Anomaly Analysis of Debit Payment Transactions in Switching Companies Using Naive Bayes, K-Nearest Neighbors, and Decision Tree Methods in Orange Data Mining

RP Fiki Wisnu Subekti[1], Agung Budi Susanto[2*], Arya Adhyaksa Waskita[3]
Graduate Program of Informatics Engineering, Universitas Pamulang
Jalan Raya Puspitek, Buaran, Kota Tangerang Selatan, Banten 15310
Email: fikiwisnu90@gmail.com[1], dosen02680@unpam.ac.id[2], dosen02104@unpam.ac.id[3]

In the digital era, the rapid growth of electronic payment transactions using debit cards has been accompanied by an increasing risk of anomalies and fraudulent activities. Identifying suspicious transactions has become crucial to ensure system security and maintain user trust. The high volume of transactions processed through switching systems in Indonesia poses significant challenges for operational teams in detecting anomalous patterns effectively. This study aims to identify anomalous debit payment transactions within switching networks by comparing three classification methods, namely Naive Bayes, K-Nearest Neighbors (K-NN), and Decision Tree. The dataset used consists of sampled daily transaction data obtained from operational monitoring, which is analyzed based on predefined transaction matrices developed by operational teams as indicators of anomaly detection. The evaluation of model performance is conducted using key metrics, including accuracy, precision, and recall, to determine the most effective classification method. The results show that machine learning-based classification significantly improves the accuracy and efficiency of anomaly detection compared to manual analysis. Furthermore, the integration of data mining techniques with operational transaction matrices provides a structured and practical approach for early anomaly identification. This approach not only enhances the effectiveness of transaction monitoring but also strengthens fraud prevention mechanisms and supports more informed and data-driven decision-making processes within switching companies.

Keywords: Transaction Anomaly, Fraud Detection, Debit Payment, Switching System, Data Mining.

Corresponding Author:
Agung Budi Susanto
Graduate Program of Informatics Engineering, Universitas Pamulang
Jalan Raya Puspitek), Buaran, Kota Tangerang Selatan, Banten 15310
dosen02680@unpam.ac.id

1. Introduction

The rapid advancement of technology in payment integration and internet accessibility has significantly transformed the way individuals conduct transactions and daily activities. Along with these developments, the payment system in Indonesia has also evolved considerably. A payment system can be defined as a set of rules, institutions, and mechanisms used to transfer funds in order to fulfill financial obligations arising from economic activities. Broadly, payment systems are categorized into two main types, namely cash payment systems and non-cash payment systems.

A cash payment system relies on physical currency as its primary medium of exchange, where transactions are carried out through the direct transfer of banknotes or coins from the payer to the recipient. In contrast, a non-cash payment system utilizes instruments other than physical money to transfer value between parties. These transactions are conducted without the use of tangible currency, instead relying on electronic or paper-based mechanisms. Non-cash payment instruments include card-based payments and electronic money. Card-based payment instruments encompass credit

cards, Automated Teller Machine (ATM) cards, and debit cards, while electronic money can be stored either in server-based systems or chip/card-based media.

One of the most rapidly growing forms of non-cash payment is electronic or digital-based transactions. These include electronic money (e-wallets or server-based systems), transactions through Electronic Data Capture (EDC) machines, mobile banking, internet banking, and QRIS (Quick Response Code Indonesian Standard). The increasing adoption of electronic money as part of the payment system indicates a continuous upward trend in digital transaction usage. This growth reflects the expanding role of electronic payment instruments in facilitating efficient, secure, and convenient financial transactions over time.

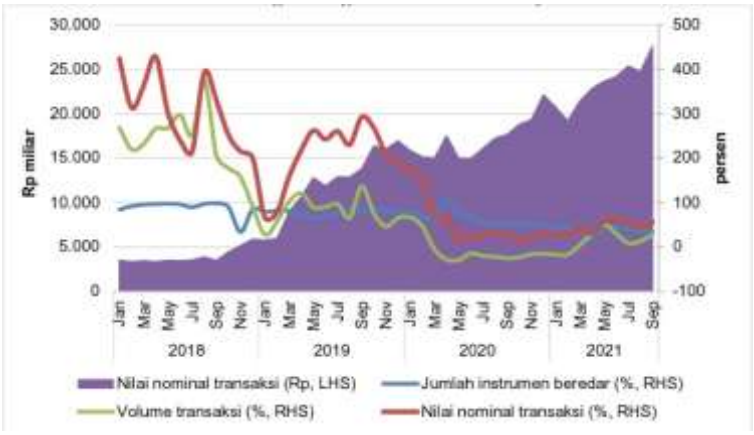


Figure 1. Development of Electronic Money (Bank Indonesia Website, 2021)

The fundamental characteristics of electronic or digital-based payment systems lie in their reliance on intermediaries, such as banks or other financial institutions, the necessity of technological infrastructure, and their flexibility to accommodate transactions of varying values, ranging from small to large amounts. One of the most widely used forms of such transactions is debit-based payment through Electronic Data Capture (EDC) devices. EDC refers to an electronic system that enables merchants to accept payments without the use of physical cash, commonly found at cashier counters in retail stores, restaurants, and various business establishments. These devices are provided by banks or payment service providers to facilitate the processing of non-cash electronic transactions.

Functionally, EDC devices operate by capturing card data through magnetic swipe, chip insertion, or contactless technologies such as Near Field Communication (NFC). The transaction data is then transmitted in real time to the issuing bank's server for verification and authorization. Once approved, the system automatically completes the payment by transferring funds from the customer's account to the merchant's account, while simultaneously generating a receipt as proof of transaction. Modern EDC systems are capable of supporting multiple non-cash payment instruments, including debit cards, credit cards, electronic money cards such as BRIZZI, Flazz, and e-Money, as well as QRIS (Quick Response Code Indonesian Standard), which is increasingly integrated into newer EDC platforms.

The utilization of EDC technology offers several operational advantages, particularly in enhancing transaction efficiency, improving security, and simplifying financial record-keeping. Transactions can be completed more quickly as cash handling and change calculation are no longer required, thereby reducing service time and increasing customer throughput. Additionally, the reduced reliance on physical cash minimizes the risk of theft, while the automatic digital recording of transactions facilitates more accurate and efficient bookkeeping processes.

The growing preference for non-cash transactions, driven by convenience and efficiency, has resulted in a significant increase in daily transaction volumes processed through switching companies,

particularly via debit channels. As highlighted by Riskiyadi, Anggono, and Tarjo (2021), the interconnectivity between banks and financial technology platforms has further accelerated transaction flows across multiple payment channels. However, the massive volume of transactions processed through switching systems in Indonesia also introduces potential risks, including opportunities for fraudulent activities. According to Rio Vernika Putra (2021), anomalies in banking transactions are often associated with various forms of financial crimes, including criminal, civil, and corruption-related offenses, given the inherent vulnerability of banking institutions to misuse of authority.

Furthermore, the evolution of debit payment technology continues to advance alongside the transformation of EDC devices from conventional machines into Android-based Mobile Point of Sale (MPOS) systems that offer greater efficiency and flexibility. The seamless integration between EDC devices and banking systems enables faster and more secure transaction processing, thereby enhancing digital literacy and promoting the adoption of safe, efficient, and accurate non-cash payment methods among both businesses and consumers. By reducing transaction time and operational complexity, EDC systems allow merchants to serve more customers within shorter periods, while providing consumers with convenient payment options. Consequently, debit card transactions have become one of the most dominant forms of payment, as evidenced by data from the Indonesian Payment System Association (ASPI), which indicates a consistent annual increase in debit transaction volumes.

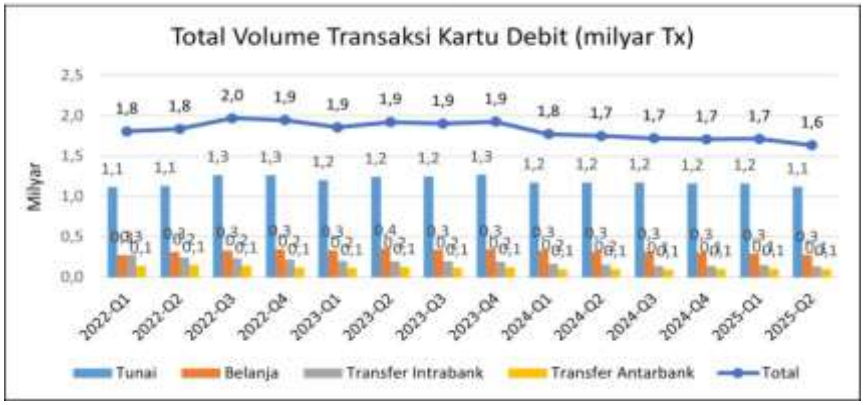


Figure 2. Recording of Total Debit Transaction Volume (ASPI Website, 2025)

In addition to Electronic Data Capture transactions, debit card usage is also widely applied in fund transfer activities, both within the same bank and between different banks. The demand for interbank transfers continues to increase in line with the growing interconnectivity of switching companies in Indonesia. Debit card-based transfers are particularly convenient for users, as they can be easily conducted through Automated Teller Machines available in various locations.

