Unveiling Hidden Patterns: A Deep Learning Framework Utilizing PCA for Fraudulent Scheme Detection in Supply Chain Analytics

Kowshik Sankar Roy[1], Koushik Paul[1], Bashirul Alam[1], Dewan Rakibul Hasan[1], Anej Chakma[1], Sumaiya Binte Haque[1], Md. Joynal Abedin[1], Md. Ariful Islam[1], Nahid Mia[1], Robin Paul[1], Md. Ahsanur Rahman[1]

[1]Department of Statistics and Data Science, Jahangirnagar University, Bangladesh

Abstract

Supply chain fraud, a persistent issue over the decades, has seen a significant rise in both prevalence and sophistication in recent years. In the current landscape of supply chain management, the increasing complexity of fraudulent activities demands the use of advanced analytical tools. Despite numerous studies in this domain, many have fallen short in exploring the full extent of recent developments. Thus, this paper introduces an innovative deep learning-based classification model for fraud detection in supply chain analytics. Addressing dimensionality challenges, the model incorporates Principal Component Analysis (PCA) to streamline data dimensions. Evaluation on the well-established 'DataCo smart supply chain for big data analysis' dataset ensures the model's robustness, achieving notable results. The proposed approach attains an 87% fraud detection rate and an impressive overall accuracy of 99.35%. Comparative analysis with various models underscores the significant enhancement in fraud transaction detection offered by the proposed model.

Keywords

Supply Chain, Fraud Detection, Machine Learning, Deep Learning, Principal Component Analysis

1. Introduction

Supply Chain Management (SCM) is a strategic approach to overseeing the entire lifecycle of goods and services, from their creation or acquisition to their delivery to the end consumer. SCM involves the coordination of various activities, including procurement, production, transportation, warehousing, and distribution, to optimize the overall efficiency and effectiveness of the supply chain. Every company, no matter its size or industry, relies on these networks to function well. Yet, fraud may also occur in supply networks, and this can have a major monetary effect on companies. In a 2020 report of Word Economic Forum (WEF), companies lose trillions of dollars annually due to supply chain fraud. PwC Global Economic Crime Survey 2022 reports that 57% of fraud is committed by insiders or a combination of insiders and outsiders, leading to losses of $50 billion annually for businesses. This includes losses from procurement fraud, employee theft, and other forms of supply chain fraud. However, operational interruptions, reputational harm, legal expenses, and so forth are all forms of SCM losses that can result from fraud. Within the vast landscape of SCM, fraudulent schemes represent a persistent and challenging threat. Fraud in the supply chain can manifest in various ways, including but not limited to misrepresentation of products, theft, counterfeiting, and deceptive practices in transactions. These schemes often exploit vulnerabilities in the complex web of interconnected processes, making detection and prevention critical for maintaining the integrity of the supply chain.

The importance of early detection of fraudulent schemes in SCM cannot be overstated. Timely identification allows for swift intervention and mitigation of potential damages. Financial losses, reputational damage, compromised product quality, and disruptions in the supply chain can be averted or minimized when fraudulent activities are detected early. Detecting fraudulent schemes early requires a proactive and technology-driven approach. Advanced tools and techniques, such as data analytics, machine learning, and deep neural networks, play a pivotal role in uncovering anomalous patterns and behaviors indicative of fraudulent activities. By leveraging these technologies, organizations can establish robust monitoring systems that enhance the resilience of the supply chain against fraudulent threats, ultimately safeguarding both economic interests and consumer trust. Several different approaches are used to detect fraud in the supply chain. These approaches can be broadly divided into two categories, Rule-based approaches and AI based techniques.

Rule-based methodologies are frequently rigid and might provide challenges in staying abreast of the most recent fraudulent techniques. Furthermore, manual fraud detection approaches have a poor level of accuracy, making it exceedingly challenging to manage substantial amounts of data. Machine learning, a branch of artificial intelligence, offers a potential approach to improve the identification and prevention of fraud in complex supply chain networks. Machine learning has the capacity to detect fraudulent trends and adapt to new and complex types of fraudulent behaviors by utilizing advanced algorithms, predictive modeling, and data analytics. Machine learning or deep learning methods can yield superior results, but they want substantial quantities of high-caliber data for training and possess the capability to uncover concealed patterns. Historically, the fraud detection process relied mostly on audit approaches that were deemed inefficient (Abdullah et. al, 2016). Nevertheless, in recent times, corporations have relied on Artificial Intelligence (AI) technology, particularly machine learning (ML) systems (Aziz and Dowling, 2019).

The motivation behind this research stems from the critical importance of securing global supply chains against fraudulent practices. As traditional fraud detection mechanisms struggle to keep pace with the ever-evolving tactics employed by fraudsters, there arises a need for a proactive and intelligent approach that can learn from historical data, recognize anomalies, and continuously improve its effectiveness. In this paper, we propose a novel deep learning framework for fraud detection in supply chain analytics incorporating principal component analysis. Our proposed framework uses a deep neural network to learn complex patterns in data from a variety of sources, including order details, customer information, and shipment information. The framework is able to detect fraudulent transactions with high accuracy and detection rate, even in cases where the fraud is complex or novel. The overall contributions of this work confined intro three segments are stated below:

- In order to detect fraudulent activity in supply chain networks, a unique deep learning architecture has been proposed.
- Principal component analysis has been employed to reduce high-dimensional data into an optimal collection of features. Throughout our effort, the working model avoids the curse of dimensionality problem.
- For the purpose of assessing the operational performance of our proposed framework on a benchmark dataset, a set of evaluation metrics has been deployed.
- To validate the robustness and superiority of the proposed model, performance metrics have been compared across a set of individual ML and deep learning classifiers along with the state-of-the-art models in the supply chain analytics.

The remaining sections of the paper have been organized in the following manner. Section 2 provides a discussion of the works that are related to the topic. Section 3 presents the comprehensive structure of our proposed model, together with a description of the associated dataset. Section 4 provides a comprehensive overview of all the experimental assessments employed in this study. Section 5 pertains to the experimental settings, whereas Section 6 encompasses the essential experimental results and debates of the whole paper. At last, we have reached the conclusion of our effort in Section 7.

