ISSN 2723-6471

Anomaly Detection in Sales Transactions for FMCG (Fast Moving Consumer Goods) Distribution

Eggy Tanuwijaya[1,*], Tuga Mauritsius[2,]

[1]*Information Systems Management Department, BINUS Graduate Program – Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia*

[2]*Information Systems Management Department, BINUS Graduate Program – Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia*

(Received: May 29, 2024; Revised: June 29, 2024; Accepted: July 9, 2024; Available online: August 10, 2024)

Abstract

In today's era, companies operating in the FMCG industry played an important role in society, especially regarding the distribution of goods used in daily life, which were distributed directly from factories or principals. Despite rapid technological advancements, many distribution companies in Indonesia still relied on human labor and conducted distribution processes manually. Concerns about inaccuracies in employee actions and other detrimental activities such as embezzlement, fraud, and so on, drove companies to undertake digital transformation processes. To reduce these risks, some FMCG companies had already implemented systems to monitor distribution activities and customer payment processes. However, another issue arose due to the limited number of employees available to conduct professional audits, resulting in suboptimal monitoring processes and increased risks of integrity issues or fraud committed by employees. To address this, the implementation of an Autoencoder system was utilized to help companies detect fraudulent activities, particularly in the sales domain. Referring to this study, it showed that the implementation of machine learning technology, such as Autoencoders, yielded positive results and was considered effective in detecting suspicious activities, especially in large transaction datasets. The Autoencoder system utilized in this research was developed using TensorFlow, showing promising results in detecting fraudulent transactions in the company. Additionally, the model was able to train on 80% of the data and was tested on the remaining 20%. According to the outcome, approximately 6.664% of transactions were predicted to be fraudulent. Based on the results, this research showed that the implementation of the AutoEncoder system had proven to be effective in helping the organization prevent and protect against potential non-compliant activities. This proof could be used as a learning opportunity for other organizations facing similar challenges.

Keywords: Unsupervised Machine Learning, Anomaly, Auto Encoder, FMCG Distribution, Sales Transaction Fraud

1. Introduction

FMCG companies in Indonesia have a significant role in society, especially in fulfilling daily needs. Despite the rapid advancement of the digital era, many FMCG companies still conduct their distribution processes manually, relying on human labour. The challenges faced by FMCG companies have begun to emerge, forcing them to adapt to the evolving situation. According to Handoyo and Mulyani, a company's behavior is influenced by both internal and external factors, indicating that the characteristics of a company alone do not necessarily result in changes in strategic orientation but are also affected by external factors such as business conditions and competitive intensity [1].

According to Alkhyyoon et al., one of the challenges faced by FMCG companies is fraud. According to ACFE (Association of Certified Fraud Examiners), fraudulent activities conducted by employees include false financial reporting, corruption, and asset manipulation [2]. A corporate fraud, typically perpetrated by employees within an organization and can be categorized into three main types: financial statement fraud, asset misappropriation, and corruption. According to Aiman, among this financial statement fraud is the costliest despite being less common compared to asset misappropriation [3]. Fraud cases can be committed by one or more employees or even encompass the entire organization, depending on the type of fraud being perpetrated. Considering the scale of an FMCG company's operations, the smaller the team and the number of products, the easier it is for the audit team to conduct inspections

[*] **Corresponding author: Eggy Tanuwijaya (eggy.tanuwijaya@binus.ac.id)**

DOI: https://doi.org/10.47738/jads.v5i3.228

and detect suspicious activities. Problems arise when an FMCG company has a large number of employees, products, branches, and various distribution transactions. The larger the number of employees, products, outlets, and transactions, the higher the potential for fraudulent activities and errors, necessitating the company to use a digital system that can assist in this process and reduce the risk of fraud or mistakes.

As part of the research conducted, the researchers investigated the issues mentioned in an FMCG distribution company in the Bandung area, West Java, Indonesia. The company is a distributor of consumer goods operating in the FMCG industry with a focus on essential products. Established in 2002, the company operates in the Bandung area and its surroundings and has 4 branches, 10-20 salespeople in each branch, 100-500 customers/stores in each branch, Total monthly sales transactions of 80,000 transactions.

Table 1 illustrates the distribution capabilities, detailing several key processes involved. These processes include the first step is involves ordering goods from customers to field sales, where sales record the sales orders. Second step, sales report the sales orders to the warehouse, and the warehouse team verifies the stock. The third step, the warehouse loads the goods into trucks and delivers them to customers who placed the orders. The finance team receives proof of the ordered goods and outgoing goods, then records them as accounts receivable in the company's journal entry. After everything is finalized, the delivery of goods is carried out by the driver, driver's assistant, and sales team. The fourth step involves the customer receiving the goods and the sales team, which participates in the delivery, verifying the number of goods received. After verifying on-site, the sales team also provides an invoice to the customer. Last step, the customer makes the payment. This step includes two significant activities for settling the sales. In the table 1, it shows the FMCG Warehouse distribution data stating on the numbers of sales team and the number of modern and traditional shops.

Table 1. FMCG Warehouse Distribution

Region/Area	Number of Sales Team	Number of Modern and Traditional Shops
Kadipaten	10-20	100-500
Banjaran	10-20	100-500
Cimahi	10-20	100-500
Sumedang	10-20	100-500

For modern trade customers, most are systemized and usually make payments via transfer, receiving direct confirmation from the finance team. Meanwhile, customers in remote areas still prefer to use cash rather than inter-bank transfers. Additionally, when making payments, multiple invoices may be settled at once. After payments, the field sales team returns to the warehouse, deposits the cash, and informs the finance team that specific invoices have been paid. Every sales process carried out by a distribution company generally has the opportunity for fraud to occur, including collaboration in committing fraud between the field sales team and the customer, collaboration in committing fraud between the field sales team and the truck driver and manager, collaboration in committing fraud between the sales team and the finance team and the customer makes a payment to the field team, but the sales team does not transfer the money to the finance team. According to Shinde et al. a company annually summarizes its financial performance in standardized financial statements such as the balance sheet, profit and loss statement, and cash flow statement. Accountants follow generally accepted accounting principles (GAAP) and international financial reporting standards (IFRS) when preparing these statements. These financial statements are scrutinized for various practical applications, including corporate governance, credit appraisal, risk analysis, taxation, auditing, and investment decisions. Common types of misinformation include overstating assets, revenues, and profits, or understating liabilities, expenses, and losses. Notable corporate frauds like Enron, WorldCom, and Satyam Computers were due to accounting misinformation, leading to monetary losses and a loss of reputation. Auditors and forensic accountants use various investigative techniques to verify the numbers in financial statements and identify misinformation, relying on their domain expertise. Due to the effort-intensive nature of these investigations, many analytic techniques have been developed to identify financial statements likely containing misinformation [4].