The advancement of interoperability and interconnectivity within the payment system has significantly facilitated non-cash transactions for the public. This development has contributed to the steady growth of interbank transfer transactions, as supported by data from the Indonesian Payment System Association, which indicates a consistent increase in transaction volume over time.

Figure 3. Types of Debit Card Transactions

The figure illustrates the percentage distribution of debit card transaction types over time, including cash withdrawals, purchase transactions, intrabank transfers, and interbank transfers. It shows that transaction patterns have evolved gradually, with a noticeable shift from cash-based activities toward non-cash transactions such as transfers and purchases. This trend reflects the increasing adoption of digital payment systems and the growing preference for electronic transactions among users. Building upon this distribution, table 1 further presents the percentage growth of debit card transactions, providing a more comprehensive view of the overall increase in transaction activity over time.

Table 1. Percentage Increase in Debit Card Transactions

Period	Cash	Purchases	Intrabank Transfer	Interbank Transfer
2013	44.09%	3.87%	39.70%	12.34%
2014	43.21%	4.06%	38.36%	14.36%
2015	42.89%	4.30%	37.72%	15.09%
2016	41.85%	4.48%	37.72%	15.96%
2017	40.79%	4.62%	37.38%	17.22%
2018	40.96%	4.23%	37.34%	17.46%
2019	42.87%	4.45%	35.44%	17.24%
2020	43.24%	4.12%	35.50%	17.14%
2021	40.95%	4.38%	37.34%	17.34%

Payment interconnection within switching companies refers to an integrated network mechanism that links multiple switching institutions with one another, while simultaneously connecting them to all participating banks (card issuers) and payment channels such as ATMs, Electronic Data Capture (EDC) devices, and QRIS (Quick Response Code Indonesian Standard). The primary objective of this interconnection is to establish a unified payment ecosystem that enables seamless transaction processing across different banks and networks.

Within this ecosystem, switching institutions serve as the core component of non-cash transaction processing, acting as central hubs that facilitate the exchange of transaction data among various stakeholders. These stakeholders include several key entities. First, the National Payment Gateway (GPN), an institution designated by Bank Indonesia, ensures interconnectivity, interoperability, and the smooth execution of domestic transaction processing. Second, switching companies themselves function as the backbone of the payment network, enabling transactions across different banks and payment channels. Third, service institutions are responsible for managing operational processes such as reconciliation, clearing, and settlement of interbank transactions. Fourth, standard institutions play

a critical role in developing and maintaining technical and security standards for payment instruments and infrastructures to ensure system compatibility and reliability.

Furthermore, Bank Indonesia acts as the regulator, supervisor, and primary facilitator of the national payment system by establishing policies—such as the GPN framework—to ensure that the payment system operates in a secure, efficient, and reliable manner. In addition, issuer banks are responsible for providing payment instruments and maintaining customer accounts, while acquirer banks facilitate transaction acceptance by providing infrastructure such as EDC machines and ATM networks in collaboration with merchants. Merchants themselves serve as business entities that accept non-cash payments, while consumers or end-users utilize payment instruments such as cards or e-wallets to conduct transactions.

Despite the advanced interconnectivity within the switching industry in Indonesia, there remains a critical need for an efficient analytical mechanism to validate and monitor interconnection-based transactions. Traditionally, transaction validation processes rely heavily on human intervention, requiring substantial time and labor resources to ensure transaction accuracy and legitimacy. However, given the operational limitations, including time constraints and the inherent role of switching institutions as transaction intermediaries, there is an increasing demand for automated systems capable of identifying suspicious or potentially fraudulent transactions.

Therefore, the switching industry requires a reliable analytical framework that can effectively monitor, evaluate, and validate transaction data across multiple payment channels, including debit cards, mobile banking, and QRIS. This study specifically focuses on debit card transactions conducted through ATM and EDC channels, as these represent a significant portion of daily transaction volumes. The massive scale of transactions processed on a daily basis necessitates the development of efficient analytical methods that can support operational reporting while simultaneously enhancing the detection of anomalous transaction patterns.

2. Literature Review and Problem Statement

Literature Review

The rapid growth of digital financial transactions has significantly increased the complexity of monitoring and securing payment systems, particularly within interbank switching networks. The proliferation of non-cash transactions, especially debit-based payments, has introduced new challenges in detecting anomalous and fraudulent activities in real time. Consequently, the application of data mining and machine learning techniques has become increasingly relevant in addressing these challenges.

Previous studies have demonstrated the effectiveness of machine learning algorithms in fraud detection within financial systems. Research by Adong Purba (2021) highlights that algorithms such as Random Forest, Logistic Regression, and Support Vector Machine (SVM) provide high performance in detecting fraudulent e-channel transactions, emphasizing the importance of preprocessing and feature selection in improving model accuracy. Similarly, Rangga Aditya Putra (2024) found that machine learning models, including Decision Tree and SVM, enhance the reliability and security of online financial transactions by identifying abnormal patterns within large datasets.

In the context of credit card fraud detection, Arief Kurniawan and Yulianingsih (2021) demonstrated that the Random Forest algorithm achieved an accuracy level of 0.85, indicating strong predictive capability. Furthermore, deep learning approaches, as discussed by Faried Zamachsari and Niken

Puspitasari (2021), have shown superior performance, with accuracy exceeding 99%, although such models often require more complex computational resources. These findings suggest that while advanced models offer high accuracy, simpler classification algorithms may still be relevant depending on operational constraints.

Several comparative studies have also evaluated the performance of classification algorithms such as Naive Bayes, K-Nearest Neighbors (K-NN), and Decision Tree. Hozairi et al. (2021) reported that Naive Bayes achieved the highest accuracy (89%) compared to K-NN and Decision Tree in student classification tasks. Conversely, other studies, such as Nandito Marbun and Jarot Prianggono (2025), found that K-NN outperformed Naive Bayes in crime classification scenarios, particularly in terms of precision and recall. Meanwhile, research by Adhitya Prayoga Permana et al. (2021) indicated that Decision Tree could outperform both Naive Bayes and K-NN in certain predictive contexts, demonstrating that algorithm performance is highly dependent on data characteristics and problem domains.

In anomaly detection, alternative approaches such as Isolation Forest have also been explored. I Made Sudarsana Taksa Wibawa and Anak Agung Istri Ngurah Eka Karyawati (2023) showed that Isolation Forest effectively identified anomalies in transaction datasets, supported by exploratory data analysis (EDA) to improve feature relevance. However, most existing studies focus on credit card transactions or general financial fraud, with limited attention given specifically to debit payment transactions within switching environments.

Moreover, prior research emphasizes that fraud detection should not rely solely on accuracy but must also consider precision and recall, as highlighted by Zamachsari and Puspitasari (2021). This is particularly important in financial systems where false positives and false negatives can have significant operational and financial consequences. Despite these advancements, the application of machine learning techniques in switching-based debit transaction environments remains underexplored, particularly in integrating operational transaction matrices as indicators for anomaly detection.

Based on the reviewed literature, it can be observed that while numerous studies have investigated fraud detection using various machine learning algorithms, there is still a research gap in the application of comparative classification methods—specifically Naive Bayes, K-Nearest Neighbors, and Decision Tree—within the context of debit payment transactions in switching companies. Additionally, the incorporation of operational transaction matrices as anomaly indicators represents a novel contribution that has not been extensively addressed in previous studies.

Problem Statement

The increasing volume of non-cash transactions, particularly debit payment transactions processed through switching systems, has created significant challenges for financial institutions in ensuring transaction security and reliability. The interconnection of multiple banks and payment channels within switching networks results in a highly complex transaction environment, where large volumes of data must be processed and monitored continuously.