2. Literature Review

The fraud detection technology in financial services can be divided into two major categories: Rule based methods and machine or deep learning techniques.

Rule-based methodologies employ a predefined set of rules to detect transactions that are prone to being fraudulent. For instance, a rule could identify a transaction as fraudulent if the order value is abnormally elevated or if the supplier is not listed among the company's authorized vendors. Furthermore, it necessitates costly and proficient domain expert teams and data scientists. Frequently, it necessitates rigorous inquiries into the additional transactions associated with deceitful behavior in order to discern patterns of fraudulent activity. Finance businesses are not achieving sufficient return on investment (ROI) despite the allocation of resources and funds towards these conventional approaches.

Edge & Falcone Sampaio (2012) introduces the financial fraud modelling language, FFML, which is a rule-based policy modeling language and comprehensive architecture. It allows for the conceptual expression and implementation of proactive fraud protection in multi-channel financial service platforms. The work demonstrates the use of a domain-specific language to streamline the financial platform by converting it into a data stream-oriented information model. The objective of this technique is to reduce the intricacy of policy modeling and limit the duration required for policy implementation. It does this via the employment of a new policy mapping language that can be utilized by both expert and non-expert users. The Improved Firefly Miner, Threshold Accepting Miner, and Hybridized Firefly-Threshold Accepting (FFTA) based Miner are new rule-based classifiers that use Firefly (FF) and Threshold Accepting (TA) algorithms. These classifiers are designed to determine if a company's financial statements are fake or not. The authors examine how t-statistic-based feature selection affects outcomes. Both FFTA and TA miners were statistically comparable. According to Pradeep et al. (2015), the two algorithms fared better than the decision tree in terms of sensitivity and rule length. In their study, Vatsa et al. (2007) introduced a two-tiered framework for detecting credit card fraud. This framework incorporates both a rule-based component and a game-theoretic component. The utility of classical game theory lies in its ability to determine optimal strategies regardless of the actions taken by the opponent, hence obviating the necessity for prediction. The study conducted by Yan et al. (2020) investigated the impact of fraud intention analysis on quality inspection. Suppliers and purchasers may engage in several transactions, including with potential fraudsters, in order to gather information about each other during the process of quality inspection. The supply contracts may also affect the profit-seeking behavior of providers. The researchers conducted experiments in a laboratory to evaluate the effectiveness of fraud intention analysis systems on decision making during inspections. They specifically examined the impact of learning and contract effects. The experiment was conducted on a dairy supply chain, which was both fascinating and essential. The experiment shown that analyzing fraud intention might enhance the efficiency of buyers' decision-making, taking into account factors such as decision time, inspection cost, and accuracy in rejecting suppliers' fraudulent shipments, provided that the contract lacks severe repercussions for fraud. The majority of traditional fraud detection approaches mostly concentrated on discrete data points. Nevertheless, these approaches are no longer enough for the demands of the present day. As fraudsters and hackers employ increasingly sophisticated and innovative methods to conceal their fraudulent actions, even from the most discerning observers. To overcome the limitations of standard approaches, an analytical approach is necessary as these methodologies can only identify known attack types (Amarasinghe et al., 2018).

Insufficient capacity to manage large volumes of big data and address financial fraud adequately can result in significant losses within supply chains (Zhou et al., 2020). To solve the problem of handling high dimensional data, many companies inclined to ML or deep learning techniques along with different platforms like Apache spark, Hadoop and so on. Artificial intelligence (AI) is being widely employed in supply chain management with big data to effectively identify and prevent fraudulent behavior. (Baryannis et al., 2019; Constante-Nicolalde et al., 2020; Mao et al., 2018).

The real-time application benefits from the efficient and effective outcomes provided by machine learning techniques. Several techniques have been used to achieve the desired outcomes. XGBoost, LR, RF, and DT are the most often used techniques (Maurya et al, 2022). In contrast to earlier writers that employed conventional techniques, Forough & Momtazi (2021) developed an ensemble model that utilizes deep recurrent neural networks and a distinctive voting mechanism based on artificial neural networks to detect fraudulent transactions. The model is specifically designed for sequential data modeling. Two real-world datasets were used by the authors to illustrate the suggested work. The transaction data that represented the behavior of the customers was collected and analyzed by Gao et al. (2021). They combined deep learning techniques with the machine learning approach, rather than relying only on it. In recent times, businesses have become reliant on machine learning systems and artificial intelligence (AI) technologies (Aziz & Dowling, 2018).

A study examined five distinct supervised learning approaches, including LR, MLP, Boosted Tree, RF and SVM. Upon comparing the results, the boosted tree model demonstrated the highest efficacy in detecting fraud, achieving a 49.83% fraud detection rate for the specified dataset (Gao et al., 2019). SVM with a specialized financial kernel was used for management fraud detection in Cecchini et al. (2010). Leveraging basic financial data, the SVM model correctly classified 80% of fraudulent cases and 90.6% of legitimate cases on a holdout set. This highlights the efficacy of SVMs in discerning fraudulent patterns and underscores the potential of this approach in enhancing current fraud detection strategies. In another study of fraud detection in credit card transactions, the XGBoost algortihms exhibits a high AUC of 0.99, but moving towards its peak may increase false positives, risking misclassification (Maurya et al, 2022). Abouloifa & Bahaj (2023) introduce a machine learning framework for predicting fraudulent activities within Supply Chain links, employing RF, KNN, and LR algorithms. The optimal model is enhanced through grid search cross-validation, demonstrating increased efficiency with a 97.7% accuracy score (Abouloifa & Bahaj, 2023). In another study of credit card fraud detection LR, RF, Naive Bayes (NB), and Multilayer Perceptron (MLP) algorithms, revealing their high accuracy. The proposed model extends applicability to detecting various irregularities (Varmedja et al, 2019). Dong et al. (2021) presented SVM as better model comparing LR and Naïve Bayes with 98.61% overall classification accuracy by using DataCo supply chain dataset. The authors Nguyen et al. (2021) presented two data-driven methodologies that enhance decision-making in supply chain management. The proposed anomaly detection technique for multivariate time series data shows superior performance when utilizing the LSTM Autoencoder network, particularly in the context of supply chain management. The DataCo Supply Chain Dataset for Bigdata Analysis was used in Wan (2021) for developing fraud detection hybrid model incorporating XgBoost and Random Forest algorithms. Zhou et al. (2020) propose distributed big data mining for supply network financial fraud detection. The method uses a distributed deep learning model, CNN. It uses Apache Spark and Hadoop's big data technology. This method speeds up parallel processing of large datasets to substantially reduce processing times. The proposed method intelligently classifies huge data samples using training and testing on the continuously updated Supply Chain Finance (SCF) dataset to detect fraudulent financing operations. This study develops and runs CNN, SVM, and Decision Tree algorithms using Apache Spark. During repeated training, the CNN model detects more financial fraud cases and less normal samples as false positives. CNN model's highest accuracy is about 93% and average precision is above 91% and consistently outperforms the other two models. These findings enhance distributed deep learning research for supply chain financial fraud detection.

