders, a type of artificial neural network, excel at compressing high-dimensional data into a latent space and reconstructing it with minimal loss of information. The training process focuses on minimizing the disparity between the input data and its reconstructed counterpart, typically measured using loss functions such as mean squared error, ensuring the model effectively captures and retains essential data features. This makes them particularly effective for identifying subtle anomalies in transactional data (Sari & Suharjito, 2022). However, their application in fraud detection is not without limitations. Autoencoders often require significant computational resources, making them less practical for real-time or large-scale systems. Moreover, while they effectively model normal transaction behaviors, the results tend to lack interpretability. The reconstruction errors, which signal anomalies, can be challenging to translate into actionable insights without supplementary techniques. Additionally, their performance in distinguishing between normal and fraudulent transactions in high-dimensional datasets can be suboptimal, as they struggle to provide distinct separations between clusters (Pumsirirat & Yan, 2018).

Between these two approaches, the results of this study demonstrate that K-Means clustering outperforms Autoencoders. With higher Silhouette Scores and lower Davies-Bouldin Index (DBI) values, K-Means consistently produces more distinct and cohesive clusters, facilitating clearer delineation between legitimate and fraudulent transactions. Its interpretability and ability to provide actionable insights make it particularly well-suited for this application. Consequently, this research adopts K-Means as the primary method for analysing fraud patterns, focusing on its efficiency and effectiveness in uncovering anomalies within transactional data.

K-Means serves as a powerful clustering method for identifying transaction patterns that deviate from normal behaviour, while t-SNE enhances interpretability by providing a visual representation of high-dimensional data and its outliers (Z. Huang et al., 2024; Zhou et al., 2019). Together, these techniques offer a practical solution for mitigating financial losses and safeguarding the reputation of service providers.

LITERATURE REVIEW

A review of existing literature highlights key advancements in fraud detection methodologies, as well as gaps in adapting these approaches to mobile recharge scenarios. The following table summarizes three relevant studies that provide a foundation for the methods proposed in this research, along with their contributions and limitations.

Table 1. Previous research in fraud detection

Author	Research Title	Description	Gap
(Pumsirirat & Yan, 2018)	Credit card fraud detection using deep learning with auto-encoder and restricted Boltzmann machine	This study uses Autoencoder and restricted Boltzmann machines to identify anomalies in credit card transactions, emphasizing deep learning's ability to handle high-dimensional data effectively.	Does not integrate t-SNE for better visualization and interpretability of high-dimensional data patterns.
(Chowdari & Parthiban, 2022)	Credit Card Fraud Detection Using Logistic Regression Compared with t-SNE	This study compares Logistic Regression with t-SNE for fraud detection, highlighting that Logistic Regression achieves higher accuracy (99.89%) compared to t-SNE (60.99%). The dataset focuses on credit card transactions and evaluates different classification models.	The study focuses solely on a supervised algorithm (Logistic Regression) and does not utilize t-SNE as a visualization tool to enhance the interpretability of clustering.
(Sari & Suharjito, 2022)	Outlier detection in inpatient claims using DBSCAN and K-Means	Examines the application of DBSCAN and K-Means for detecting outliers in inpatient claims, showcasing clustering techniques' utility in anomaly detection.	Focuses on healthcare claims; lacks adaptation to mobile recharge fraud scenarios and combined use of K-Means, Autoencoder, and t-SNE.

The three reviewed studies provide critical context and complementary insights for addressing fraud detection in mobile recharge transactions using K-Means, Autoencoder, and t-SNE visualization. Pumsirirat and Yan (2018) demonstrate the effectiveness of Autoencoders in handling high-dimensional data and identifying anomalies, which supports the inclusion of Autoencoders in this study for capturing subtle fraud patterns. However, their lack

*name of corresponding author

of visualization tools like t-SNE highlights the need for better interpretability, which this research addresses by integrating t-SNE for clearer insights into data clustering. Chowdari and Parthiban (2022) emphasize the role of visualization in fraud detection, showing t-SNE's potential to reveal hidden patterns, even though their focus was limited to supervised methods like Logistic Regression. This aligns with the current study's goal of enhancing clustering interpretability and extends the application of t-SNE to unsupervised methods like K-Means. Finally, Sari and Suharjito (2022) validate the effectiveness of K-Means in detecting anomalies but restrict their application to healthcare claims. Their findings affirm K-Means' utility in clustering large datasets, providing a foundation for its application in this study, which adapts it to mobile recharge fraud detection while combining it with Autoencoders and t-SNE for a comprehensive approach. Together, these studies guide the methodological choices in this research, bridging gaps in visualization, scalability, and domain-specific adaptation.

METHOD

The methodology employed in this study utilizes advanced clustering techniques and visualization tools to effectively identify potential fraud in mobile recharge transactions. By systematically processing transactional datasets, this approach ensures that the data is prepared for robust analysis. The data preparation phase includes selecting relevant features, addressing missing values, and standardizing variables—steps critical for maintaining data integrity and ensuring meaningful comparisons across records(Ahmed et al., 2020; Murena et al., 2018).