Currently, the process of identifying anomalous or suspicious transactions within switching companies largely relies on manual analysis conducted by operational personnel. This approach is not only time-consuming but also inefficient, given the massive scale of daily transaction data. The reliance on human intervention introduces limitations in terms of speed, consistency, and accuracy, which may lead to delays in detecting fraudulent activities and increase potential financial risks.

Furthermore, there is a lack of standardized analytical frameworks or models that can systematically classify and detect anomalous debit transactions based on predefined transaction patterns or matrices. Although switching institutions play a critical role in facilitating interbank transactions, their operational function is primarily limited to routing transactions, rather than actively analyzing transaction anomalies. As a result, there is a growing need for an automated and reliable analytical system that can support real-time transaction validation and anomaly detection.

Another key issue is the absence of comparative evaluation of classification algorithms specifically applied to debit transaction data within switching environments. While previous studies have explored various machine learning methods in fraud detection, there is limited empirical evidence regarding which algorithm provides the best performance in this specific context. Without such comparative analysis, it is difficult for organizations to determine the most effective method for implementation.

In addition, the lack of integration between operational transaction indicators and machine learning models further limits the effectiveness of anomaly detection systems. Transaction matrices developed by operational teams have not been optimally utilized as structured input for predictive modeling, resulting in missed opportunities to enhance detection accuracy and decision-making processes.

Therefore, this study seeks to address these gaps by developing and comparing classification models using Naive Bayes, K-Nearest Neighbors, and Decision Tree algorithms to identify anomalous debit payment transactions within switching companies. By integrating transaction matrix indicators into the data mining process, this research aims to provide a more efficient, accurate, and scalable solution for anomaly detection, thereby supporting operational decision-making and improving the overall security of digital payment systems.

3. Methods

This study employs a quantitative research approach with a data mining classification framework to identify anomalous debit payment transactions within switching companies. The research is designed to compare the performance of three widely used classification algorithms, namely Naive Bayes, K-Nearest Neighbors (K-NN), and Decision Tree, in detecting transaction anomalies based on operational transaction patterns. The analysis is conducted using Orange Data Mining software, which enables systematic model development, visualization, and evaluation within a unified environment.

The data utilized in this study consists of daily debit transaction records obtained from the operational monitoring unit. These transactions represent interconnection-based payment activities processed through switching systems, including ATM and EDC channels. The dataset covers a one-month observation period with an average of approximately 1,000 transactions per day, ensuring sufficient data volume for classification modeling. Each transaction record contains several key attributes that are relevant for anomaly detection, as presented in Table 2.

Table 2. Structure of Transaction Dataset

No	Attribute Name	Description
1	Card Number	Unique identifier of the debit card
2	Transaction Amount	Value of the transaction
3	Transaction Time	Timestamp of transaction
4	Transaction Channel	Channel used (ATM/EDC)
5	Label	Anomaly or Non-Anomaly classification

Prior to model development, the dataset undergoes a preprocessing stage to ensure data quality and analytical readiness. This stage includes data cleaning to eliminate incomplete or inconsistent records,

transformation of variables into appropriate formats, and labeling of transactions based on predefined operational criteria. The labeling process plays a crucial role in this research, as it relies on transaction pattern matrices developed by the operational team to distinguish between normal and anomalous transactions.

The classification framework in this study is guided by three transaction matrices, namely N1, N2, and N3, which represent different levels of transaction behavior. These matrices serve as practical indicators for anomaly identification and are integrated into the data mining process as classification references. The conceptual representation of these matrices is shown in Table 3.

Table 3. Transaction Pattern Matrix

Matrix	Description	Interpretation
N1	Normal Anomaly Pattern	Transactions follow standard anomaly patterns
N2	Moderate Deviation	Transactions show slight irregularities
N3	High Anomaly Pattern	Transactions indicate strong anomaly signals

Following preprocessing, the study proceeds to the model development stage, where three classification algorithms are implemented and trained using the same dataset. The selection of Naive Bayes, K-Nearest Neighbors, and Decision Tree is based on their representativeness in probabilistic, instance-based, and rule-based learning approaches, respectively. This allows for a comprehensive comparison of classification performance across different algorithmic paradigms.

To ensure the validity of the evaluation process, the dataset is divided into training and testing subsets. The training data is used to build the classification models, while the testing data is utilized to assess their predictive performance. The proportion of data distribution applied in this study is presented in Table 4.

Table 4. Data Partitioning

Dataset Type	Proportion	Function
Training Data	70%	Model development
Testing Data	30%	Model validation

The performance of each classification model is evaluated using standard performance metrics, including accuracy, precision, and recall. These metrics are essential in assessing the effectiveness of anomaly detection, particularly in distinguishing between true anomalies and normal transactions. In addition, the use of a confusion matrix provides a more detailed evaluation of classification outcomes by illustrating the relationship between predicted and actual classes. The evaluation framework applied in this study is summarized in Table 5.

Table 5. Evaluation Metrics

Metric	Description
Accuracy	Overall correctness of classification results
Precision	Proportion of correctly predicted anomalies
Recall	Ability to identify all actual anomaly transactions

While accuracy, precision, and recall provide a comprehensive overview of the overall classification performance, these aggregated metrics alone are not sufficient to fully capture the detailed behavior of the model in distinguishing between anomalous and normal transactions. Therefore, to obtain a deeper and more granular understanding of the classification results, it is necessary to analyze the confusion matrix. This matrix presents the distribution of prediction outcomes by comparing actual and predicted classes, thereby enabling the identification of correct and incorrect classifications. Through this approach, the strengths and weaknesses of the model—particularly in terms of detecting

anomalies and minimizing misclassification—can be evaluated more precisely, as illustrated in Table 6.

Table 6. Confusion Matrix Structure

	Predicted Anomaly	Predicted Normal
Actual Anomaly	True Positive	False Negative
Actual Normal	False Positive	True Negative

Through this methodological framework, the study aims to identify the most effective classification algorithm for detecting anomalous debit transactions within switching systems. The integration of operational transaction matrices with machine learning techniques represents a practical and data-driven approach that not only enhances detection accuracy but also supports operational decision-making processes. Furthermore, this methodology contributes to improving the efficiency and reliability of transaction monitoring systems in the increasingly complex digital payment ecosystem.

4. Result and Discussion

Data Acquisition

The data used in this study were obtained from debit transaction records within a switching company. The dataset consists of daily transaction data from various merchants processed through the switching network. The data were extracted from the database, containing debit transaction fields collected over a one-day period.

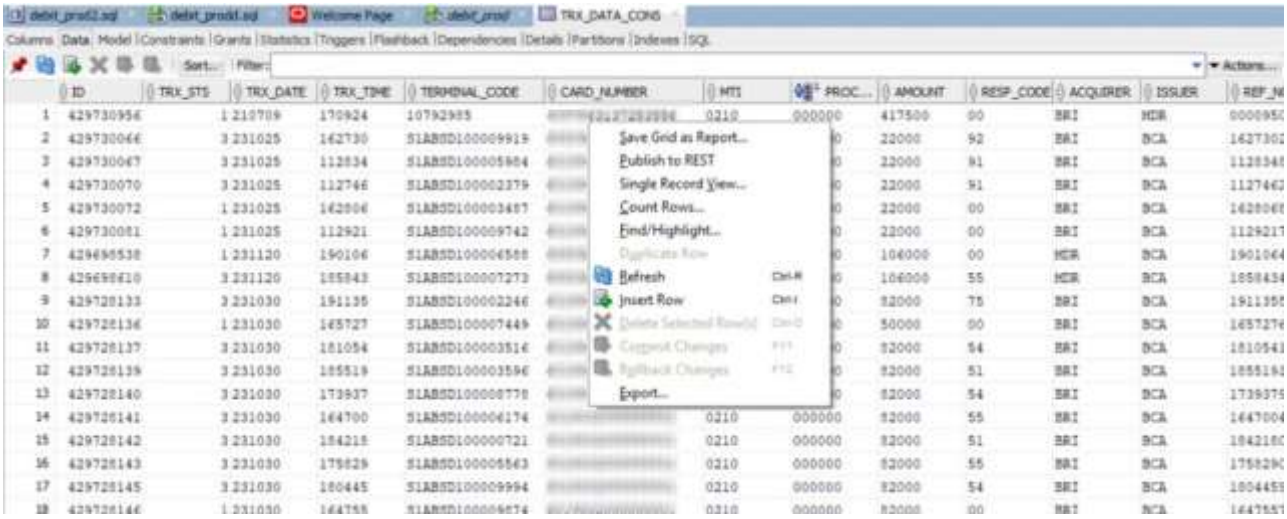


Figure 4. Database Data Display

Data extraction was performed from the database tables to obtain the data required for this study. The following shows the structure of the database fields used in this research:

Figure 5. Database Field Display

The data were extracted and exported to an Excel file to facilitate data processing in the Orange Data Mining application. The process involved filtering, searching, and sorting relevant transaction data.