3. Proposed Approach

In this paper, we introduce a novel hybrid method for detecting fraudulent transactions in the supply chain using a deep neural network (DNN) with a focus on principal component analysis (PCA). To facilitate a comprehensive understanding of our proposed approach's workflow and architecture, this section is organized into four sequential sub-sections. Sub-section 3.1 provides an overview of our proposed model and its general architecture. Sub-section 3.2 delineates the characteristics of the dataset utilized in this study. The pre-processing unit of our model, addressing feature transformation and dimensionality reduction, is thoroughly explained in sub-section 3.3.

Finally, sub-section 3.4 delves into the detailed analysis of the model designed for identifying fraudulent schemes, succinctly outlining each fundamental element of the overall model.

3.1 Proposed Architecture

Illustrated in Fig. 1, our proposed model comprises two core components: a pre-processing unit and a DNN model for the classification phase. The initial segment of the pre-processing unit handles feature transformation, beginning with the removal of irrelevant features. Each ordinal feature is then converted into a label-encoded format, representing each input byte as an n-dimensional vector. Subsequently, a data standardization operation is applied after numerical representation conversion. The second segment involves a dimensionality reduction unit aimed at addressing the curse of dimensionality. PCA serves as the foundation for this feature reduction operation. Utilizing PCA, the chosen features from the datasets are transformed into a specific number of principal components, from which only a selected few are retained for the detection model. This process is consistent for both the training and testing datasets. Following the completion of the pre-processing unit, the reduced and transformed features are directed into the DNN model, which plays a pivotal role in fraud transaction detection.

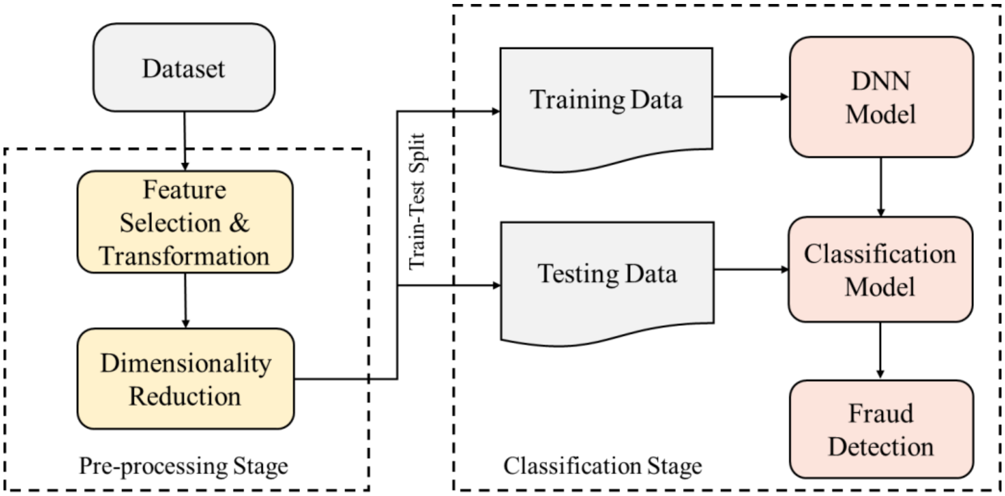


Fig. 1: Overview of proposed architecture

3.2 Dataset Description

In order to assess the efficacy and dependability of any fraud detection technology, a proficient dataset is required. An effective dataset comprises a substantial quantity of precise data that accurately represents actual networks in the real world. We have utilized the well-recognized public supply chain dataset called DataCo SMART SUPPLY CHAIN FOR BIG DATA ANALYSIS for our research in this article (Constante-Nicolalde et al., 2019). The dataset has collected from Kaggle that was created to help people understand how big data can be used to improve supply chain efficiency. The dataset contains data on orders, shipments, and customers from a large e-commerce company. This data can be used to analyze trends in customer behavior, identify areas for improvement in the supply chain, and optimize the company's logistics operations. It can be used to improve the efficiency, effectiveness, and profitability of supply chains. Table 1 illustrates the description of the dataset.

Table 1

List of variables with data types

SL No.	FIELDS	TYPES OF VARIABLES	SL No.	FIELDS	TYPES OF VARIABLES
1	Type	Categorical	28	Order Customer Id	Id
2	Days for shipping (real)	Numerical	29	Order date (Date Orders)	Date-Time
3	Days for shipment (scheduled)	Numerical	30	Order Id	Id
4	Benefit per order	Numerical	31	Order Item Cardprod Id	Id
5	Sales per customer	Numerical	32	Order Item Discount	Numerical
6	Delivery Status	Categorical	33	Order Item Discount Rate	Numerical
7	Late_delivery_risk	Numerical	34	Order Item Id	Id
8	Category Id	Id	35	Order Item Product Price	Numerical
9	Category Name	Categorical	36	Order Item Profit Ratio	Numerical
10	Customer City	Categorical	37	Order Item Quantity	Numerical
11	Customer Country	Categorical	38	Sales	Numerical
12	Customer Email	Text	39	Order Item Total	Numerical
13	Customer Fname	Text	40	Order Profit Per Order	Numerical
14	Customer Id	Id	41	Order Region	Categorical
15	Customer Lname	Text	42	Order State	Categorical
16	Customer Password	Id	43	Order Status	Categorical
17	Customer Segment	Categorical	44	Order Zip code	Numerical
18	Customer State	Categorical	45	Product Card Id	Id