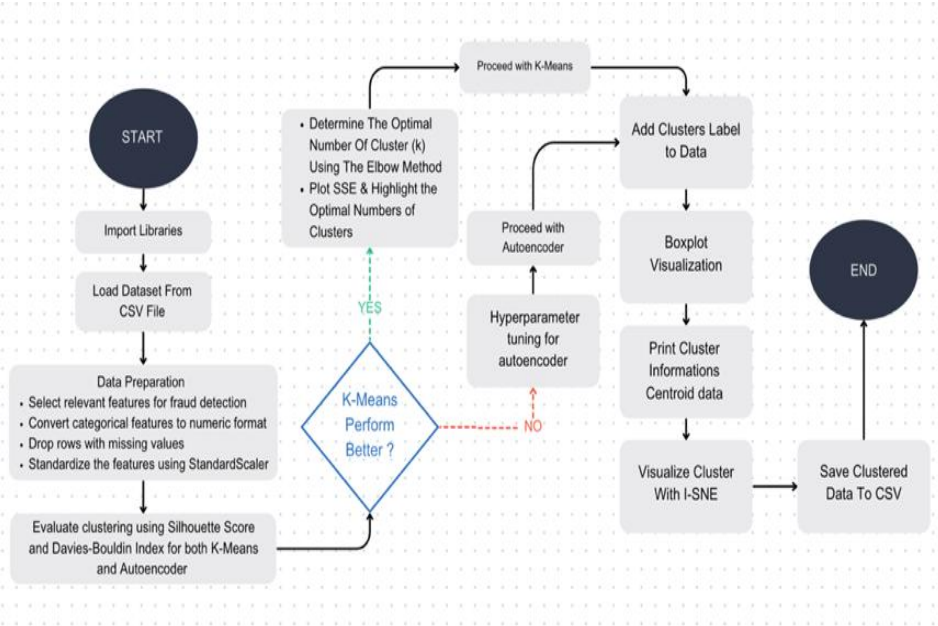
START
Import Libraries
Load Dataset From CSV File
Data Preparation
• Select relevant features for fraud detection
• Convert categorical features to numeric format
• Drop rows with missing values
• Standardize the features using StandardScaler
Evaluate clustering using Silhouette Score and Davies-Bouldin Index for both K-Means and Autoencoder
K-Means Perform Better ?
YES
NO
• Determine The Optimal Number Of Cluster (k) Using The Elbow Method
• Plot SSE & Highlight the Optimal Numbers of Clusters
Proceed with K-Means
Hyperparameter tuning for autoencoder
Proceed with Autoencoder
Add Clusters Label to Data
Boxplot Visualization
Print Cluster Informations Centroid data
Visualize Cluster With t-SNE
Save Clustered Data To CSV
END

Fig. 1 Proposed Flow of Identification Fraud Potential in Mobile Recharge Transaction
Sources: Researcher Property

Data Description

The data used in this study consists of transaction logs from mobile recharge voucher activities. The dataset includes three months of transactional data (June, July, and August 2024), comprising 184 files. This dataset captures various transactional features, including numerical, categorical, and datetime attributes, allowing a comprehensive analysis of recharge behaviours.

Dataset Overview

The dataset utilized in this study comprises 26 columns and more than 200,000 rows, capturing a comprehensive record of mobile recharge transactions. The dataset includes features such as *Serial_number*, *Nominal*, *Redeem_state*, *Redeem_state Date*, *Created Datetime*, *B Number*, *Open error*, *Process Time*, *Channel type*, *Region ID*, and several others. These attributes provide detailed insights into transaction behaviors, making the dataset a robust resource for identifying fraudulent patterns.

Table 2. Sample Dataset

Serial_nu	Nominal	Redeem_state	Redeem state Date	Created Datetime	B Number	Open error	Process Time	Delivery Chann	Status Voucher	Region ID	Channel type	Channel ID	Recharge type

mber								el Name					
9017327xxxxx	21500	3	31/08/24 21.15	31/08/24 21.15	62822956xxxxx	2	16	NaN	3	3	2	f0	1
9017330xxxxx	12000	2	31/08/24 21.15	31/08/24 21.15	62821687xxxxx	2	27	NaN	2	1	2	f0	1
9017334xxxxx	12000	3	31/08/24 21.15	31/08/24 21.15	62812658xxxxx	2	17	NaN	3	1	2	f0	1
8003803xxxxx	12000	2	31/08/24 21.15	31/08/24 21.15	62813622xxxxx	2	25	NaN	2	1	2	f0	1

Each column provides valuable insights into specific aspects of the transactions,