The database stores all transactions processed through the switching company; however, this study focuses only on debit payment transactions. Data were retrieved from the trx_data_cons table by selecting the required fields, followed by the export process as illustrated below.

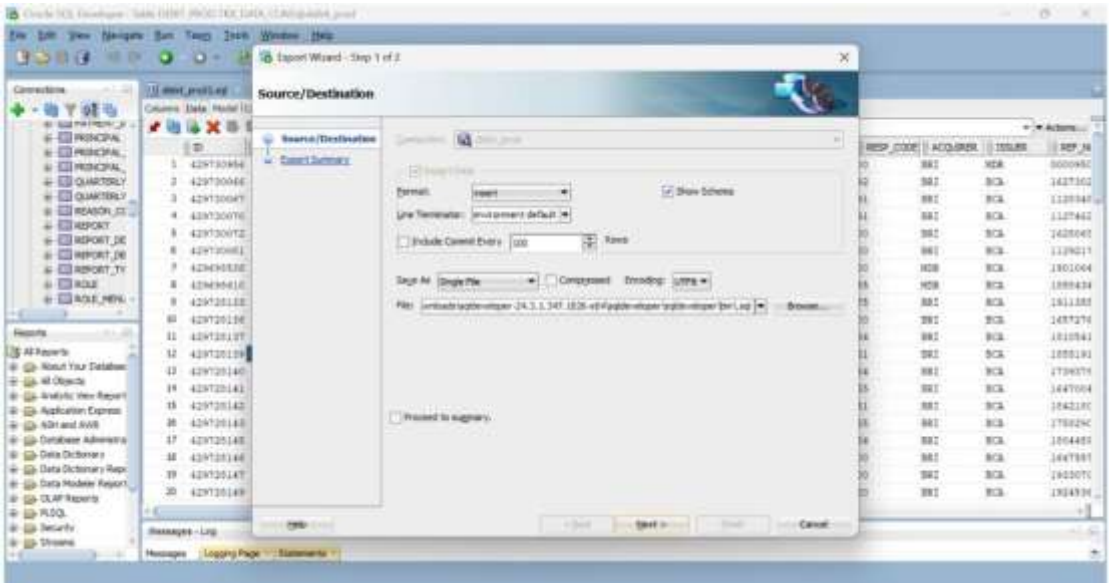


Figure 6. Database Data Extraction Process

The data extraction process was then completed, and the data were successfully converted into an Excel file format.

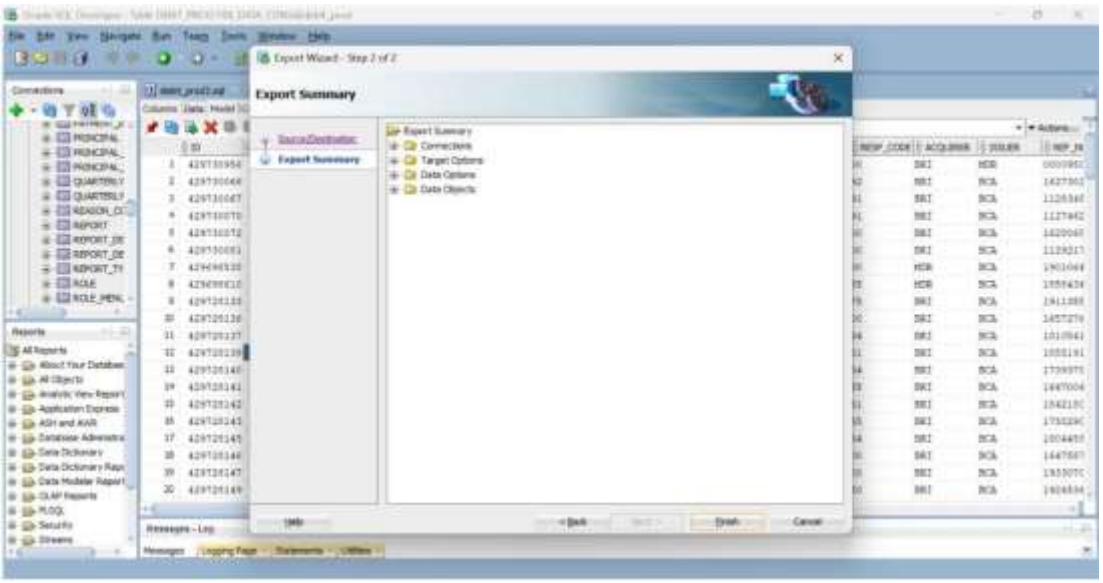


Figure 7. Data Extraction Process Completed

The following presents the dataset of debit payment transactions over one day used in this study (sample of debit transaction data):

Table 7. Debit Transaction Data

ID	Channel	Transaction Date	Transaction Time	Amount	Response Code	Acquirer	Issuer	Merchant Information
5.84E+08	Debit	240801	19:49:16	229,500	0	ALT	MDR	Ramen Ya, Lippo Mall,

ID	Channel	Transaction Date	Transaction Time	Amount	Response Code	Acquirer	Issuer	Merchant Information
								West Jakarta, ID 62
5.84E+08	Debit	240801	21:06:23	13,000	0	BNI	MDR	Cinepolis Citimall, ID
5.21E+08	Debit	240801	21:06:26	100,000	0	ALT	MDR	Gas Station 34.10205, Central Jakarta, ID 62
5.21E+08	Debit	240801	21:06:26	56,000	0	ALT	MDR	Gas Station 34.10205, Central Jakarta, ID 62
5.21E+08	Debit	240801	21:06:26	700,000	0	ALT	MDR	Gas Station 34.10205, Central Jakarta, ID 62
5.21E+08	Debit	240801	21:06:26	400,000	0	ALT	MDR	Gas Station 34.10205, Central Jakarta, ID 62
5.21E+08	Debit	240801	21:06:26	550,000	0	ALT	MDR	Gas Station 34.10205, Central Jakarta, ID 62
5.84E+08	Debit	240801	20:44:56	250,000	0	ALT	MDR	SRC Ucok-HO, East Jakarta, ID 62
5.84E+08	Debit	240801	20:55:19	1,858,300	0	RTS	MDR	ACE Hardware SCP, Samarinda, ID
5.84E+08	QR	240801	19:31:43	945,000	0	ALT	MDR	Annisa Salon & Spa-HO, Bekasi, ID 62

Description of Debit Transaction Data

1. ID
   A unique identifier used to distinguish each transaction record in the database.
2. Channel
   The transaction channel that connects the sender and receiver within the payment system.
3. Trx_date
   The date on which the transaction occurred and was validated in the system.
4. Trx_time
   The specific time when the transaction occurred, used for tracking, auditing, and reconciliation purposes.
5. Amount
   The monetary value of the debit transaction, indicating the amount charged or transferred.
6. Resp_Code
   A response code indicating the transaction status (e.g., success, failure, or suspected anomaly).

7. ACQ (Acquirer)
   The financial institution responsible for processing the transaction from the terminal side.
8. ISS (Issuer)
   The financial institution that issued the debit card and verifies transaction authorization.
9. Info_merchant
   Information about the merchant where the transaction occurred, including name, location, or identifier, used for tracking and audit purposes.

Model Implementation

Data Processing in the System

The initial step in this study is data labeling, which is performed automatically within the system to handle large volumes of data efficiently. Transactions are classified into anomalous and non-anomalous categories based on predefined matrix parameters aligned with the company's operational requirements.