This study is reinforced by the results of the annual report from ACFE, where 81% of the organizations surveyed have been victims of fraud, with losses of USD $100,000 per case, and 42% of the main perpetrators are from internal management. Due to the company's failure to implement internal controls, fraud occurs, and auditors have the knowledge and abilities to identify fraud in the company's books. The implementation of the management control system includes improving information systems and increasing auditor competence, especially in providing non-audit services (tax, investigative audit, consulting services), thereby improving the performance of public accounting firms. [5] Researchers will focus on the relationship between the sales team and finance regarding payments. The main objective of this research is to highlight the effectiveness of the Auto Encoder system implementation in an FMCG company facing potential fraud by employees and conducting the overall process manually, which causes issues.

2. Literature Review

2.1. Machine Learning

In today's rapidly evolving digital landscape, the detection of fraudulent activities remains a significant challenge, particularly due to the dynamic nature of fraud in small medium enterprise. According to Stojanović et al, one of the primary challenges in fraud detection is the necessity for real-time processing. Manual fraud detection techniques typically exhibit low accuracy and are both time-consuming and resource-intensive. Furthermore, the dynamic nature of fraudulent behavior, coupled with constantly changing profiles of normal and fraudulent activities, exacerbates the challenge. Existing information about fraud is often biased and unreliable [6]. Numerous studies worldwide have investigated fraud, with financial organizations frequently encountering fraud-related cases. Research by Hilal has demonstrated that multiple machine learning algorithms can be employed to detect fraud in financial transactions, including supervised, semi-supervised, and unsupervised algorithms for anomaly detection [7]. In some cases, techniques for detecting fraud utilize the same data mining process, but are adjusted based on the knowledge and requirements of the organization. Some organizations have created financial statement fraud detection (FSFD) systems, which categorize transactions from financial statements as fraudulent or non-fraudulent. Machine learning models, both supervised and unsupervised, are used to identify problematic transactions. The classification method is currently a popular technique for detecting suspicious or fake financial reports. Most financial statement fraud practices typically involve two stages. In the first stage, the model is trained on a dataset containing features and labels. In the second stage, several data samples are tested using the trained model. The performance of a machine learning or data mining (ML/DM) algorithm is directly related to the way features are extracted from the input data and how informative those features are. Selecting inappropriate features can lead to irrelevant or meaningless features and weak performance [8]. Previous research by Baur has identified several challenges associated with supervised machine learning, including the necessity for annotated data prior to training, which limits the model's learning range to the annotated data. Unsupervised machine learning is proposed to detect abnormalities more effectively without requiring annotated data [9]. Further research by Park and Kim highlights that supervised machine learning methods for detecting abnormal data rely on labelled data, whereas unsupervised methods can utilize unlabeled data, offering greater flexibility in identifying data anomalies [10]. The audit field is undergoing a significant digital transformation driven by information technology. Traditional audit practices are evolving towards continuous auditing by automating accounting and audit procedures with the help of support systems. In certain scenarios, auditors must use an audit support toolkit to ensure compliance with standards, speed up processes, and facilitate decision-making. This toolkit includes various models and information technologies that organizations utilize to enhance the efficiency and effectiveness of audits. Fundamentally, an audit is a systematic process of impartially evaluating evidence related to statements about economic activities and events to determine their conformity with predetermined criteria, with the results communicated to relevant stakeholders [11]. This research utilizes machine learning technology to create warnings for users and decision-makers within the company, helping them to identify and understand the distribution of data within clusters that are anomalous [12]. This overview underscores the complexities and evolving methodologies in the field of fraud detection, highlighting the importance of advanced machine learning techniques in enhancing detection accuracy and efficiency.

2.2. Auto Encoder

In the realm of fraud detection, supervised anomaly detection techniques rely on the premise that the dataset consists of labelled instances categorized as either normal or anomalous. Methods in this category typically build predictive models for both classes, enabling the classification of new, unseen data by comparing it against these established models. A notable challenge with supervised anomaly detection, as mentioned earlier, is the infrequency of the anomalous class relative to the normal class. Additionally, obtaining precise labels that accurately represent the anomalous class is difficult. This issue, known as the class imbalance problem, manifests in practical applications where the ratio between normal and anomalous classes can range from 1:100 to as extreme as 1:10,000. Autoencoders, a type of unsupervised learning model, offer significant advantages by learning the normal data distribution and flagging deviations. This makes them effective in detecting sophisticated and previously unseen fraudulent activities. Compared to traditional methods, autoencoders handle the class imbalance problem more effectively and reduce reliance on labelled data [7] The proposed neuro-symbolic architecture enhances fraud detection by integrating neural networks and symbolic reasoning. This system combines the high-performance anomaly detection capabilities of neural models with the interpretability of symbolic models. The rule-based model interprets the behavior of the autoencoder model, providing insights into the alarms triggered by the neural network. Earlier strategies of fraud detection, which relied on computational and signature-based tactics, have proven ineffective in handling the complexities of modern fraud. These methods often generate a high number of false positives, mistaking legitimate actions for fraudulent ones, leading to operational inefficiencies and customer dissatisfaction [13]. Autoencoders address these issues by learning efficient representations of normal transactions, enabling the detection of anomalies that indicate potential fraud. This reduces false positives and accurately identifies fraudulent activities, enhancing fraud detection reliability and performance. According to Gama, et.al, the goal of anomaly detection is to identify errors and help explain behaviors that cannot be accounted for by the overall system. To achieve this, an anomaly detection framework can be utilized. [14]. The most common type of autoencoder is the undercomplete autoencoder, where the hidden dimension is less than the input dimension. The architecture of such an autoencoder is shown in figure 1.