19	Customer Street	Categorical	46	Product Category Id	Id
20	Customer Zip code	Id	47	Product Description	Text
21	Department Id	Id	48	Product Image	Text
22	Department Name	Text	49	Product Name	Text
23	Latitude	Numerical	50	Product Price	Numerical
24	Longitude	Numerical	51	Product Status	Categorical
25	Market	Categorical	52	Shipping date (Date Orders)	Date-Time
26	Order City	Categorical	53	Shipping Mode	Categorical
27	Order Country	Categorical			

Table 1 reveals that the dataset comprises 53 variables or features of varying data types and Fig. 2 demonstrates the count of different types of variables.

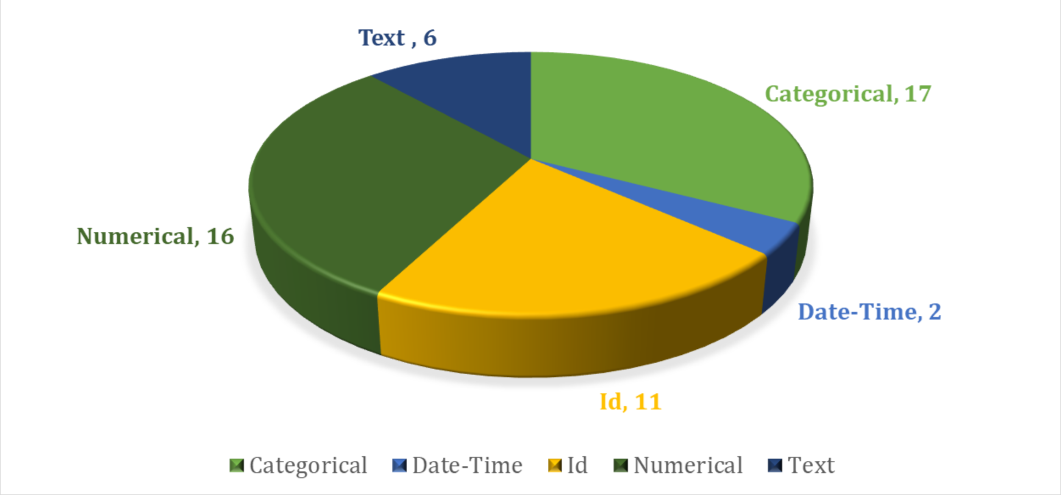


Fig 2: Breakdown of variable types

3.3 Data Cleaning and Preprocessing

In our dataset, the pre-processing stage encompasses two consecutive steps: feature selection and transformation, followed by dimensionality reduction.

Several redundant variables have been eliminated from the dataset. Variables related to customer demographics, such as 'Customer Email,' 'Product Status,' 'Customer Password,' 'Customer Street,' 'Customer Fname,' 'Customer Lname,' 'Customer Zipcode,' 'Product Description,' 'Product Image,' and 'Order Zipcode,' have been removed, as they wouldn't contribute to creating classification models. Additionally, numeric variables serving as unique IDs for departments or products, including 'Category Id,' 'Customer Id,' 'Department Id,' 'Order Customer Id,' 'Order Id,' 'Order Item Cardprod Id,' 'Order Customer Id,' 'Order Item Id,' 'Product Card Id,' and 'Product Category Id,' have been excluded from the dataset. Furthermore, 'order date (Date Orders)' and 'shipping date (Date Orders)' variables have been dropped as the year, month, and day have already been extracted for use in the model.

In this stage of pre-processing, both numericalization and standardization of the data have been implemented. To address the limitation of machine learning algorithms in handling categorical features, numericalization of the data was prioritized in the initial steps. As the dataset contains 17 categorical features, label encoding was employed to convert non-numeric values into a numeric format. Although one hot encoding is another commonly used method for this purpose, it has the drawback of generating a substantial number of new dimensions by assigning binary vectors to nominal data.

After selecting the relevant features, the dataset has been split into training and testing sets with a ratio of 80% to 20% where random seed is 42. Before feeding the data into the model, we labeled the "Suspected_Fraud" transactions as 1 and the rest of the "Order Status" transactions as 0, indicating legitimate transactions. The count of two kinds of transactions in the supply chain has been shown in Table 2 along with breakdown of label data of train and test set.

Table 2:

Number of records of each class

Order Status	Total	Train Data	Test Data
Legitimate	176457	141203	35254
Fraud	4062	3212	850

The heatmap of Fig. 3 represents the correlation or strength of the relationship between each feature. Here it can be seen that the number of high correlated variables are comparatively low, which is good for the classification model. Low correlation suggests that each variable contributes unique and independent information to the model, allowing it to capture a broader range of patterns and relationships in the data. This independence can lead to improved model performance, as the variables provide diverse perspectives and avoid introducing multicollinearity issues. Additionally, low correlation enhances the interpretability of the model, as the influence of each variable can be more easily discerned, facilitating a better understanding of the underlying features driving the classification outcomes.