Table 3. Data Field Description

Field	Description
Serial_number	A unique identifier assigned to each voucher transaction, ensuring traceability and preventing redundancy.
Nominal	Represents the monetary value or denomination of the voucher processed in a transaction, which is crucial for understanding financial patterns.
Redeem_state	Indicates the redemption status of the voucher, such as whether it has been successfully used or remains unused.
Date & Created Datetime	These fields record when the transaction occurred and when it was created, enabling the analysis of temporal patterns and trends.
B Number & A Number	Contain the destination and source phone numbers involved in the transaction, offering insights into user behaviour and interaction networks.
Open error & Error Info	Reflect errors encountered during transaction processing, which may indicate system issues or fraudulent activities.
Process Time	Records the time taken to complete each transaction, with unusually high or low values potentially highlighting anomalies.
Delivery Channel Name	Specifies the channel through which the voucher was delivered, although significant missing values limit its utility for this study.
LACCI A Number & LACCI B Number	Contain codes associated with cell towers or geographic regions, providing a basis for location-based analysis.
DC Order ID	A unique order identifier that helps in tracking and analysing individual transactions.
Status Voucher	Indicates the current status of the voucher, such as valid, redeemed, or void, which is essential for identifying discrepancies or misuse.
Region ID	Represents the geographic region where the transaction occurred, facilitating the identification of fraud patterns based on location.
Store ID & Channel type	Identify the store or channel type used for the transaction, though missing values in these fields limit their contribution to the analysis.
Channel ID	Offers specific details about the transaction channel, helping to uncover anomalies or patterns in routing.
Recharge type	Specifies the type of recharge, enabling segmentation and classification of transaction types.

This dataset forms the cornerstone of this study, providing a rich source of transactional data for identifying patterns, anomalies, and potential fraud. For this study, key features such as Nominal, Process Time, Open error, Redeem_state, Channel type, and Region ID are selected to serve as critical indicators of potential fraud. These features were chosen based on their relevance to capturing anomalies in transaction amounts, processing times, error occurrences, and geographic or channel-specific patterns, all of which are common fraud markers. It is important to note that some columns, such as Delivery Channel Name and Store ID, exhibit significant missing values, limiting their utility in this analysis. Other attributes, like Node B# and Dealer Code, also contain partial missing data, which necessitates careful handling during the data preparation phase.

Methodology

Identifying potential fraud in mobile recharge transactions requires robust methodologies capable of detecting anomalies and irregular patterns within transactional data. A range of techniques exists to address this challenge, each tailored to uncover suspicious activities based on specific patterns. These methods include anomaly detection, classification models, and unsupervised learning techniques, all of which have proven effective in various contexts.

Anomaly detection in fraud detection employs various methodologies, including Isolation Forest, Local Outlier Factor (LOF), and Autoencoders. Autoencoders, a deep learning approach, encode data into a compact latent space and reconstruct it, identifying anomalies based on reconstruction errors. While powerful, this method often requires substantial computational resources and careful tuning (Ikeda et al., n.d.; Wu & Wang, 2021). For unsupervised learning, clustering techniques like K-Means are widely utilized to uncover patterns and anomalies in the absence of labelled data. In contrast, supervised classification models, such as Random Forest, Decision Trees, Gradient Boosting (XGBoost, LightGBM), and Logistic Regression, are effective when labelled datasets are available, enabling precise prediction of fraudulent activities. These methods collectively offer a robust toolkit for addressing the complexities of fraud detection in large-scale transactional data.

This study evaluates two methodologies **K-Means clustering** and **Autoencoders** to identify fraudulent patterns in mobile recharge transactions. K-Means clustering is a highly regarded algorithm commonly employed to divide large datasets into distinct and meaningful clusters by identifying patterns of similarity among data points. Its simplicity and computational efficiency make it particularly suitable for analysing vast transactional data. By identifying clusters that deviate from typical patterns, K-Means proves effective in detecting anomalous behaviours indicative of fraud (Jiang et al., 2023). Autoencoders are neural networks designed for unsupervised feature learning. They reduce dimensionality by compressing input data into a latent representation and reconstructing it, where deviations in reconstruction errors can signify anomalies (Sari & Suharjito, 2022). t-SNE Visualization To enhance interpretability, **t-Distributed Stochastic Neighbour Embedding (t-SNE)** is employed to project high-dimensional data into a lower-dimensional space. This technique visualizes clustering results, revealing patterns and anomalies that may remain hidden in numerical analysis (Rezapour, 2019).

Evaluation

In the context of identifying potential fraud in mobile recharge transactions, evaluating the quality of clustering is crucial to ensure reliable and meaningful results. Effective clustering not only needs to form well-defined groups but also distinguish normal transactions from suspicious patterns. To achieve this, Silhouette Score and Davies-Bouldin Index (DBI) are utilized as key metrics to evaluate the performance of the clustering methods applied in this study. This metric is particularly useful for assessing how distinct and cohesive the clusters are, especially when detecting potential fraud, which often manifests as small, distinct clusters or outliers (Sari & Suharjito, 2022; Setiawan et al., n.d.)