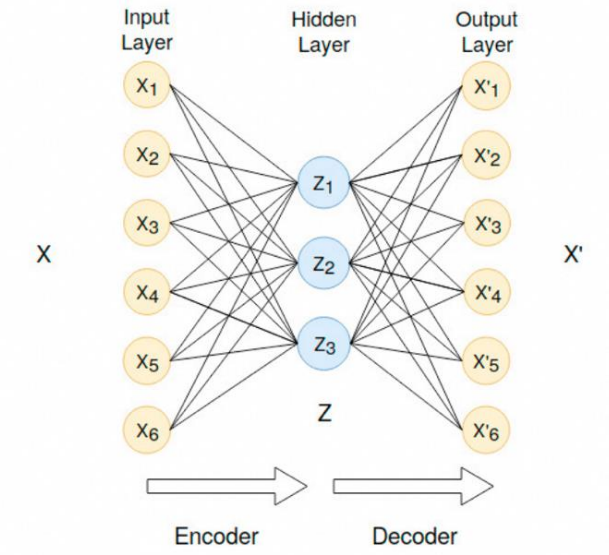

Figure 1. Architecture of autoencoder with a single encoding layer and a single decoding layer [15]

An Autoencoder is used to detect fraud, including credit card fraud. It is designed to recreate high-dimensional information using a neural network model with layers that have narrow constraints in the middle. The Autoencoder has an equal number of input and output units in the output layer, which can accommodate a large number of input units. [16]. The Autoencoder is a suitable option for detecting fraudulent transactions because this model identifies anomalous data by comparing it with normal data. To detect fraud, it must identify biased data by examining several irrelevant features as input. These two factors hinder the ability to properly classify large amounts of transaction data. To address this problem, a two-stage approach has been proposed. In the first stage, lower-dimensional features are extracted from the input, and in the next stage, the model determines whether the transaction is fraudulent or not. This approach utilizes

Autoencoders, which can efficiently create lower-dimensional representations of input data while also identifying non-linearly correlated features [15]. The Autoencoder structure consists of input, encoder, bottleneck, decoder, and reconstructed input layers. The encoder learns to reduce the dimensions of the input, compressing it into an encoded representation and the bottleneck contains a compressed representation of the input data and has the smallest dimension while the decoder helps to reconstructs the data from the encoded representation aiming to closely match the original input.

To estimate error, various mathematical functions are used, with the mean squared error (MSE) being commonly employed. The system's performance impacts the accuracy of the reconstructed data. Minimizing this error ensures that the output closely resembles the original training data, achieving near-identical replication [17]. According to Al-Shabi, the hidden layer within the core layer is a focal point in auto-encoder research, as it holds crucial information that can be extracted from the input values. This condition compels the hidden layer to learn data patterns effectively while filtering out "noise". In an auto-encoder model, the hidden layer typically has smaller dimensions compared to the input or output layers, resembling a wide funnel on the input side and narrowing towards the output. Figure 2 provides significant idea of the Auto Encoder structure.

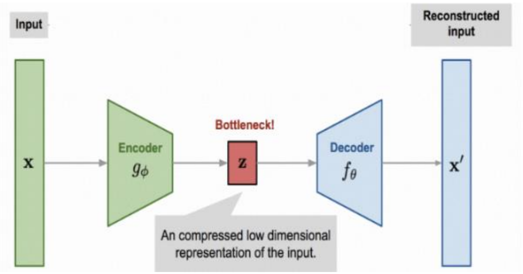

Figure 2. Structure of AutoEncoder [16]

The decoding process reconstructs information to produce results. It mirrors the coding process but in reverse—a narrow funnel on the left and wide on the right. Typically, the model is structured so that decoding reflects coding. The number of neurons and hidden layers in both processes' correlates. Before using the autoencoder, there are four crucial parameters. The first parameter is code size if the number of nodes in the middle layer is small, the pressure will be high. The second parameter is the numbers of layers it will determines the flexibility and depth of the layers. The third parameter is number of nodes per layer, the nodes decrease after the encoder and increase the decoder with adjustable numbers for each layer. Last parameter is loss function is to measure error in reconstructing input data typically MSE is being used. After determining these parameters and running the model, it is evaluated for performance, particularly in detecting fraudulent transactions.

$$\mathrm{MSE} = \frac{1}{n}\sum_{\{\mathrm{i}=1\}}^{\mathrm{n}}(\mathrm{x_i} - \bar{\mathrm{x}}_\mathrm{t})^2 \quad (1)$$

The identification of the formula above is "n" indicating size for input and output, "x" indicating input data, "X" indicating output data, and MSE.

To determine whether a transaction process is considered fraud or not, a threshold can be applied. Typically, this threshold (k) distinguishes between normal and anomalous transactions, often set assuming that 5% of the data contains anomalous transactions. In the model compilation section, The MSE serves as the loss function for identifying outliers based on higher MSE values, while Adam is chosen as the optimizer. In the model fitting section, input and output are defined as normal transactions. Subsequently, predictions can be made to classify transactions as either normal or fraudulent, with each input assessed against the threshold value. This approach can be formulated using the following equation: [18] Normal transaction is MSE < k, Fraudulent transaction is MSE > k, k is Threshold set, Precision and Recall, one of the most widely used standards for handling unbalanced data assesses the suitability and accuracy between results and their expected solutions. Recall measures the number of relevant outputs returned, aiming to approach these results. High recall indicates fewer False Negatives (FN), whereas high precision indicates fewer False Positives (FP). High ratings in both FP and FN indicate that the classifier provides accurate results.