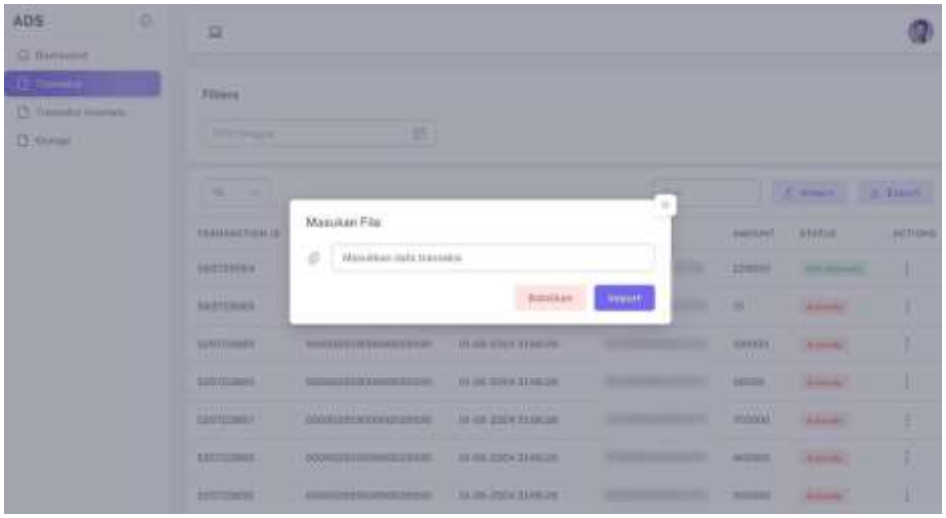


Figure 8. Data Labeling Process

The processed database data are imported into the system for labeling. The data are then classified into two categories: anomalous and non-anomalous transactions. After processing, the system generates labeled output data as illustrated in the following figure.

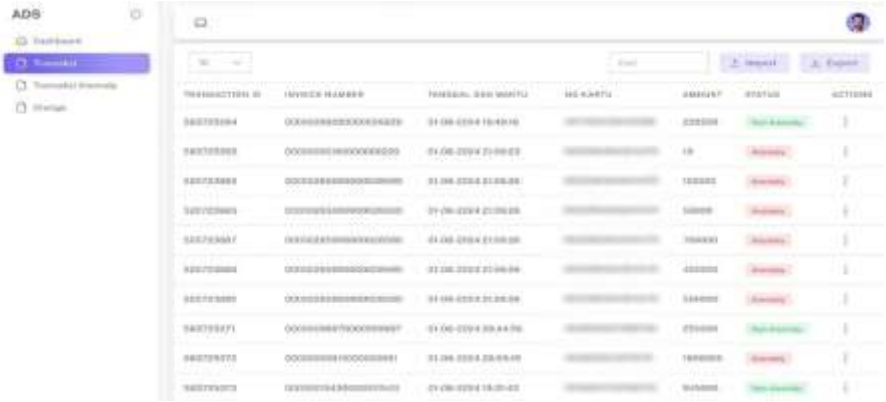


Figure 9. Labeled Data

The labeled data are then further processed using the Orange Data Mining application

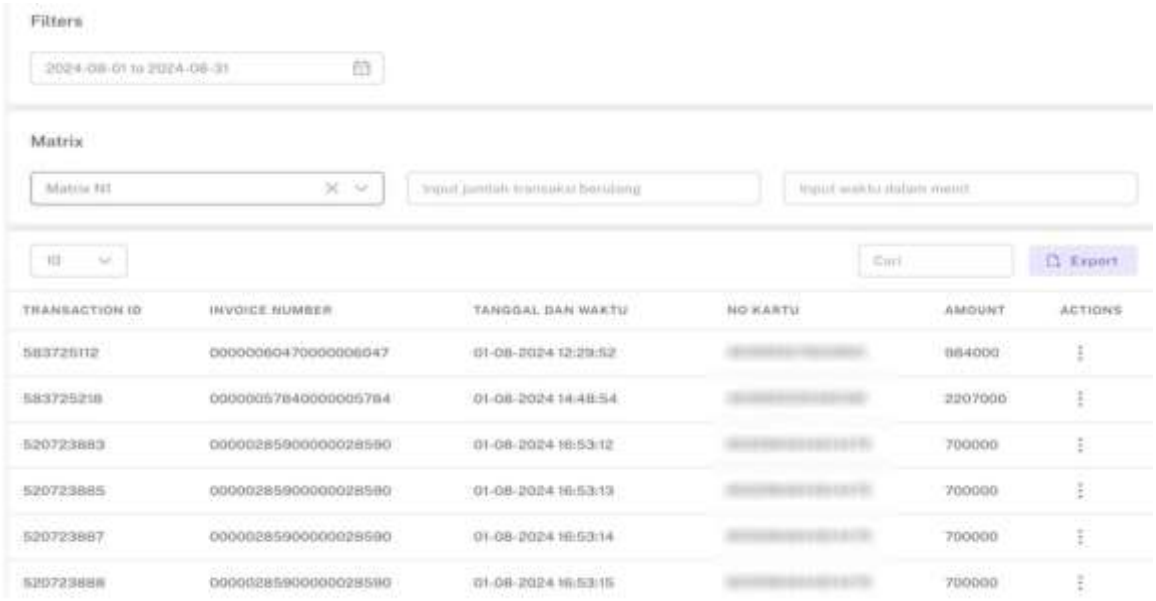


Figure 10. Matrix Data Labeling (N1)

Data Processing in Orange Data Mining

The next step involves classifying the data using the Orange Data Mining application. Given the large dataset, classification is performed to identify anomalous transactions based on predefined matrix parameter attributes. The following are the matrix parameters used in the classification process:

Table 8. Initial Attribute Matrix

Matrix	Attribute Description
N1	A card number performs 5 repeated transactions within 5 minutes
N2	A card number performs 3 transactions exceeding 25 million during unusual hours (00:00–06:00)
N3	A card number performs 5 repeated transactions at the same time

The classification model is tested using the Naive Bayes Classifier, K-Nearest Neighbors, and Decision Tree algorithms. The following shows the data testing and data training widgets in the Orange Data Mining application.

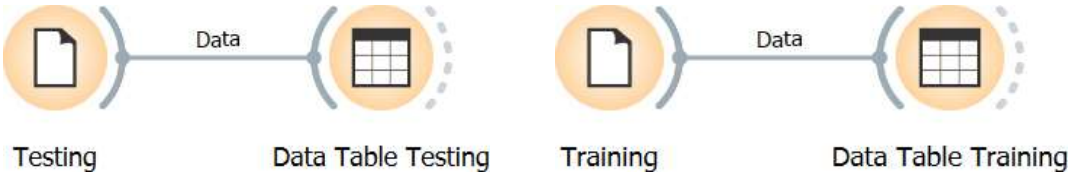


Figure 11. Data Testing in Orange and Data Training in Orange

The initial process involves inputting the testing and training data. The following shows the display of testing data in the Orange application:

Table 9. Sample Testing Data in Orange

No	Terminal Code	Merchant Information	ID	Channel	Transaction Date
1	D0462179	Ramen Ya Lippo Mall	5.84E+08	Debit	240801
2	9022512	Cinepolis Citimall	5.84E+08	Debit	240801
3	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801
4	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801
5	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801

No	Terminal Code	Merchant Information	ID	Channel	Transaction Date
6	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801
7	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801
8	D0AU0815	SRC Ucok-HO	5.84E+08	Debit	240801
9	W0722201	ACE Hardware	5.84E+08	Debit	240801
10	D2960618	Annisa Salon	5.84E+08	Debit	240801
11	10459084	SPBU 43.511.29	5.84E+08	Debit	240801
12	D0851171	Aston Inn	5.84E+08	Debit	240801
13	W0722201	ACE Hardware	5.21E+08	Debit	240801
14	W0722201	ACE Hardware	5.21E+08	Debit	240801
15	W0722201	ACE Hardware	5.21E+08	Debit	240801
16	W0722201	ACE Hardware	5.21E+08	Debit	240801
17	W0722201	ACE Hardware	5.21E+08	Debit	240801
18	D2AI5945	Element Family	5.84E+08	Debit	240801
19	D0AY2695	SPBU 11.29470	5.84E+08	Debit	240801
20	D2953293	Reich Vapor Store	5.84E+08	Debit	240801

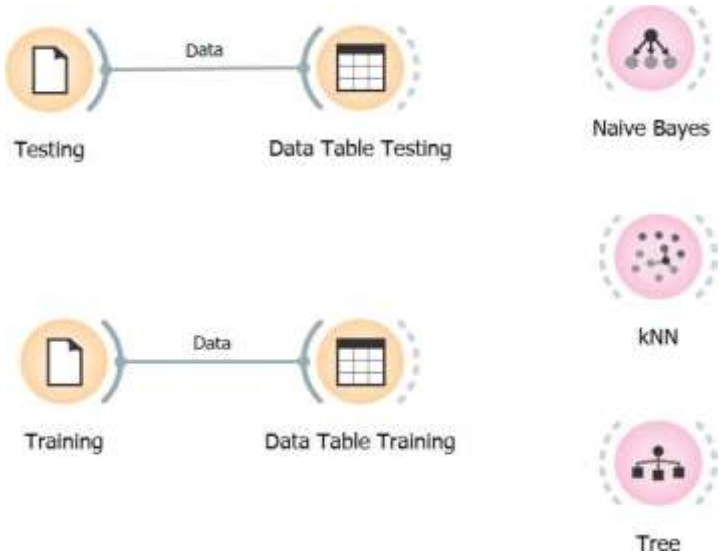
Based on the Sample Testing Data in Orange, the dataset shows debit transactions occurring within the same date, indicating a daily transaction snapshot. The data includes various merchants such as restaurants, fuel stations, retail stores, and services, reflecting diverse transaction activities. Repeated terminal codes for certain merchants suggest recurring transaction patterns, which are important indicators for anomaly detection. Overall, the dataset provides a structured foundation for identifying transaction patterns and potential anomalies in the classification process.