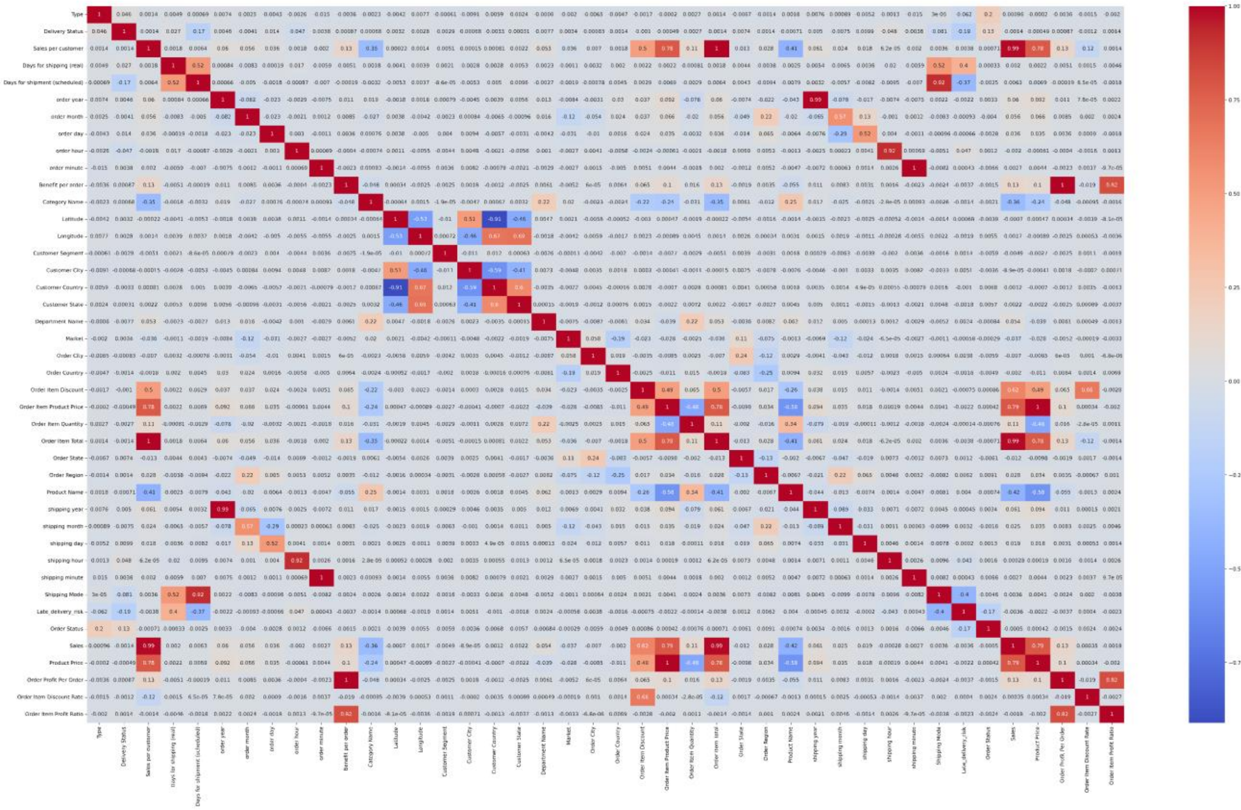


Fig 3: Heatmap of correlated variables

The objective of feature scaling is to bring all features in the dataset to a nearly equal scale, facilitating analysis by most machine learning algorithms. In this study, standardization was chosen for feature scaling, proving to be more effective than the traditional min–max normalization approach. Following label encoding, standardization was implemented to rescale all features, ensuring a mean of 0 and a standard deviation of 1, resulting in a distribution that is centered around zero and has a consistent scale. This makes it easier for machine learning algorithms to converge and perform well, especially in cases where features have different units or magnitudes. The formula is expressed as follows in Eq 1:

$$s = \frac{x - \text{mean}(x)}{\text{std}(x)} \tag{1}$$

where std means standard deviation, s is the standardized value of the feature and x represents original value of the feature.

A lot of research has shown that the ability of any classifier to predict things gets better as the number of variables of the training samples rises. But work starts to fall apart after a while. Because of this, the event is called the "curse of dimensionality" (Udas et al., 2022). For the purpose of getting rid of this problem in our model, PCA has been used. It helps reduce the size of the information to a level that you want. Once the main parts of the real features have been found, the variation level of each feature has been used to choose the smallest number of features. In this way, the model stays free of any very high levels of complexity. One quick look at the model's pre-processing stage can be seen in Fig. 4.

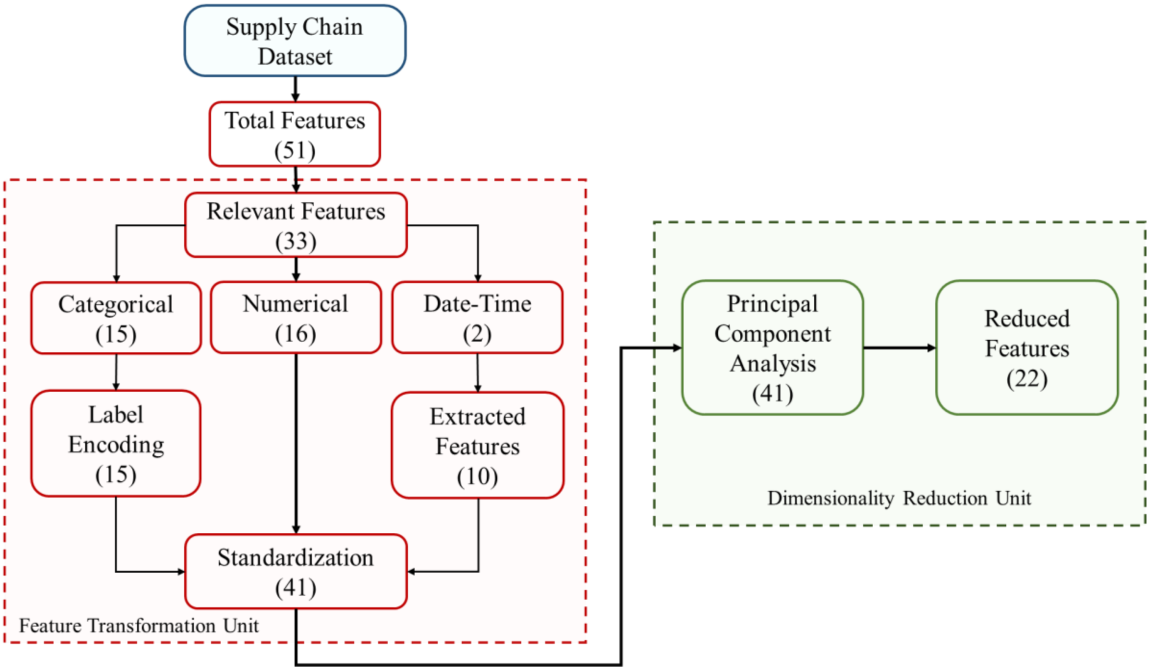


Fig. 4: The procedural flow during the pre-processing stage.