The Confusion Matrix is used to assess the performance of a classification model by comparing its predictions against the actual values in a dataset. It presents a structured view of the counts of various types of outcomes, in table 2 showing how many transactions fall into each category. And in table 3 showing how to measure the performance of Classifications through Precision, Recall, and F1 Score detail information.

Table 2. Confusion Matrix

	Predicted genuine (0)	
Actual Genuine (0)	TN – True Negative	FP – False Positive
Actual Fraud (1)	FN – False Negative	TP – True Positive

Table 3. Precision, Recall and F1 Score

Measure	**Definition**
Sensitivity (Recall)	TP/(TP + FN)
Precision	TP/(TP + FP)
F-measure	2 * Precision * Recall / (Precision + Recall)
Accuracy	(TP + TN) / (TP + TN + FP + FN)
F1 Score	2 * (Precision – Recall) / (Precision + Recall)

After implementing the model, performance evaluation is necessary for the autoencoder model. Several indicators will be used in this evaluation, including precision, recall, and the confusion matrix. The Precision (Positive Predictive Value) is to measures the proportion of correctly identified fraud cases out of all cases predicted as fraud. The Recall (Sensitivity)is to measures the proportion of actual fraud cases that have been correctly identified out of the total number of fraud cases. TP (True Positive) is the number of fraud cases correctly identified. FP is the number of legitimate transactions incorrectly flagged as fraudulent. FN is the number of fraud cases incorrectly classified as legitimate transactions. TN (True Negative) is the number of legitimate/non-fraud transactions correctly identified. These measures are crucial for using the model to detect fraud. However, they must be applied carefully in real-world implementation, as misclassifications can result in similar losses to true fraudulent transactions [19].

2.3. Previous Research

To support research on using autoencoders for fraud detection, researchers gathered several studies from Scopus-indexed international journals published in the last 6 years. The search revealed that journals specifically discussing fraud and anomaly detection often explore transaction anomalies in credit card fraud detection using unsupervised machine learning, particularly autoencoders. The first study, conducted by Hilal et al. in 2022, highlights the increasing prominence of financial sector topics in recent years. Some of the latest literature on autoencoders demonstrates significantly improved performance compared to previous methods [7]. The second study, by Misra et al. in 2020, focuses on detecting credit card fraud using a model capable of handling biased data and irrelevant features in inputs. Traditional classification methods often experience reduced accuracy with large datasets, whereas autoencoders efficiently create lower-dimensional representations of input data and identify nonlinear, significant features [15]. The third study, conducted by Tingfei et al., addresses credit card fraud detection as a binary classification problem where fraud cases are vastly outnumbered by non-fraudulent transactions, typically less than 1% of total data. To enhance classification effectiveness, frameworks for fraud detection strive to bridge this gap. Autoencoders are employed in this context to identify abnormal data within imbalanced datasets [20].

ISSN 2723-6471

3. Proposes Methodology

This research utilizes the CRISP-DM (Cross-Industry Standard Process for Data Mining) method. CRISP-DM is a widely used methodology for data mining and knowledge discovery in databases. It provides a structured approach to planning and executing a data mining project. The stages of CRISP-DM are first Business Understanding: In this stage, data is retrieved from the company. Second Data Understanding: This stage involves collecting data to understand the transactional data flowing within the company. Third Data Preparation: Here, data is prepared as input for processing through a data transformation process. This includes retrieving data that will be used later in the model. Fourth Modelling: This stage involves making predictions about transactions suspected of being fraudulent. Typically, about 80% of the data is used for training, while the remaining 20% serves as test data. The modelling stage includes a general understanding of classification algorithms for evaluating and predicting outcomes, which are crucial for the deployment stage. The last stage is Deployment: This final stage involves implementing the data modelling and mining results. Applications in this stage send notifications to assist decision-makers or auditors in identifying potential fraud in sales transactions.

3.1. Business Understanding

Data collection involves gathering sales transactions and payment transactions from various customers and agents in the Bandung area and surrounding regions. With approval from company management, researchers utilized this data to develop insights for detecting fraud in sales transactions. Figure 3 illustrates the cross-functional diagram depicting the sales transaction process outlined above. The stages of this process are as follows: First customers place orders with the sales team, who record these orders in the order book. Second, the sales team reports sales orders to the warehouse, where staff verify stock availability. If a customer requests items not in cartons, warehouse personnel open the cartons and retrieve smaller units. The third, goods are loaded onto trucks by the warehouse team and delivered to customers who placed orders. Simultaneously, the finance team receives proof of order for the goods, which are then recorded as outgoing goods and become receivables in the journal entry. Once all verification processes for outgoing goods are complete, the goods are delivered by the driver, driver assistant, and sales team. To give better idea, figure 3 shows how the sales process is run in this organization.