The formula for calculating the Silhouette Score for a single data point x is as follows (Rousseeuw, 1987):

$$s(x) = \frac{w(x)-v(x)}{\max\ \{v(x), w(x)\}} \qquad (1)$$

Where:
Cohesion v(x): The average distance between x and other points in its own cluster (cohesion).
Separation w(x): The average distance between xxx and points in the nearest neighbouring cluster (separation).
s(x) = [-1, +1]: -1=bad, 0=indifferent, 1=good

The overall **Silhouette Coefficient (SC)** for the dataset is the average score for all data points:

$$SC = \frac{1}{N}\sum_{x=1}^{N} s(x) \qquad (2)$$

Interpretation of Silhoutte:
A Silhouette Score near +1 indicates that clusters are well-defined and separated, ideal for distinguishing normal transaction patterns from anomalies.
A score near 0 suggests that points lie on the border between clusters, potentially representing borderline or ambiguous cases.
A negative score indicates that points may be misclassified, closer to another cluster than their own, often highlighting outliers or potential fraud.

The Davies-Bouldin Index (DBI) measures the average similarity between each cluster and its most comparable neighboring cluster. Lower DBI scores reflect superior clustering performance, indicating that clusters are both densely compact and distinctly separated from one another (Tran et al., 2019). This metric ensures that normal and fraudulent transaction clusters remain distinct and interpretable. This index, introduced by **David L. Davies** and **Donald W. Bouldin**, is detailed in their seminal paper published in the *IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. PAMI-1, No. 2, April 1979*. Mathematically, it can be expressed as (Fu et al., 1977) :

$$DBI = \frac{1}{n}\sum_{x=1}^{n} \max_{x \neq y} R_{xy} \ (3)$$

Where R_{xy} The maximum similarity between cluster x and any other cluster y, calculated as:

$$R_{xy} = \frac{SSW_x + SSW_y}{SSB_{xy}} \qquad (4)$$

Where Intra-cluster distance (SSW):

$$SSW_x = \left\{\frac{1}{Mx}\sum_{y=1}^{Mx} |x_y - A_x|^q\right\}^{1/q} (5)$$

Where Inter-cluster distance (SSB):

$$SSB_{xy} = \left\{\sum_{l=1}^{K} |b_{lx} - b_{ly}|^p\right\}^{1/p} \qquad (6)$$

Interpretation of DBI:

Low DBI: Indicates compact, well-separated clusters, which is ideal for clustering tasks, especially in fraud detection where distinct groups help isolate normal and suspicious transactions.

High DBI: Suggests overlapping or poorly separated clusters, making it challenging to distinguish between normal and fraudulent behaviours.

By applying the DBI calculation, the study ensures that the chosen clustering method that are both compact and distinct, enhancing the reliability and interpretability of the fraud detection process

RESULT

Based on proposed flow of the identification fraud potential in mobile recharge transaction, this study evaluates the potential of two clustering techniques, **K-Means** and **Autoencoders**, to identify fraudulent activities in mobile recharge transactions. The performance of these methods was assessed using well-established metrics: **Silhouette Score** and **Davies-Bouldin Index (DBI)**, with additional insights provided through **t-SNE visualization**.

The experiment followed a systematic process to ensure robust results. Initially, the necessary libraries were imported to implement clustering methods and visualization tools. The transactional dataset was then loaded, containing features relevant to fraud detection. In the data preparation stage, key features such as *Nominal*, *Process Time*, *Open Error*, *Redeem State*, *Channel Type*, and *Region ID* were selected for their relevance in identifying potential fraud. Categorical features were converted into numeric formats, and the dataset was cleaned by removing incomplete rows to ensure consistency and integrity. To maintain uniformity and comparability across features, the data was standardized using Standard Scaler.

To evaluate the effectiveness of both K-Means and Autoencoders, two key metrics were employed: **Silhouette Score** and **DBI**. These metrics provided a comprehensive framework for comparing clustering methods and ensured alignment with the study’s objectives. The results demonstrated that K-Means consistently outperformed Autoencoders in clustering performance. Table 4 illustrate that K-Means produced more precise and well-defined groupings, effectively distinguishing between normal and anomalous transaction patterns. This performance, combined with interpretability and computational efficiency, led to the selection of K-Means for further analysis.

Table 4. Evaluation Metrics

Method	Silhouette Score	DBI
K-Means	0,6215	0,7074
Autoencoder	0,5021	1,3609

The elbow method was employed to determine the optimal number of clusters (*k*). By calculating the Sum of Squared Errors (SSE) across different cluster counts, the "elbow point," where reductions in SSE began to plateau, was identified as the ideal cluster number (Figure 2).

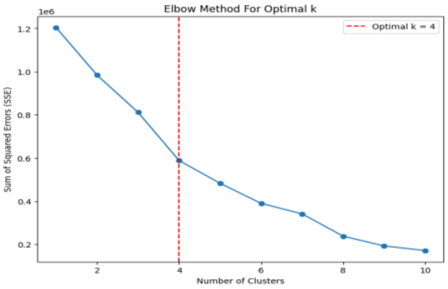

Fig. 2 K-Means elbow method
Sources: Researcher Property

The **KneeLocator tool** confirmed this selection, ensuring an optimal balance between cluster compactness and computational efficiency, the analysis revealed that the most suitable number of clusters for this dataset is **four**.