PCA is a method that doesn't rely on class labels to identify the most important features in a dataset. This means that the components found by PCA will be the same regardless of how the data is labeled. The importance of a component is determined by how much of the variation in the data it explains. In the dataset used in this study, the first 22 components account for more than 90% of the variation in the data which is shown in Fig. 5.

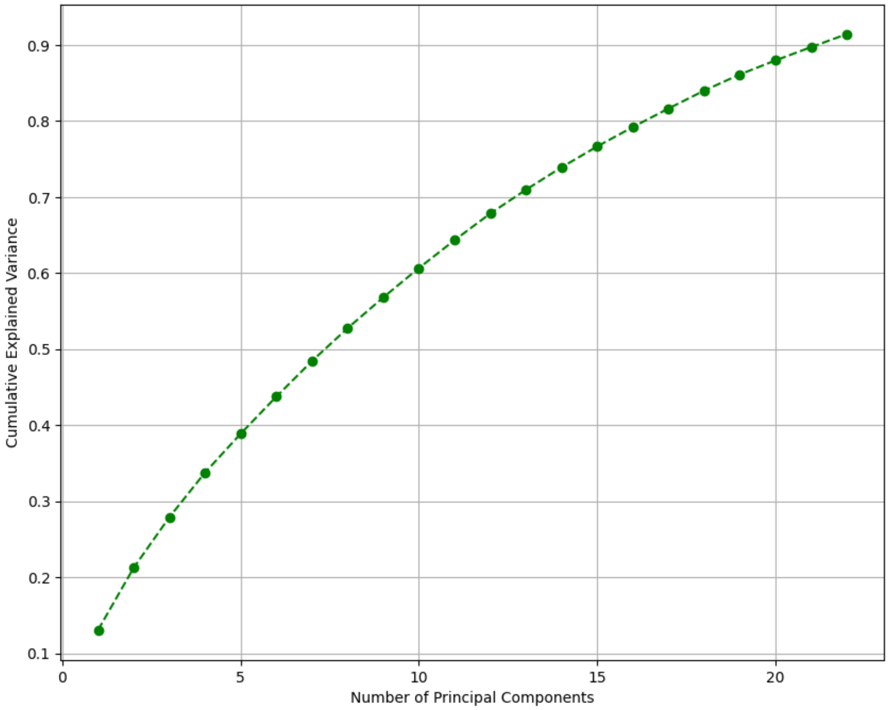


Fig. 5: Cumulative Explained Variance for PCA Components

3.4 DNN Model

After using PCA to reduce the number of features, a deep neural network was created to classify the data. The reduced set of features was used as the input to the neural network. The deep neural network consists of four fully connected layers, and the final layer uses a sigmoid function to activate the output. The details of the parameters of the neural network are provided in Table 3. The remaining details of the model are outlined in subsection 3.4.1.

Table 3

Parameters of the deep learning classifier

Hyper-Parameters	Functions/ Values
Dense Layer (1)	Activation = ReLu, Neurons = 512
Dense Layer (2)	Activation = ReLu, Neurons = 128
Dense Layer (3)	Activation = ReLu, Neurons = 64
Dense Layer (4)	Activation = Sigmoid, Neurons = 1
Learning Rate	0.001
Cost Function	Binary Cross Entropy
Batch Size	64
Optimizer	Adam
Iterations	200

3.4.1 Dense Layers

A dense layer, commonly referred to as a fully connected layer, is an essential component in deep neural networks. Each neuron in a layer is linked to every neuron in the subsequent layer, which is a defining characteristic. The term "dense" refers to the dense connections between neurons. The architecture of a dense layer involves weights and biases, which are parameters that the neural network learns during the training process (Roy et al., 2023).

Here's a more detailed breakdown of the dense layer architecture:

- Neurons/Nodes: Each node in a dense layer represents an artificial neuron. The number of nodes in a dense layer is the layer's width or size.
- Weights: Each connection between neurons in adjacent layers has a weight associated with it. Weights refer to parameters that the neural network acquires through the training process, and they play a crucial role in determining the intensity of connections between neurons.
- Biases: Every neuron in a dense layer is associated with a bias. Biases allow the model to account for situations where all input features are zero.
- Activation Function: Each neuron typically has an activation function that introduces non-linearity to the network. The sigmoid, the rectified linear unit (ReLU), and the hyperbolic tangent (tanh) are all common activation functions.
- Forward Pass: During the forward pass, input data is multiplied by weights, and the biases are added to the result. The sum is then passed through the activation function to introduce non-linearity.
- Training: During training, the weights and biases are adjusted using optimization algorithms such as gradient descent. The model learns to minimize the difference between its predictions and the actual target values.
- Backpropagation: Backpropagation is the process by which the neural network adjusts its weights and biases based on the error calculated during training. This process entails calculating the gradients of the loss function in relation to the weights and biases, and subsequently adjusting them based on these gradients.

The architecture of deep learning models often involves stacking multiple dense layers along with other types of layers like convolutional layers and recurrent layers. This hierarchical structure allows deep neural networks to learn complex hierarchical representations of data, capturing intricate patterns and relationships. The fundamental dataflow diagram of dense layer architecture is represented in Fig.6.