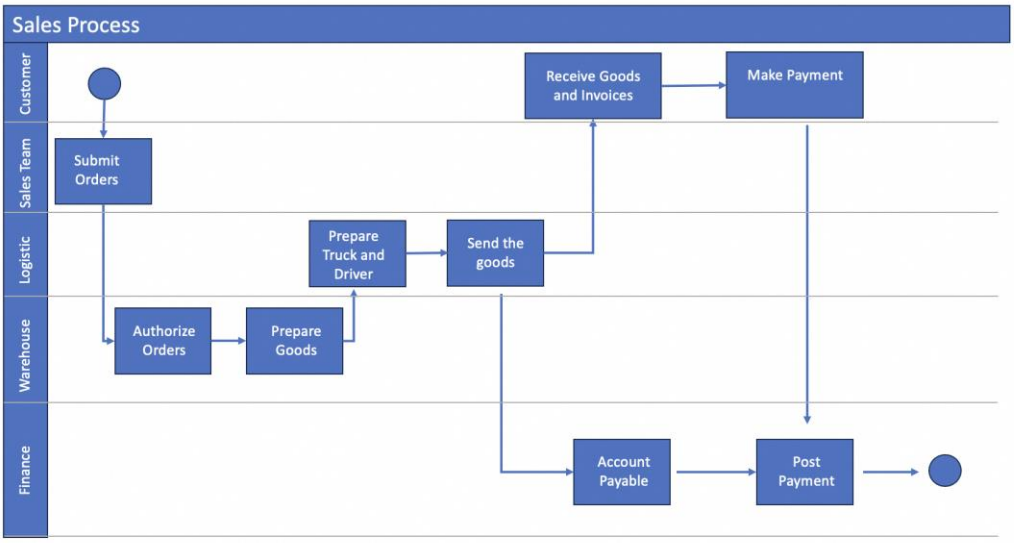

Figure 3. Sales Process

Fourth, the customer receives the goods, and both the customer and the sales team verify the quantity received during delivery. After on-site verification, the sales team also provides an invoice to the customer. Lastly, the customer makes payment. This fifth step involves two significant activities in settling the sales transactions. For modern trade customers, most transactions are systematized, and payments are typically made via bank transfer, directly confirmed with the finance department while in contrast, customers in remote areas often prefer cash payments over inter-bank transfers. Moreover, when making payments, it's common to settle multiple invoices at once. After receiving payment, the sales team in the field returns to the warehouse, deposits the cash, and informs the finance team of the paid invoices, specifying their numbers.

Currently, the company utilizes a distribution system that includes a payment module integrated within. This system manages data such as seller and customer records, stock transactions, and payment transactions. Despite these advancements, the company still struggles to detect fraud due to the high volume of monthly sales transactions, totaling approximately 80,000. Instances of fraud have resulted in significant losses for the company, ranging from Rp.20,000,000 to Rp.500,000,000 per fraudulent transaction at individual branches. Such losses have had serious repercussions, with some distribution companies being forced to shut down and declare bankruptcy due to these financial impacts. One common fraudulent activity involves sales personnel selling goods and pocketing payments without depositing them into the company's accounts.

3.2. Data Understanding

The data to be used will be sourced from a distribution application currently operational in one of the distribution companies in Bandung, with prior approval from company management. Before implementing this system, audit data was manually collected and extracted over a period of one to three months. During this process, the company relied on employees who had access to the data to provide the necessary information. Handling incomplete information or discrepancies involved cross-referencing each record and information obtained from employees, resulting in unreliable accuracy and efficiency.

To enhance the process, the company now utilizes a distribution management system. This system serves as a prerequisite for verifying anomalies in ongoing transactions. The extracted data originates from several tables, namely Master salesman, Master customer, Sales Transactions and Payment Transactions. The data for this research will include sales transaction data from January 2023 to February 2023 and payment transactions for sales up to June 2023. This extended timeframe accounts for possible delays in customer payments beyond the initial period. Currently, the company handles around 80,000 sales transactions per month. For this study, a total of 160,000 data points will be analyzed from January and February 2023.

3.3. Data Preparation

In this stage, the researcher will manipulate and transform data from several tables provided by the company, which are initially unclean. Therefore, the researchers first need to conduct data exploration (observation) and select features that can be used in the model development process. Implementation involves several stages due to the data being provided in multiple files. The first stage involves extracting data from the FTP Server and loading it into the Machine Learning service. This step simplifies data analysis through queries. The second stage includes data transformation and cleansing from multiple tables into a consolidated table. This process adjusts scales, resolutions, or feature representations. For instance, numeric features may be converted to logarithmic scales, mathematical functions may be applied, and string data may be converted into meaningful numerical representations. Data cleansing addresses formatting discrepancies, adjusts inappropriate field contents, and handles null or empty data in various columns. The third stage focuses on feature selection, where the most relevant and informative subset of features is chosen for model development. Methods such as statistical analysis, correlation analysis, or specialized machine learning algorithms may be used for this purpose. Selected features are chosen based on their potential to reveal patterns and anomalies indicative of fraudulent activities. Key columns like Salesman ID, Customer ID, Salesman Entry Date, Sales Date, Payment Date, and Allowed Credit Duration are specifically selected. These columns are transformed into features that highlight fraudulent behavior by providing insights into sales transactions, payment histories, and relationships between customers and salesmen.

3.4. Modelling

This research will employ an unsupervised method using Autoencoder. The model creation will be implemented in Python programming language with TensorFlow, integrated with data services. After completing the data transformation process, researchers will proceed to the next stage: developing a fraud detection model. Figure 4 illustrates the process of model creation, detailing each phase.

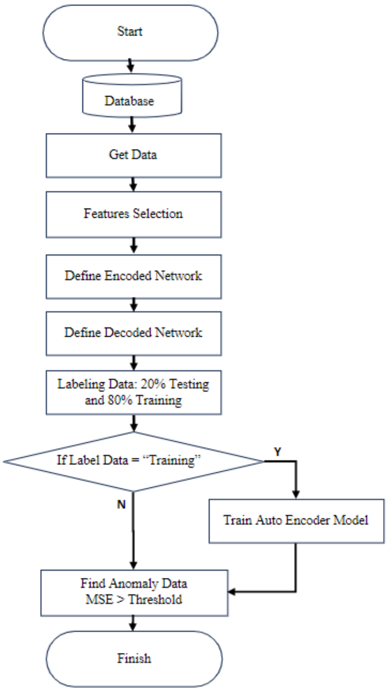

Figure 4. Auto Encoder Model Creation

Based on figure 4, the steps to create the model are number one retrieve the data from sources processed in previous stages. Two define Encoder and Decoder in the Autoencoder. Three split the dataset into two parts: 80% for training data and 20% for testing data. Four train the Autoencoder model. Five identify suspicious transaction data by determining MSE > threshold. To test the model's results and demonstrate performance, three indicators will be used: precision, recall, and the confusion matrix. Precision is the proportion of correctly identified fraud cases out of all cases predicted as fraud. Recall is the proportion of actual fraud cases correctly identified out of the total number of fraud cases. TP is the number of fraud cases correctly identified. FP is the number of legitimate transactions incorrectly flagged as fraudulent. FN is the number of fraud cases incorrectly classified as legitimate transactions. TN is the number of legitimate/non-fraud transactions correctly identified. To provide a clearer understanding of how the Autoencoder is applied specifically to the dataset, several essential steps are outlined below (table 4) to complete the process:

Table 4. Steps for Fraud Detection Using Machine Learning

Step	Details
Step 1: Data Preparation	Select tables: customers, payment, sales transactions and customers Import data: Audit report manual, converted from Excel to CSV, and input into the table named tr_audit_manual.
Step 2: Data Transformation	Select columns: Salesman ID Customer ID Customer Group (Group or Individual) Salesman Entry Date Sales Transactions Date Payment Date Settlement Duration = Payment Date – Sales Date Outstanding Amount = Total Sales Transactions – Total Payments Length of working = Datetime(now) – Salesman Entry Date

Step 3: Feature's selection	Length of Working, Settlement Duration, Outstanding Amount, Customer Group

Step 4: Model Building and system parameter
Hyperparameter detail:
Optimizer: Adam
Loss Function: MSE
Epochs: 100
Batch Size: 128
	encoded = Dense(32, activation='relu')(input_data)
	decoded = Dense(input_shape[0], activation='sigmoid')(encoded)
	autoencoder(optimizer='adam', loss='mean_squared_error')
	autoencoder.fit(scaled_data, scaled_data, epochs=100, batch_size=128)
	reconstructed_data = autoencoder.predict(scaled_data)
	mse = np.mean(np.power(scaled_data - reconstructed_data, 2), axis=1)
	#configure the threshold
	threshold = np.percentile(mse, 95) configure

Step 5: Anomaly/Fraud Status	actual_labels = df['fraudstatus'].values Update fraud status for the suspect of fraudulent persons
Step 6: Validations	Compare between Table Audit Report Manual with fraudulents persons : Recall Precisions Confusion Matrix y_pred = df['manualauditstatus'] y_true = df['machinelearningstatus'] confusion_matrix(y_true, y_pred)

The model was tested using data from the company's distribution system, identifying suspicious data points. A MSE threshold was set at the 95%, indicating that data points with MSE values above this threshold were considered suspicious and flagged for further audit.

4. Result and Discussion

After conducting research using data from the company's distribution system, suspicious data was identified. Using a MSE threshold of less than 0.5 draws attention for auditors and business owners to scrutinize the data more closely. The results showed that the model was able to detect the transactions as fraudulent and after completing all modelling using the Auto Encoder, it demonstrates the effectiveness of machine learning, especially in handling activities within large-scale transaction datasets.

4.1. Results

In the current modelling process, data is exported from the company's distribution system. After export, this data is uploaded by the finance team to a folder using the FTP Server. Once CSV or TXT files are uploaded, the server automatically runs a daily schedule to input the data into a Relational Database. After extracting the data, a Virtual Machine automatically executes the Autoencoder model and performs classification. If fraud is detected in the classification results, the system automatically sends alerts to the auditor and company owner. Out of the 160,000 raw data entries from January to February 2023, there were 141 cases handled according to the manual audit report conducted by 10 persons in the company. Below are the queries to retrieve the numbers from the manual audit report table first select count(documentno) from tr_audit_manual tam then select count(distinct salesmanname) from tr_audit_manual tam

Using an Autoencoder model developed with TensorFlow and data in virtual machines, promising results were demonstrated in detecting fraudulent transactions at the company. The model was trained on 80% of the data and tested on the remaining 20%. Based on the results from the Autoencoder, approximately 6.664% of transactions were predicted to be fraudulent. Furthermore, the histogram in figure 5 indicates that most samples exhibit low reconstruction errors, falling towards the left side of the distribution, which corresponds to normal transactions because the MSE values are close to zero. Conversely, samples with higher reconstruction errors, represented towards the right side of the histogram, are potential outliers or anomalies. These data points have significantly higher MSE values, suggesting that the autoencoder struggled to reconstruct them accurately. This discrepancy implies that these transactions deviate substantially from the normal data patterns and are likely to be fraudulent or anomalous as shown on figure 5.

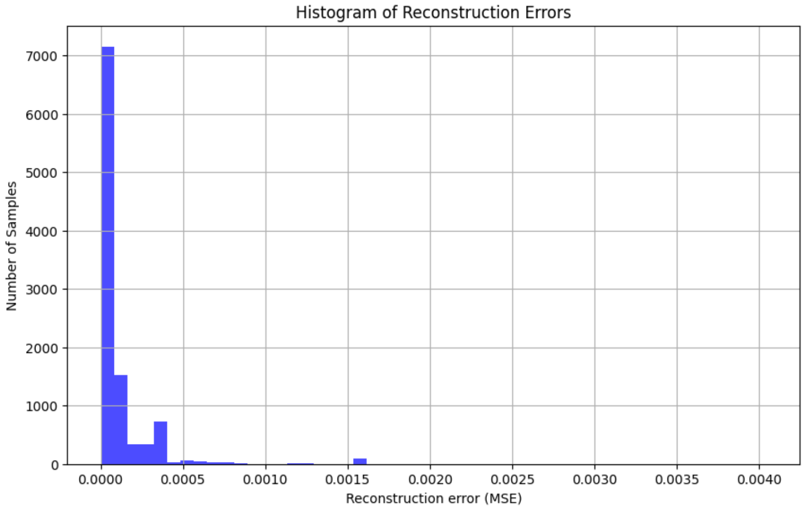

Figure 5. Normal and Anomaly Transactions

In the constructed model, the data obtained from all parties, including fraud category data, will be entered into a table that will be audited by the audit team. Furthermore, in the discussion section, it will be explained how the accuracy of the auditor's reports compares with the confusion matrix. Table 5, illustrates an example of a report generated by a salesperson engaged in fraud. This result is derived from the autoencoder that has been developed, providing information about the sales ID and the salesman involved in fraudulent activities, thereby enhancing the accuracy of the data or information provided.