Using the optimal number of clusters, the data was processed with **K-Means** to generate cluster labels that categorize transactions based on behavioral patterns. Boxplot visualizations (Figures 3–6) were employed to analyze the distribution of key features across the identified clusters. The **Nominal feature** (Figure 3) displays distinct value ranges and variability, highlighting clear differences between clusters. In the **Process Time** boxplot (Figure 4), **Cluster 2** exhibits extreme outliers with significantly higher processing times compared to Clusters 0, 1, and 3, signalling potentially anomalous transactions. The **Redeem State** boxplot (Figure 5) reveals a notable distinction, with **Cluster 3** showing higher redeem state values, indicating unique transactional behavior, whereas Clusters 0 and 1 demonstrate more consistent and uniform patterns. Lastly, the **Region ID** boxplot (Figure 6) indicates that Clusters 2 and 3 span a wider range of regions, while Clusters 0 and 1 are more geographically restricted, suggesting localized behavior versus distributed anomalies.

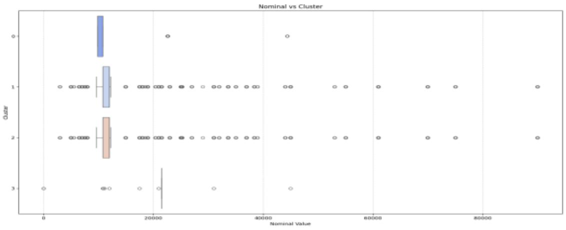

Fig. 3 Boxplot Nominal vs Cluster
Sources: Researcher Property

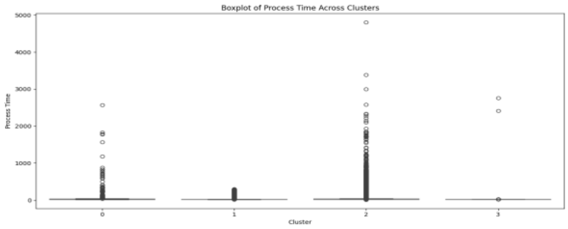

Fig. 4 Boxplot of Process Time across Cluster
Sources: Researcher Property

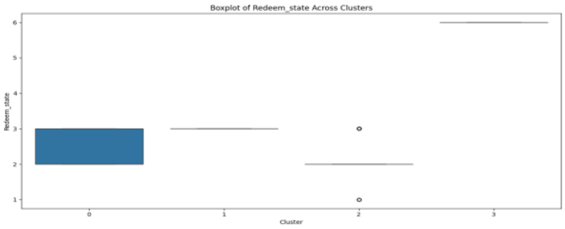

Fig. 5 Boxplot of Redeem State across Cluster
Sources: Researcher Property

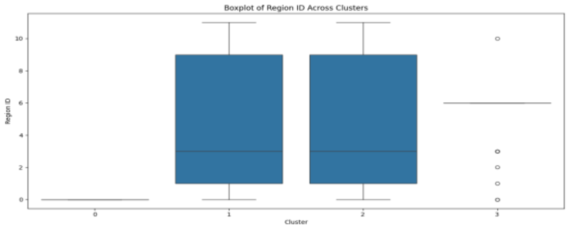

Fig. 6 Boxplot of Region ID across Cluster
Sources: Researcher Property

The t-SNE for K-Means plots (Figures 7–11) provided distinct visual representations of transaction clusters, revealing patterns and anomalies that might have otherwise been missed in numerical analysis.
Visualization with t-SNE

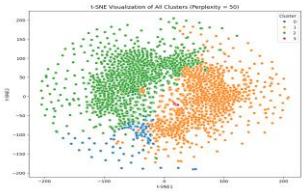

Fig. 7 t-SNE K-Means All Cluster
Sources: Researcher Property

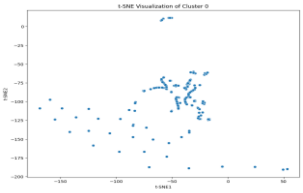

Fig. 8 t-SNE K-Means Cluster 0
Sources: Researcher Property

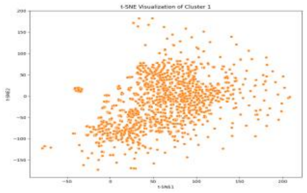

Fig. 9 t-SNE K-Means Cluster 1
Sources: Researcher Property

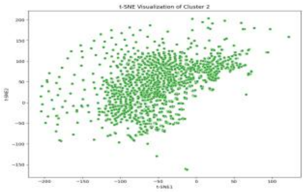

Fig. 10 t-SNE K-Means Cluster 2
Sources: Researcher Property

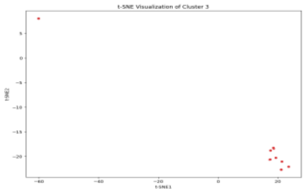

Fig. 11 t-SNE K-Means Cluster 3
Sources: Researcher Property

Comparison with Autoencoder: t-SNE is also applied to visualize the clustering results of Autoencoder (Figure 12-14). This comparison highlights the differences in cluster separability and interpretability between the two methods, with K-Means showing clearer distinctions.