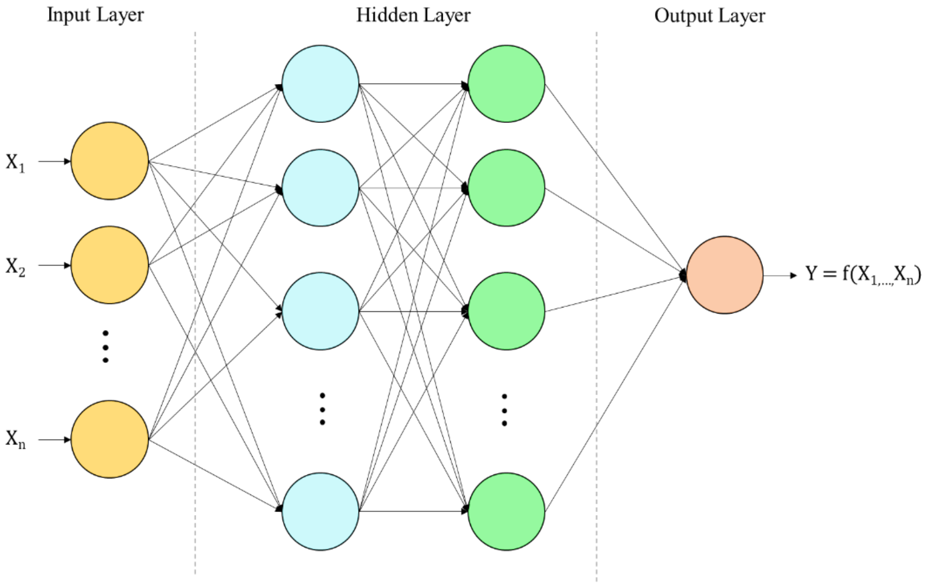


Fig. 6: Dense layer architecture

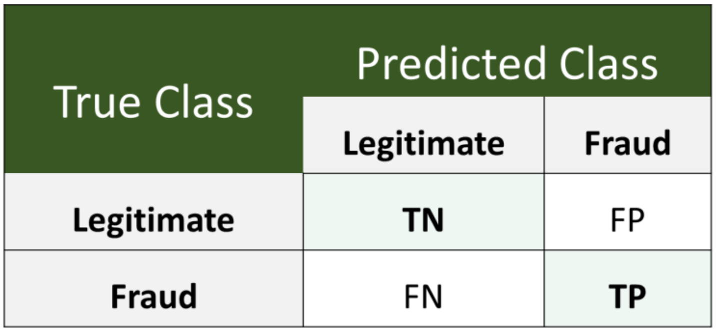
Given the exhibited class imbalance in the dataset and the presence of highly collinear features, employing a Deep Neural Network (DNN) is considered a suitable choice to address the problem. Deep neural networks (DNNs) can address data imbalance and multicollinearity issues through their inherent capacity to learn hierarchical representations of data. In the case of data imbalance, DNNs can adaptively assign different weights to under-represented classes during training, mitigating the bias towards the majority class. Additionally, techniques like oversampling and under sampling can be integrated into the training process. Regarding multicollinearity, the deep architecture of neural networks enables them to automatically extract relevant features and hierarchies, reducing the impact of redundant or highly correlated input features. This intrinsic ability to learn complex relationships allows DNNs to handle imbalanced datasets and multicollinear features, making them robust and effective in various real-world applications.

4. Experimental setup

The research that was done for this work was done using the programming language Python, especially version 3.6.9. Python tools that are often used, like Pandas and Numpy, were used to analyze the data. Keras, a deep-learning API that works on the Tensorflow platform, was used to put deep learning models into action. Using a TPU, all tasks related to the project were done on Google Colaboratory.

5. Evaluation Metrics

The assessment of a model's effectiveness in any detection system depends on its evaluation metrics, specifically the confusion matrix. This matrix serves as a comprehensive representation of a classification algorithm's performance, offering essential relative information. For his study, four widely recognized performance metrics—Accuracy, Precision, F1-Score, and Recall—have been extracted from the confusion matrix of the detection model.



True Class	Predicted Class	
	Legitimate	**Fraud**
Legitimate	**TN**	FP
Fraud	FN	**TP**

Fig. 7: Confusion Matrix

Fig. 7 illustrates the confusion matrix, delineating four potential outcomes. The analysis of overall results is based on these outcomes, and it involves the utilization of the four most commonly employed evaluation metrics:

- TN (True Negative): Instances of legitimate correctly classified by the classifier.
- FP (False Positive): Instances of legitimate misclassified by the classifier.
- FN (False Negative): Instances of fraud misclassified by the classifier.
- TP (True Positive): Instances of fraud correctly classified by the classifier.

I. Accuracy: Determines the proportion of correctly classified test instances relative to the total number of test instances.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{2}$$

II. Precision: Measures how many instances that were predicted as positive were actually positive.

$$Precision = \frac{TP}{TP+FP} \tag{3}$$

III. Recall (Detection Rate, True Positive Rate): The proportion of positive instances in the test set that were accurately identified in relation to the overall count of positive instances.

$$Recall = \frac{TP}{TP+FN} \tag{4}$$

IV. F1 Score: The harmonic average of precision and recall is interpreted, creating a balance between the two measurements.

$$F1\ Score = \frac{2*Recall*Precision}{Recall+Precision} \tag{5}$$

These metrics are frequently employed to evaluate the efficacy of a classification model, especially in tasks like fraud transaction detection where correctly identifying positive instances (fraud) is crucial, and balancing precision and recall is important.

6. Result Analysis

The performance of the supply chain fraud transaction detection model is gauged by its evaluation metric scores. In an effort to make the findings of this study more understandable, they have been divided into two distinct periods. Performance criteria for binary classification are outlined in the first phase of the segment. After that, Phase 2 provides a comparative study of the total findings, taking into account individual machine learning and deep learning classifiers in addition to models that are considered to be state-of-the-art in the relevant sector.

Phase 1: Results of classification using both the actual and reduced features

As indicated in Table 2, it is evident that the classes of the order status variable exhibit imbalance. Consequently, we evaluated our proposed model using weighted metrics. Given that our model is designed for early fraud transaction detection in the supply chain, our primary focus was on the fraud detection rate. The evaluation metrics, derived from the confusion matrix, are displayed in Table 4. The model underwent evaluation both before and after employing PCA. Interestingly, the deep learning model performed better without using PCA compared to its performance with PCA. Specifically, we observed a 0.07% improvement in accuracy without PCA, but a 1% higher fraud detection rate with PCA. A set of 22 principal components was chosen, as they collectively explain a substantial percentage of the variance in the dataset. This selection did not lead to a noteworthy decrease in accuracy but contributed to improved computational efficiency, highlighting the effectiveness of retaining key information while reducing the dimensionality of the features. Moreover, the training and testing times with PCA were significantly lower due to dimensionality reduction, achieving a reduction rate of 46.34%. Due to a smaller amount of data in the training set, a noticeable decline in performance has been observed for instances labeled as suspected fraud when compared to the legitimate class.