Table 5. Normal and Anomaly Transactions

Sales Id (Character)	Sales Name (Character)
JHHP 202669	AHMAD GOJALI (SUMEDANG) --JHHP--
JHHP 198545	YAYAN SURYANA
JHHP 197675	SANI ABUDIRAFI --JHHP--
760523000606	HANDI WAHYUDIN -SASA-
JHHP201506	JUDIKA H. LUMBANTORUAN--JHHP--
JHHP202712	SURYANA SLD--JHHP--
JHHP 198510	NENDEN LIDIYAWATI --JHHP--

4.2. Discussions

After completing all modeling using the Autoencoder, the results demonstrate the effectiveness of machine learning, especially in handling activities within large-scale transaction datasets. This is particularly relevant for FMCG distribution companies that manage high transaction volumes, where manual monitoring proves inefficient and unreliable. Figure 6 depicts a TSNE (t-Distributed Stochastic Neighbor Embedding) plot chart showing the distribution of normal and anomalous transactions. TSNE is a machine learning technique used for dimensionality reduction and visualizing high-dimensional data to validate anomaly transactions detected by the Autoencoder against the real audit report provided by the company. The audit report is manually generated by internal auditors within the company, but this manual process limits the auditors' ability to access all necessary data related to fraudulent transactions. The audit report includes details such as salesman names and transactions involved in fraudulent activities.

Before adopting the Autoencoder, the company explored other systems such as VAE (Variational Autoencoder) and GAN (Generative Adversarial Network). While these systems are effective in understanding data distributions, identifying anomalies, and generating new data samples, the company ultimately chose Autoencoders due to their significant advantages. Autoencoders excel in anomaly detection by learning the normal data distribution and flagging deviations, thereby detecting sophisticated and previously unseen fraudulent activities—a critical challenge for the company. Implementing this solution has reduced data discrepancies and errors, and decreased reliance on human resources. Automating the distribution process has improved time efficiency, enhanced business effectiveness, and reduced instances of non-compliance, thereby minimizing disciplinary actions against employees as shown in figure 6.

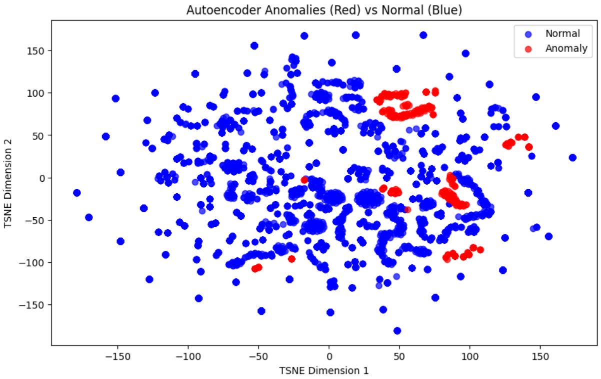

Figure 6. Auto Encoder

To validate fraud transactions between the manual audit report and the Autoencoder results, several indicators were used. First the precision: the model achieved a precision rate of 89.3%, indicating its effectiveness in correctly identifying fraudulent transactions among those classified as fraud. Second the recall: The recall rate was 100%, reflecting the model's ability to correctly classify all fraudulent transactions from the total number of fraud cases. Third the Confusion Matrix as indicated on table 6.

Table 6. Confusion Matrix

	True	**False**
Positive	118	14
Negative	0	0

This confusion matrix shows that all positive instances were correctly identified. The data size is small because the results are generated from the model and used to inform the suspected individuals. Afterwards, we compare these results with the manual audit report.

5. Conclusion

This paper proposes a new method for detecting fraud, especially in the sales transaction's domain. By applying a TensorFlow-based model to transaction data from January to February 2023, we automated the identification of suspicious transactions with a reasonable degree of accuracy. The prototype described in this paper follows the CRISP-DM process to enhance understanding of the data collection process used for detection. Additionally, implementing the prototype will enable the Finance team to conduct regular audits more efficiently. They can upload files related to sales and settlement transactions, and predictions from the model demonstrate its current success in detecting fraud within the company.

Based on these findings, several recommendations are proposed number one Continuous Model Training: Regularly updating the model with fresh and diverse datasets will improve its accuracy and adaptability to new fraud patterns. Two Integration with Internal Systems: Embedding the autoencoder model directly into financial and operational systems can streamline fraud detection, enabling real-time analysis and alerting. Three Holistic Fraud Detection Strategy: While machine learning is a powerful tool for identifying potential fraud, it should complement broader fraud detection and prevention strategies that include manual checks, employee training, and other security measures.

In conclusion, adopting machine learning models like autoencoders offers a promising approach to enhancing fraud detection in FMCG distribution networks. Despite challenges, the benefits of improved detection rates and operational efficiency suggest that further development and integration of such models could significantly strengthen the company's ability to prevent fraudulent transactions to make it more reliable this action need to be supported by having additional employee’s code of conduct business training, impose a company culture focusing on integrity value, and other policy to enhance the fraud prevention activities. The result of the research showed that by implementing this system, it will help the company solve issues related to data discrepancies or any potentially fraudulent activities that might be carried out by employees. This research brings a new perspective to other organizations within the same or different industry and encouraging them to start shifting from manual processes to more digitized systems. For future research, we recommend expanding the dataset, refining the model, and exploring additional machine learning techniques to enhance fraud detection capabilities further. Moreover, exploring other domains such as early detection of fraudulent activities in finance, cybersecurity threat detection, and other sectors not covered in this study, including healthcare, education, and public sectors, should be considered.