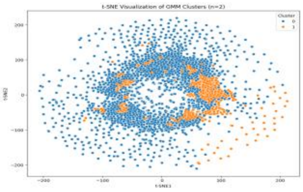

Fig. 12 t-SNE Autoencoder
Sources: Researcher Property

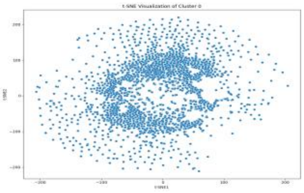

Fig. 13 t-SNE Autoencoder Cluster 0
Researcher Property

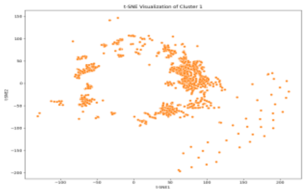

Fig. 14 t-SNE Autoencoder Cluster 1
Sources: Researcher Property

DISCUSSIONS

While numerous methodologies can be employed to detect fraud, this study evaluates the application of K-Means clustering and t-SNE visualization to identify fraudulent activities in mobile recharge transactions. The findings confirm the effectiveness of K-Means in clustering large datasets and identifying patterns that deviate from typical behaviours. These deviations, often indicative of fraudulent activities (Jiang et al., 2023), establish a solid foundation for anomaly detection and transactional analysis. The comparative analysis revealed that K-Means consistently produced well-defined clusters with high Silhouette Scores and low Davies-Bouldin Index values, indicating compact, clearly separated groups. This makes K-Means not only computationally efficient but also interpretable, which is essential for identifying actionable insights in real-world scenarios. While Autoencoders demonstrated potential in handling high-dimensional datasets, their results lacked the interpretability and clarity achieved with K-Means. The t-SNE visualization of Autoencoder-based clusters revealed less distinct separations, making it challenging to derive actionable insights. Conversely, K-Means combined with t-SNE provided clearer, well-defined clusters, making the interpretation of transactional behaviours more intuitive and reliable.

The integration of t-SNE visualization with K-Means clustering significantly enhanced the interpretability of high-dimensional data. By projecting the data into a lower-dimensional space, t-SNE enabled the identification of subtle patterns and anomalies that might have been overlooked in purely numerical analysis (Rezapour, 2019). This combination proved highly effective in balancing computational efficiency, accuracy, and clarity, addressing the inherent complexity and size of the dataset. Although methods such as Autoencoders and DBSCAN hold value in other contexts, they were less suitable for this study, which prioritized practical, interpretable, and scalable techniques for detecting fraudulent behaviours in mobile recharge systems.

The evaluation of the two clustering methods, **K-Means** and **Autoencoder**, highlighted the strengths of K-Means in analysing this dataset. The results provided clear evidence that K-Means outperformed Autoencoder in identifying meaningful patterns and anomalies, particularly in the context of fraud detection. **Higher Silhouette Scores:** K-Means consistently achieved higher Silhouette Scores, indicating that its clusters were well-defined and exhibited clear boundaries. This suggests that transactions within each cluster were closely related, while being distinctly separated from other clusters. Such clarity is essential for distinguishing normal transactional patterns from potentially fraudulent activities (Josyula, 2023). **Lower Davies-Bouldin Index (DBI):** The lower DBI values achieved by K-Means confirmed the compactness and separation of its clusters. This metric underscores the interpretability and reliability of the clustering results, which is crucial for drawing actionable insights in fraud detection (Cho S., 2023). The execution of Autoencoders consumed substantially more computational resources, requiring approximately five times the runtime of K-Means for the same dataset in this study. This resource intensity poses limitations for scalability and real-time implementation, especially in environments where rapid anomaly detection is critical.

Based on these findings, **K-Means** emerged as the most suitable clustering method for this study. Its ability to consistently deliver higher-quality clustering results demonstrates its robustness and practicality for analysing complex transactional datasets. Clusters identified through K-Means revealed meaningful insights into transactional behaviours. Certain clusters displayed extreme values in features such as high nominal amounts, prolonged process times, or frequent errors, all of which were flagged as indicators of potential fraud. Geographic patterns were also analysed by examining the most frequent region IDs associated with anomalous clusters, providing additional context for fraud identification (Matloob et al., 2020). For instance, clusters characterized by moderate but variable transaction values and slower-than-average processing times exhibited a higher likelihood of fraudulent activities. Other clusters, with consistently high transaction values or rapid processing times, further suggested the presence of manipulative or abusive behaviour. A summary of these cluster characteristics and their corresponding fraud potential is detailed in Table 5.

The utility of K-Means was further validated through t-SNE visualization, which offered an intuitive representation of clustering results. Distinct and well-separated clusters reflected unique transactional characteristics, facilitating the identification of deviations from the norm. Patterns indicative of fraud, such as unusually high transaction values or frequent errors, were made visually apparent, supporting the prioritization of these anomalies for further investigation. The interpretability provided by t-SNE, combined with the precision of K-Means clustering, underscores the effectiveness of this approach in detecting fraudulent activities in mobile recharge transactions.