Table 10. Sample Labeled Data (Testing Data in Orange)

No	Merchant Information	ID	Channel	Label	Transaction Date
1	Ramen Ya Lippo Mall	5.84E+08	Debit	Non-Anomaly	240801
2	Cinepolis Citimall	5.84E+08	Debit	Non-Anomaly	240801
3	SPBU 34.10205	5.21E+08	Debit	Anomaly	240801
4	SPBU 34.10205	5.21E+08	Debit	Anomaly	240801
5	SPBU 34.10205	5.21E+08	Debit	Anomaly	240801
6	SPBU 34.10205	5.21E+08	Debit	Anomaly	240801
7	SPBU 34.10205	5.21E+08	Debit	Anomaly	240801
8	SRC Ucok-HO	5.84E+08	Debit	Non-Anomaly	240801
9	ACE Hardware	5.84E+08	Debit	Non-Anomaly	240801
10	Annisa Salon	5.84E+08	Debit	Non-Anomaly	240801
11	SPBU 43.511.29	5.84E+08	Debit	Non-Anomaly	240801
12	Aston Inn	5.84E+08	Debit	Non-Anomaly	240801
13	ACE Hardware	5.21E+08	Debit	Anomaly	240801
14	ACE Hardware	5.21E+08	Debit	Anomaly	240801
15	ACE Hardware	5.21E+08	Debit	Anomaly	240801
16	ACE Hardware	5.21E+08	Debit	Anomaly	240801
17	ACE Hardware	5.21E+08	Debit	Anomaly	240801
18	Element Family	5.84E+08	Debit	Non-Anomaly	240801
19	SPBU 11.29470	5.84E+08	Debit	Non-Anomaly	240801
20	Reich Vapor Store	5.84E+08	Debit	Anomaly	240801

The data are then processed according to the selected algorithm models. The following shows the implementation of the Naive Bayes Classifier, K-Nearest Neighbors, and Decision Tree models used in the Orange application in this study.

Figure 12. Training Data Display in Orange



The data classification process is then carried out using widgets in the Orange application.

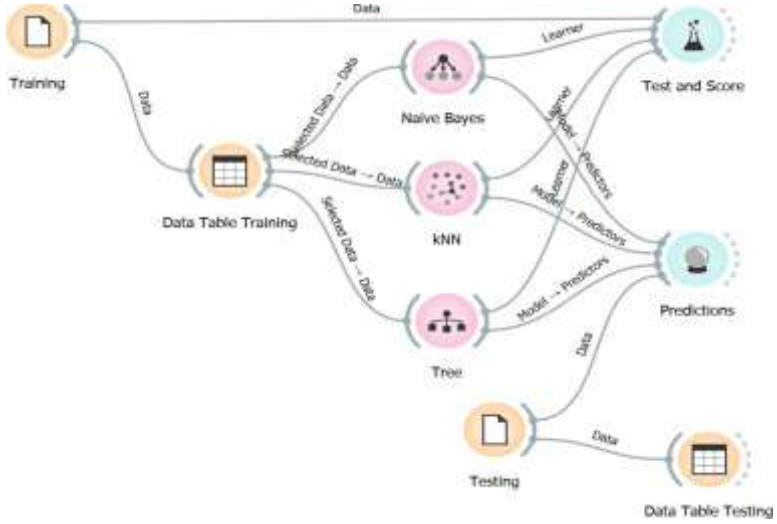


Figure 13. Data Classification Using Orange

After the processing stage, prediction results are generated from the three algorithms used. The following shows the predicted data output in tabular form within the Orange application based on the implemented models.

Table 11. Display of Predicted Data

No	Naive Bayes	KNN	Decision Tree	Terminal Code	Merchant Information	ID	Channel	Transaction Date	Transaction Time
1	Non-Anomaly	Non-Anomaly	Non-Anomaly	D0462179	Ramen Ya Lippo Mall	5.84E+08	Debit	240801	19:49:16
2	Non-Anomaly	Non-Anomaly	Non-Anomaly	9022512	Cinepolis Citimall	5.84E+08	Debit	240801	21:06:23

No	Naive Bayes	KNN	Decision Tree	Terminal Code	Merchant Information	ID	Channel	Transaction Date	Transaction Time
3	Non-Anomaly	Anomaly	Anomaly	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801	21:06:26
4	Non-Anomaly	Anomaly	Anomaly	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801	21:06:26
5	Non-Anomaly	Anomaly	Anomaly	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801	21:06:26
6	Non-Anomaly	Anomaly	Anomaly	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801	21:06:26
7	Non-Anomaly	Anomaly	Anomaly	D0AJ4790	SPBU 34.10205	5.21E+08	Debit	240801	21:06:26
8	Non-Anomaly	Non-Anomaly	Non-Anomaly	D0AU0815	SRC Ucok-HO	5.84E+08	Debit	240801	20:44:56
9	Non-Anomaly	Non-Anomaly	Non-Anomaly	W0722201	ACE Hardware	5.84E+08	Debit	240801	20:55:19
10	Non-Anomaly	Non-Anomaly	Non-Anomaly	D2960618	Annisa Salon	5.84E+08	Debit	240801	19:31:43
11	Non-Anomaly	Non-Anomaly	Non-Anomaly	10459084	SPBU 43.511.29	5.84E+08	Debit	240801	21:50:13
12	Non-Anomaly	Non-Anomaly	Non-Anomaly	D0851171	Aston Inn	5.84E+08	Debit	240801	19:02:17
13	Non-Anomaly	Anomaly	Anomaly	W0722201	ACE Hardware	5.21E+08	Debit	240801	20:55:19
14	Non-Anomaly	Anomaly	Anomaly	W0722201	ACE Hardware	5.21E+08	Debit	240801	20:56:19
15	Non-Anomaly	Anomaly	Anomaly	W0722201	ACE Hardware	5.21E+08	Debit	240801	20:56:50
16	Non-Anomaly	Anomaly	Anomaly	W0722201	ACE Hardware	5.21E+08	Debit	240801	20:57:19
17	Non-Anomaly	Anomaly	Anomaly	W0722201	ACE Hardware	5.21E+08	Debit	240801	20:58:19
18	Non-Anomaly	Non-Anomaly	Non-Anomaly	D2AI5945	Element Family	5.84E+08	Debit	240801	16:53:12

No	Naive Bayes	KNN	Decision Tree	Terminal Code	Merchant Information	ID	Channel	Transaction Date	Transaction Time
19	Non-Anomaly	Non-Anomaly	Non-Anomaly	D0AY2695	SPBU 11.29470	5.84E+08	Debit	240801	8:03:51
20	Non-Anomaly	Non-Anomaly	Anomaly	D2953293	Reich Vapor Store	5.84E+08	Debit	240801	12:41:57

Display of Confusion Matrix Results for the Naïve Bayes Classifier Algorithm:

Table 12. Confusion Matrix of the Naïve Bayes Classifier

Actual \ Predicted	Anomaly	Non-Anomaly	Total
Anomaly	12	1	13
Non-Anomaly	31	955	986
Total	43	956	999

The total number of true positive results is 12 out of the 1,000 dataset used. The following shows the confusion matrix results using the K-Nearest Neighbors algorithm:

Table 13. Confusion Matrix of the K-Nearest Neighbors Algorithm

Actual \ Predicted	Anomaly	Non-Anomaly	Total
Anomaly	7	6	13
Non-Anomaly	7	979	986
Total	14	985	999

The total number of true positive results is 7 out of the 1,000 dataset used. The following shows the confusion matrix results using the Decision Tree algorithm:

Table 14. Confusion Matrix of the Decision Tree Algorithm

Actual \ Predicted	Anomaly	Non-Anomaly	Total
Anomaly	0	13	13
Non-Anomaly	0	986	986
Total	0	999	999

There are no true positive results in this model, indicating that no anomaly data were detected from the 1,000 dataset used. The following table presents the performance scores generated in Orange using the Naïve Bayes Classifier, K-Nearest Neighbors, and Decision Tree algorithms.