6. Declaration

6.1. Author Contributions

Conceptualization: E.T. and T.M.; Methodology: E.T. and T.M.; Software: E.T.; Validation: E.T. and T.M.; Formal Analysis: E.T. and T.M.; Investigation: E.T.; Resources: E.T. and T.M.; Data Curation: E.T.; Writing Original Draft Preparation: E.T. and T.M.; Writing Review and Editing: T.M. and E.T.; Visualization: E.T.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. Handoyo, S. Mulyani, E. K. Ghani, and S. Sudarsono, “Firm Characteristics, Business Environment, Strategic Orientation, and Performance,” *Adm Sci*, vol. 13, no. 3, pp. 1–23, Mar. 2023, doi: 10.3390/admsci13030074.

[2] H. Alkhyyoon, M. R. Abbaszadeh, and F. N. Zadeh, “Organizational Risk Management and Performance from the Perspective of Fraud: A Comparative Study in Iraq, Iran, and Saudi Arabia,” *Journal of Risk and Financial Management*, vol. 16, no. 3, pp. 1–27, Jan. 2023, doi: 10.3390/jrfm16030205.

[3] A. M. Aiman, T. N. T. Ismail, and M. Anisa. Safiah, “The Relationship Between Perceived Pressure, Perceived Opportunity, Perceived Rationalization and Fraud Tendency Among Employees: A Study from THE People’s Trust in Malaysia,” *Studies in Business and Economics*, vol. 17, no. 2, pp. 23–43, Aug. 2022, doi: 10.2478/sbe-2022-0023.

[4] A. Shinde, S. Vaishampayan, M. Apte, and G. K. Palshikar, "Unsupervised Detection of Misinformation in Financial Statements," *The Florida Artificial Intelligence Research Society (FLAIRS)*, vol. 35, no. 5, pp. 1-4, May 2022.

[5] E. S. Mardjono, E. Suhartono, and G. T. Hariyadi, "Does Forensic Accounting Matter? Diagnosing Fraud Using the Internal Control System and Big Data on Audit Institutions in Indonesia," *WSEAS Transactions on Business and Economics*, vol. 21, no. 53, pp. 638–655, 2024, doi: 10.37394/23207.2024.21.53.

[6] B. Stojanovi´c, J. Boži´c, K. Hofer-Schmitz, and A. Weber, "Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications," *Sensors*, vol. 21, no. 5, pp. 1–43, Feb. 2021, doi: 10.3390/s21051594.

[7] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances ," *Expert Syst Appl*, vol. 193, no. 12, pp. 957–1474, 2022, doi: 10.1016/j.eswa.2021.116429.

[8] M. N. Ashtiani and B. Raahemi, "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review," *IEEE Access*, vol. 10, no. 7, pp. 72504–72525, Jul. 2022, doi: ACCESS.2021.3096799.

[9] C. Baur, S. Denner, B. Wiestler, S. Albarqouni, and N. Navab, "Autoencoders for Unsupervised Anomaly Segmentation in Brain MR Images: A Comparative Study," *Med Image Anal*, vol. 69, no. 101952, pp. 1-16, Apr. 2021, doi: 10.1016/j.media.2020.101952.

[10] J. S. Park and S. Kim, "Improved Interpolation and Anomaly Detection for Personal PM2.5 Measurement," *Applied Sciences*, vol. 10, no. 2, pp. 1-13, Jan. 2020, doi: 10.3390/app10020543.

[11] D. Wiryadinata, A. Sugiharto, and Tarno, "The Use of Machine Learning to Detect Financial Transaction Fraud: Multiple Benford Law Model for Auditors," *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 2, pp. 239–252, Oct. 2023, doi: 10.20473/jisebi.9.2.239-252.

[12] V. Zaslavsky and A. Strizhak, "Credit Card Fraud Detection using Self Organizing Maps," *Information and Security: An International Journal*, vol. 18, no. 1, pp. 48–63, 2006.

[13] H. Abbassi, S. E. Mendili, and Y. Gahi, "Real-Time Online Banking Fraud Detection Model by Unsupervised Learning Fusion ," *HighTech and Innovation Journal*, vol. 5, no. 1, pp. 185–199, Mar. 2024, doi: 10.28991/hij-2024-05-01-014.

[14] J. Gama, R. P. Ribeiro, S. Mastelini, N. Davari, and B. Veloso, "From fault detection to anomaly explanation: A case study on predictive maintenance," *Journal of Web Semantics*, vol. 81, no. 100821, pp. 1–9, Jul. 2024, doi: 10.1016/j.websem.2024.100821.

[15] S. Misra, S. Thakur, M. Ghosh, and S. K. Saha, "An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction," *Procedia Comput Sci*, vol. 167, no. 159537, pp. 254–262, 2020, doi: 10.1016/j.procs.2020.03.219.

[16] P. Sharma and S. Pote, "Credit Card Fraud Detection using Deep Learning based on Neural Network and Auto-encoder," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 5, pp. 284–288, Jun. 2020, doi: 10.35940/ijeat.E1234.069520.

[17] M. Žarkovi and G. Dobri, "Artificial Intelligence for Energy Theft Detection in Distribution Networks," *Energies (Basel)*, vol. 17, no. 7, p. 1580, Mar. 2024, doi: 10.3390/en17071580.

[18] M. Mahdi and R. Mashhadi, "Anomaly Detection using Unsupervised Methods: Credit Card Fraud Case Study," International *Journal of Advanced Computer Science and Applications*, vol. 10, no. 11, pp. 1–7, Jan. 2019, doi: 10.14569/IJACSA.2019.0101101.

[19] M. A. Al-Shabi, "Credit Card Fraud Detection Using Autoencoder Model in Unbalanced Datasets," *Journal of Advances in Mathematics and Computer Science*, vol. 33, no. 5, pp. 1–16, Aug. 2019, doi: 10.9734/jamcs/2019/v33i530192.

[20] H. Tingfei, C. Guangquan, and H. Kuihua, "Using Variational Auto Encoding in Credit Card Fraud Detection," *IEEE Access*, vol. 8, no. 8, pp. 149841–149853, 2020, doi: 10.1109/ACCESS.2020.3015600.