Focusing on K-Means and t-SNE, this research delivers a scalable and interpretable framework for fraud detection. The insights derived from this study demonstrate the practical applicability of these methods, providing service providers with a robust tool to safeguard against financial risks and operational vulnerabilities. Moreover, the research paves the way for the development of enhanced fraud detection strategies that can be adapted to similar domains with large-scale transactional data. By prioritizing clustering and visualization techniques, this research contributes to a scalable, interpretable, and practical framework for detecting fraudulent activities in mobile recharge systems. This approach not only provides actionable insights but also paves the way for more robust fraud detection strategies in similar domains.

Table 5. Fraud Cluster Conclusion

Cluster	**Name**	**Key Characteristics**	**Fraud Potential**
0	Standard Transactions	- Low transaction amounts with minimal variability.	**Low**: Transactions appear standard and consistent, with no significant anomalies.
		- Average processing time: 28 seconds.	
		- Predominantly occurs on Channel Type 1.	
		- Geographically concentrated in Region ID 0.	
1	Diverse Transactions	- Moderate transaction amounts but high variability.	**Moderate**: High variability in transaction amounts and wide geographic distribution may indicate unusual activity.
		- Faster processing time (average: 22 seconds).	
		- Occurs across multiple regions (Region IDs 1, 10, and 3), predominantly on Channel Type 2.	
2	Suspicious Slow Transactions	- Moderate transaction amounts with high variability.	**High**: Slower processing times combined with significant variability may suggest suspicious activity.
		- Slowest processing time (average: 34 seconds).	
		- Found in multiple regions (Region IDs 1, 10, and 3), predominantly on Channel Type 2.	
3	High-Value Transactions	- High transaction amounts with minimal variability.	**Very High**: Consistently high-value transactions may indicate potential manipulation or misuse.
		- Moderate processing time (average: 26 seconds).	
		- Concentrated in Region ID 6 and occurs on Channel Type 2.	

The identification of fraudulent activities relied on the analysis of clusters with extreme values in key transactional features. Clusters characterized by unusually high nominal amounts, prolonged process times, or frequent errors were flagged as potential indicators of fraud. Geographic patterns also played a significant role in this analysis, with the most frequent Region IDs within anomalous clusters offering additional context for identifying suspicious activities.

The clustering process with K-Means produced distinct and well-separated groups, each reflecting unique transactional characteristics. These clusters revealed considerable variations in features such as *Nominal*, *Process Time*, and *Open Error*, enabling the detection of transactions that deviated significantly from established norms. This level of differentiation was instrumental in uncovering potentially fraudulent behaviours.

Certain clusters demonstrated patterns that were strongly indicative of fraud. For instance, transactions with consistently high values, abnormally long processing times, or repeated errors emerged as clear anomalies. The integration of t-SNE visualization further enhanced the interpretability of these findings. By projecting high-dimensional data into a two-dimensional space, t-SNE provided a clear visual representation of the clustering outcomes. This visualization offered a straightforward confirmation of anomalies, aiding in their prioritization for further investigation and enabling service providers to address suspicious activities with greater precision.

The combination of K-Means clustering and t-SNE visualization proved to be a powerful approach, not only in isolating fraudulent patterns but also in providing actionable insights that enhance the overall robustness and reliability of fraud detection frameworks. This synergy underscores the practical value of these methodologies in managing and mitigating risks in mobile recharge systems.

For practical implementation in the industry, K-Means clustering can be effectively integrated into real-time fraud detection systems by leveraging incremental learning to adapt to evolving fraud patterns. Embedding this framework into existing business intelligence tools enhances accessibility and enables intuitive monitoring and analysis of transactional data. Furthermore, refining key features such as transaction value, processing time, and geographic patterns through domain-specific insights ensures greater accuracy and relevance in detecting fraudulent activities. Looking ahead, future research can explore the integration of hybrid models or advanced feature engineering techniques to further enhance detection accuracy and adaptability to evolving fraud patterns. The findings presented here lay a solid foundation for continued innovation in fraud detection systems, offering a clear path for developing more robust and adaptable solutions in this critical domain.

CONCLUSION

This study makes a meaningful contribution to the field of fraud detection in mobile recharge transactions by presenting a robust and practical framework that combines K-Means clustering with t-SNE visualization. The proposed approach addresses critical challenges in fraud detection, including scalability, interpretability, and computational efficiency. By leveraging K-Means' ability to form well-defined and distinct clusters, the framework effectively identifies anomalous patterns indicative of fraudulent activities. The comparative analysis underscores the clear advantages of K-Means over Autoencoders. While Autoencoders excel at reducing dimensionality, their interpretability and computational efficiency are limited, requiring up to five times longer processing times and yielding less actionable results. In contrast, K-Means demonstrated superior performance, achieving higher Silhouette Scores (0.6215) and lower Davies-Bouldin Index values (0.7074). These metrics confirm its ability to produce compact, well-separated clusters that highlight potential fraudulent transactions with clarity and precision. The integration of t-SNE further enhances the interpretability of these results, offering intuitive and visually compelling insights into high-dimensional data that would otherwise be challenging to analyze. By determining the optimal number of clusters using the Knee Locator algorithm, the study ensures a balance between computational efficiency and clustering accuracy. The result—four distinct clusters—provides actionable insights for service providers to identify and address fraudulent behaviors effectively. Notably, clusters characterized by high nominal values, prolonged processing times, and frequent errors were flagged as potential indicators of fraud, offering a practical roadmap for operational improvements. This research not only validates the practicality and effectiveness of K-Means and t-SNE for high-volume transactional datasets but also provides a scalable and interpretable solution that aligns with the operational needs of service providers. By bridging the gap between computational efficiency and real-world applicability, this study delivers a framework that is both academically rigorous and practically impactful.