Table 15. Prediction Results Table for the Three Algorithm Models

Model	AUC	Accuracy (CA)	F1 Score	Precision	Recall	MCC
Naive Bayes	1	0.919	0.953	0.995	0.919	0.231
Decision Tree	0.5	0.995	0.992	0.99	0.995	0
k-Nearest Neighbors (kNN)	0.998	0.996	0.997	0.998	0.996	0.744

The results indicate optimal performance among the three tested algorithm models. The comparative values obtained are as follows:

1. AUC = 0.998
2. Classification Accuracy (CA) = 0.996
3. F1 Score = 0.997
4. Precision = 0.998
5. Recall = 0.996
6. MCC = 0.744

Model Testing

Training Data Processing Using Matrix Attributes

The next step involves training the dataset using various matrix attribute combinations. Similar to previous testing in Orange, the Naive Bayes Classifier, K-Nearest Neighbors, and Decision Tree algorithms are applied to evaluate all data. The following presents the classification accuracy results based on training data attributes:

a. Evaluation of Matrix Attribute N1

The N1 matrix parameter identifies card numbers performing 5 debit transactions within a 5-minute interval. The following shows the evaluation results:

Table 16. Classification Accuracy Results for Matrix Attribute N1

Model	AUC	Accuracy (CA)	F1 Score	Precision	Recall	MCC
Naive Bayes	1	0.919	0.953	0.995	0.919	0.231
Decision Tree	0.5	0.995	0.992	0.99	0.995	0
k-Nearest Neighbors (kNN)	0.998	0.996	0.997	0.998	0.996	0.744

The maximum Classification Accuracy achieved is 0.996 using the K-Nearest Neighbors (KNN) algorithm. Further analysis is conducted by varying the training data attributes for comparison. The next evaluation uses a matrix parameter where a card number performs 10 repeated transactions within 5 minutes. The following presents the evaluation results:

Table 17. Classification Accuracy Results (Matrix Attribute Variation – 10 Transactions in 5 Minutes)

Model	AUC	Accuracy (CA)	F1 Score	Precision	Recall	MCC
Naive Bayes	1	0.978	0.989	1	0.978	0.553
Decision Tree	0.5	0.99	0.995	0.99	1	0
k-Nearest Neighbors (kNN)	0.999	0.995	0.997	1	0.995	0.814

The maximum Classification Accuracy obtained is 0.995 using the KNN algorithm. However, for matrix N1, the selected attribute is based on the highest accuracy value of 0.996, which corresponds to the condition where a card number performs 5 repeated transactions within 5 minutes.

b. Evaluation of Matrix Attribute N2

The N2 matrix parameter identifies card numbers performing 3 debit transactions with unusually high amounts (above 25 million) during abnormal hours (00:00–06:00). The following presents the evaluation results:

Table 18. Classification Performance Results for Matrix Attribute N2

Model	AUC	Accuracy (CA)	F1 Score	Precision	Recall	MCC
k-Nearest Neighbors (kNN)	0.569	0.994	0.991	0.988	0.994	0
Decision Tree	0.433	0.994	0.991	0.988	0.994	0
Naive Bayes	1	0.968	0.979	0.995	0.968	0.391

The maximum Classification Accuracy achieved is 0.994 using the KNN algorithm. Further evaluation is conducted by varying the training data attributes for comparison. The next scenario examines card numbers performing 3 debit transactions with unusually high amounts (above 50 million) during abnormal hours (00:00–06:00). The following presents the evaluation results:

Table 19. Classification Performance Results (Matrix Attribute Variation – Amount > 50 Million)

Model	AUC	Accuracy (CA)	F1 Score	Precision	Recall	MCC
k-Nearest Neighbors (kNN)	0.554	0.988	0.982	0.976	0.988	0
Decision Tree	0.449	0.988	0.982	0.976	0.988	0
Naive Bayes	0.969	0.99	0.991	0.993	0.99	0.676

The maximum Classification Accuracy achieved is 0.990 using the Naive Bayes algorithm. However, for matrix N2, the selected attribute is based on the highest accuracy value of 0.994, which corresponds to card numbers performing 3 debit transactions with unusually high amounts (above 25 million) during abnormal hours (00:00–06:00).

c. Evaluation of Matrix Attribute N3

The N3 matrix parameter identifies card numbers performing 5 debit transactions at the same time. The following presents the evaluation results:

Table 20. Classification Performance Results for Matrix Attribute N3

Model	AUC	Accuracy (CA)	F1 Score	Precision	Recall	MCC
Naive Bayes	0.998	0.968	0.978	0.992	0.968	0.48
Decision Tree	0.5	0.99	0.985	0.98	0.99	0
k-Nearest Neighbors (kNN)	0.995	0.992	0.993	0.996	0.992	0.742

The maximum Classification Accuracy achieved is 0.992 using the KNN algorithm. Further evaluation is conducted by varying the training data attributes for comparison. The next scenario examines card numbers performing 10 repeated debit transactions at the same time. The following presents the evaluation results:

Table 21. Classification Performance Results (Matrix Attribute Variation – 10 Transactions at the Same Time)

Model	AUC	Accuracy (CA)	F1 Score	Precision	Recall	MCC
Decision Tree	0.491	0.954	0.931	0.91	0.954	0
Naive Bayes	0.994	0.977	0.978	0.978	0.977	0.752
k-Nearest Neighbors (kNN)	0.996	0.982	0.983	0.987	0.982	0.84

The maximum Classification Accuracy achieved is 0.982 using the KNN algorithm. Therefore, for matrix N3, the selected attribute is based on the highest accuracy value of 0.992, corresponding to card numbers performing 5 repeated debit transactions at the same time.

Model Evaluation

The next step involves evaluating QRIS transaction data over a one-month period using the same implementation process as before. This aims to compare the highest anomaly occurrences within the month, using 1,000 datasets per day. The parameter attributes applied are based on the results of the previous training data comparison. The following are the matrix parameters used for the one-month data evaluation:

Table 22. Matrix Parameters for Anomaly Detection

Matrix	Attribute Description
N1	A card number performs 5 repeated transactions within 5 minutes
N2	A card number performs 3 transactions exceeding 25 million during unusual hours (00:00–06:00)
N3	A card number performs 5 repeated transactions at the same time

Based on the implementation process described in the previous section, the Classification Accuracy results for one month of data can be presented in the following table:

Table 23. Debit Transaction Classification Accuracy (August 2024)

Date (August 2024)	Classification Accuracy (CA)
1-Aug-24	0.991
2-Aug-24	0.993
3-Aug-24	0.987

4-Aug-24	0.986
5-Aug-24	0.992
6-Aug-24	0.994
7-Aug-24	0.988
8-Aug-24	0.992
9-Aug-24	0.991
10-Aug-24	0.993
11-Aug-24	0.993
12-Aug-24	0.995
13-Aug-24	0.993
14-Aug-24	0.99
15-Aug-24	0.994
16-Aug-24	0.99
17-Aug-24	0.996
18-Aug-24	0.988
19-Aug-24	0.982
20-Aug-24	0.987
21-Aug-24	0.989
22-Aug-24	0.988
23-Aug-24	0.985
24-Aug-24	0.993
25-Aug-24	0.988
26-Aug-24	0.989
27-Aug-24	0.994
28-Aug-24	0.994
29-Aug-24	0.988
30-Aug-24	0.998

The evaluation process is conducted to assess the performance of the applied models, using Classification Accuracy as the main reference for each matrix attribute analysis. Based on the one-month evaluation, the highest accuracy was achieved on August 30, with a Classification Accuracy value of 1 using the K-Nearest Neighbors algorithm. The overall results for the month are illustrated in the following chart.

Figue 14. Anomaly Data Chart Over One Month

The chart illustrates the distribution of detected anomalous transactions over a one-month period based on the applied classification model. It shows fluctuations in anomaly occurrences across different dates, highlighting patterns of transaction irregularities within the observed timeframe.

5. Conclusion

This study demonstrates that the application of machine learning classification techniques is highly effective in detecting anomalous debit payment transactions within switching systems. Among the evaluated models, the K-Nearest Neighbors (K-NN) algorithm achieved the highest performance with an accuracy of 0.996, indicating excellent classification capability. The Decision Tree algorithm followed closely with an accuracy of 0.995, while Naive Bayes showed comparatively lower performance at 0.919. These results suggest that instance-based learning approaches such as K-NN are particularly well-suited for identifying subtle deviations in transaction patterns within high-volume switching environments. Furthermore, the integration of operational transaction matrices (N1, N2, and N3) proved to be an effective approach in enhancing anomaly detection. By incorporating domain-specific knowledge into the classification process, the system was able to identify irregular transaction patterns at an early stage. This highlights the importance of combining data-driven techniques with practical operational frameworks to improve the relevance and accuracy of anomaly detection systems.

From an operational perspective, the implementation of data mining techniques provides significant benefits in improving efficiency and effectiveness in transaction monitoring processes. The automated classification of transactions reduces reliance on manual validation, minimizes the risk of human error, and strengthens fraud detection capabilities. Additionally, the results support better decision-making by providing structured and data-driven insights for operational teams. Overall, this study contributes to the development of a reliable and scalable anomaly detection framework for debit payment transactions in switching systems. Future research is recommended to expand the dataset, incorporate more diverse transaction sources, and explore alternative analytical tools to further enhance model performance and generalizability.

6. References

[1] Adhitya Prayoga Permana, K. A. (2021). Analisis perbandingan algoritma decision tree, K-nearest neighbor, dan naive Bayes untuk prediksi kesuksesan start-up. *JISKa*, 178–188.

[2] Ainurrohmah, D. T. (2023). Analisis performa algoritma decision tree, naive Bayes, dan K-nearest neighbor untuk klasifikasi zona daerah risiko Covid-19 di Indonesia. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 115–122.

[3] Kurniawan, A., & Hindriyanto, D. P. (2024). Sistem deteksi anomali pada transformator menggunakan dissolved gas analysis dengan metode K-nearest neighbor. *Jurnal Media Informatika Budidarma*, 144–153. https://doi.org/10.30865/mib.v8i1.7034

[4] Aliyah, A., Azzahra, N., & Putri, A. I. (2024). Analisis sentimen Twitter terhadap tren penyebaran informasi pelaku kejahatan menggunakan algoritma naive Bayes. *Jurnal Publikasi Sistem Informasi dan Telekomunikasi*, 85–97.

[5] Franko, B., Wilyanto, N., & Irsyad, H. (2024). Analisis sentimen terhadap naturalisasi pemain pada YouTube menggunakan decision tree dan naive Bayes. *Jurnal Session*, 8–16.

[6] Kurniawan, B. D., Heriansyah, R., & Mair, Z. R. (2025). Analisis prediksi terhadap peningkatan tindak pidana dengan metode naive Bayes berdasarkan laporan kriminalitas. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 4234–4241.

[7] Pratmanto, D., & Imaniawan, F. F. D. (2023). Analisis sentimen terhadap aplikasi Canva menggunakan algoritma naive Bayes dan K-nearest neighbors. *Computer Science (CO-SCIENCE)*, 110–117.

[8] Mardiani, E., Rahmansyah, N., Kurniati, I., Matondang, N., Zanitha, D. A., & Romzy, I. (2023). Membandingkan algoritma data mining dengan tools Orange untuk social economy. *Digital*

Transformation Technology (Digitech), 686–693.

[9] Zamachsari, F., & Puspitasari, N. (2021). Penerapan deep learning dalam deteksi penipuan transaksi keuangan secara elektronik. *Jurnal RESTI*, 203–212.

[10] Hozairi, A., Anwari, & Alim, S. (2021). Implementasi Orange data mining untuk klasifikasi kelulusan mahasiswa dengan model K-nearest neighbor, decision tree, serta naive Bayes. *Jurnal Ilmiah NERO*, 133–144.

[11] Wibawa, I. M. S. T., & Karyawati, A. A. I. N. E. (2023). Isolation forest dengan exploratory data analysis pada anomaly detection untuk data transaksi. *Jurnal Nasional Teknologi Informasi dan Aplikasinya*, 803–810.

[12] Kurniawan, A., & Yulianingsih. (2021). Pendugaan fraud detection pada kartu kredit dengan machine learning. *KILAT*, 320–325. https://doi.org/10.33322/kilat.v10i2.1482

[13] Kurniawan, Y. I. (2020). Aplikasi klasifikasi penentuan pengajuan kartu kredit menggunakan metode K-nearest neighbor di Bank BNI Syariah Surabaya. *Komputa Jurnal Ilmiah Komputer dan Informatika*, 73–82.

[14] Mahya, L., Tarjo, T., Sanusi, Z. M., & Kurniawan, F. A. (2023). Intelligent automation of fraud detection and investigation: A bibliometric analysis approach. *Jurnal Reviu Akuntansi dan Keuangan*, 588–613. https://doi.org/10.22219/jrak.v13i3.28487

[15] Mantik, H. (2024). Pengembangan electronic payment berbasis Android studi kasus PT ABC. *Universitas Dirgantara Marsekal Suryadarma*, 81–92.

[16] Apriyani, M. E., Renaldi, R., & Cinderatama, T. A. (2024). Analisis sentimen berita hoax menggunakan naive Bayes. *JIP (Jurnal Informatika Polinema)*, 1–6.

[17] Saddam, M. A., Kurniawan, E., & D. (2023). Analisis sentimen fenomena PHK massal menggunakan naive Bayes dan support vector machine. *Jurnal Informatika (JPIT)*, 226–233.

[18] Darmawan, M. B. A., Dewanta, F., & Astuti, S. (2023). Analisis perbandingan algoritma decision tree, random forest, dan naive Bayes untuk prediksi banjir. *TELKA*, 52–61.

[19] Muharrom, M. (2023). Analisis penggunaan Orange data mining untuk prediksi harga USDT/BIDR Binance. *Bulletin of Information Technology*, 178–184.

[20] Azhari, M., Situmorang, Z., & Rosnelly, R. (2021). Perbandingan akurasi, recall, dan presisi klasifikasi pada algoritma C4.5, random forest, SVM, dan naive Bayes. *Jurnal Media Informatika Budidarma*, 640–651. https://doi.org/10.30865/mib.v5i2.2937

[21] Marbun, N., & Prianggono, J. (2025). Analisis klasifikasi tindak kejahatan pencurian dengan algoritma K-nearest neighbor dan naive Bayes di Polres Buol. *JEMSI*, 3350–3365. https://doi.org/10.38035/jemsi.v6i5

[22] Purba, A. (2021). Pendeteksian fraud e-channel menggunakan algoritma pembelajaran mesin. *Buletin Riset Kebijakan Perbankan*, 42–61.

[23] Putra, R. A. (2024). Penerapan machine learning dalam deteksi kecurangan pada transaksi keuangan online. *Duniadata.org*, 1–16.

[24] Putra, R. V. (2021). Upaya pencegahan fraud pada bank berplat merah yang merugikan keuangan negara. *Jurnal Magister Hukum Perspektif*, 14–24.

[25] Ramayanti, P., & Sutabri, T. (2023). Perbandingan algoritma naive Bayes dan SVM untuk analisis penyalahgunaan kejahatan carding. *JINTEKS*, 18–24.

[26] Ningsih, P. T. S., Gusvarizon, M., & Hermawan, R. (2022). Analisis sistem pendeteksi penipuan transaksi kartu kredit dengan algoritma machine learning. *Jurnal Teknologi Informatika dan Komputer*, 386–401. https://doi.org/10.37012/jtik.v8i2.1306

[27] Firdaus, R., Hadiana, A. I., & Kasyidi, F. (2022). Model deteksi botnet menggunakan algoritma decision tree untuk mengidentifikasi serangan click fraud. *Journal of ICT*, 1–11.

[28] Khalida, R., & Setiawati, S. (2020). Analisis sentimen sistem e-tilang menggunakan algoritma naive Bayes dengan optimalisasi information gain. *JIFORTY*, 19–26.

[29] Lestari, T. S., & Sirodj, D. A. N. (2020). Klasifikasi penipuan transaksi kartu kredit menggunakan metode random forest. *Journal Riset Statistika*, 160–167. https://doi.org/10.29313/jrs.v1i2.525

[30] Yazid, A. F. (2017). Mendeteksi kecurangan pada transaksi kartu kredit menggunakan metode SVM. *Indonesian Journal of Applied Informatics*, 61–66.