REFERENCES

Ahmed, M., Seraj, R., & Islam, S. M. S. (2020). The k-means algorithm: A comprehensive survey and performance evaluation. In *Electronics (Switzerland)* (Vol. 9, Issue 8, pp. 1–12). MDPI AG. https://doi.org/10.3390/electronics9081295

Cho S., D. W. , T. B. C. (2023). Fraud Detection in Malaysian Financial Institutions using Data Mining and Machine Learning. *Journal of Information and Technology, 7(1),* 13–21. https://doi.org/10.53819/81018102t4152

Chowdari, B., & Parthiban, S. (2022). Credit Card Fraud Detection using Logistic Regression Compared with t-SNE to Improve Accuracy. *International Journal of Research Publication and Reviews*, 1000–1004. https://doi.org/10.55248/gengpi.2022.3.8.37

Dwi Aulia, D., & Nurahman, N. (2023). Comparison Performance of K-Medoids and K-Means Algorithms In Clustering Community Education Levels. *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, *12*(2), 273–282. https://doi.org/10.23887/janapati.v12i2.59789

Fu, S., Lu, S. Y., Davies, D. L., & Bouldin, D. W. (1977). The string-to-string correction problem. In *J. Ass. Comput. Mach* (Vol. 1, Issue 2).

Goh, C. H., Wong, K. K., Tan, M. P., Ng, S. C., Chuah, Y. D., & Kwan, B. H. (2022). Development of an effective clustering algorithm for older fallers. *PLoS ONE*, *17*(11 November). https://doi.org/10.1371/journal.pone.0277966

Hanae, A., Abdellah, B., Saida, E., & Youssef, G. (n.d.). End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 14, Issue 6). www.ijacsa.thesai.org

Huang, Z., Zheng, H., Li, C., & Che, C. (2024). Application of Machine Learning-Based K-means Clustering for Financial Fraud Detection. In *Academic Journal of Science and Technology* (Vol. 10, Issue 1).

Ikeda, C., Ouazzane, K., Yu, Q., & Hubenova, S. (n.d.). New Feature Engineering Framework for Deep Learning in Financial Fraud Detection. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Issue 12). www.ijacsa.thesai.org

Jiang, S., Dong, R., Wang, J., & Xia, M. (2023). Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network. *Systems*, *11*(6). https://doi.org/10.3390/systems11060305

Josyula, H. P. (2023). *Fraud Detection in Fintech Leveraging Machine Learning and Behavioral Analytics*. https://doi.org/10.21203/rs.3.rs-3548343/v1

Matloob, I., Khan, S. A., & Rahman, H. U. (2020). Sequence Mining and Prediction-Based Healthcare Fraud Detection Methodology. *IEEE Access*, *8*, 143256–143273. https://doi.org/10.1109/ACCESS.2020.3013962

Murena, P.-A., Sublime, J., Matei, B., & Cornuéjols, A. (2018). *An Information Theory based Approach to Multisource Clustering*.

Pumsirirat, A., & Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 9, Issue 1). www.ijacsa.thesai.org

Rezapour, M. (2019). Anomaly Detection using Unsupervised Methods: Credit Card Fraud Case Study. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 10, Issue 11). www.ijacsa.thesai.org

Rousseeuw, P. J. (1987). Silhouet tes: a graphic al aid to the interpre tation and validati on of cluster analysis. In *Journal of Computational and Applied Mathematics* (Vol. 20).

Sari, P. O. C., & Suharjito, S. (2022). Outlier Detection in Inpatient Claims Using DBSCAN and K-Means. *JURNAL TEKNIK INFORMATIKA*, *15*(1), 1–10. https://doi.org/10.15408/jti.v15i1.25682

Setiawan, R., Tjahjono, B., Firmansyah, G., & Akbar, H. (n.d.). Fraud Detection In Credit Card Transactions Using HDBSCAN, UMAP And SMOTE Methods. In *International Journal of Science*. http://ijstm.inarah.co.id1333

Tran, L., Tran, T., & Mai, A. (2019). Solve fraud detection problem by using graph based learning methods. *Journal of Engineering and Science Research*, *3*(4), 2289–7127. https://doi.org/10.26666/rmp.jesr.2019.6.4

Wu, T., & Wang, Y. (2021). *Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection*. http://arxiv.org/abs/2108.02501

Zhou, H., Sun, G., Fu, S., Jiang, W., & Xue, J. (2019). A scalable approach for fraud detection in online e-commerce transactions with big data analytics. *Computers, Materials and Continua*, *60*(1), 179–192. https://doi.org/10.32604/cmc.2019.05214