Table 4

Comparison of performance between actual and reduced features

Measure	With PCA (%)	Without PCA (%)
Overall Accuracy	99.35	**99.42**
Weighted Precision	99.34	**99.41**
Weighted Recall	99.35	**99.42**
Weighted F1- Score	99.35	**99.42**
Fraud Detection Rate	**87**	86
Training Time (Seconds)	**2715**	3350
Testing Time (Seconds)	**85**	128

In Fig. 8, the observation indicates that when our model does not incorporate PCA, it covers a slightly larger area compared to the model that doesn't use PCA. Nevertheless, in both categories, the balance between the true positive rate (TPR) and false positive rate (FPR) at various threshold values demonstrates exceptional performance.

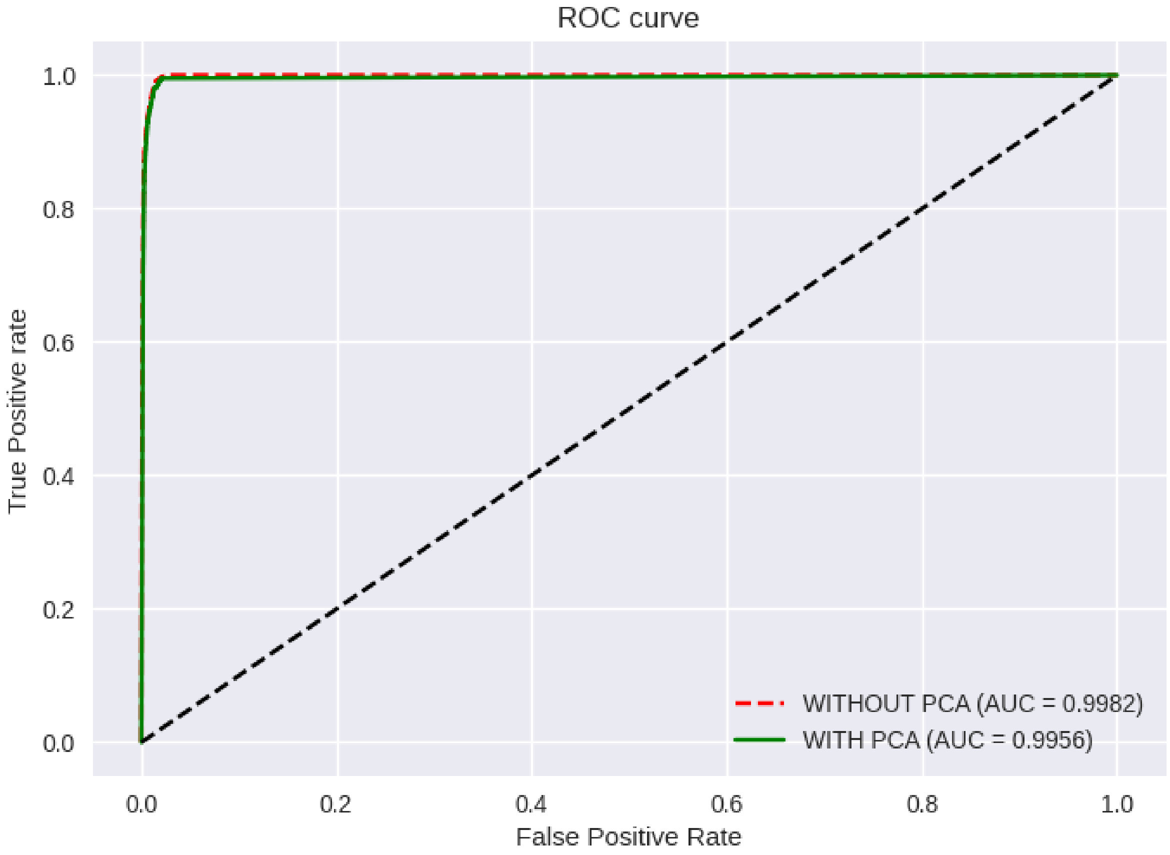


Fig. 8: ROC curve for the classification model

Phase 2: Comparisons of other approaches and earlier works

In order to demonstrate the efficacy of the proposed model in a wider scope, the complete procedure has been replicated for several conventional machine learning and deep learning classifiers. For this instance, there are no modifications made to any of the preparatory phases in the entire procedure. It has been shown in Table 5 that a comparison has been made between the proposed fraud detection model and other conventional models. In terms of accuracy, the only model that outperforms the one we propose is the random forest model; nevertheless, our proposed model beats any other model by a minimum of 5% in terms of the fraud detection rate.

Table 5

Comparison of the proposed classifier model to others.

Model	Overall Accuracy	Fraud Detection Rate
RF	**99.47**	81
DT	99.21	82
SVM	98.11	30
KNN	98.02	20
MLP	98.81	70
Proposed Approach	99.35	**87**

The proposed supply chain fraud detection model has been compared with existing state-of-the-art fraud classification models in Table 6. This table includes metrics commonly used in various studies, such as accuracy, recall, and F1-score, enabling a comprehensive model comparison. Researchers in this field have employed diverse categorization algorithms for fraud analysis. In Baryannis et al. (2019), the authors validated their proposed methodology using a supply chain risk management dataset, where SVM exhibited superior classification results. Zhou et al. (2020) achieved 93% accuracy with the SCF dataset by employing CNN. Several studies utilized the DataCo smart supply chain dataset for big data analysis. Dong et al. (2021) and Lokanan & Maddhesia (2022) employed SVM and ANN techniques, achieving impressive accuracies of 98.61% and 99%, respectively. A hybrid model with Xgboost and random forest was developed in Wan (2021), attaining a remarkable F1-score of 99.45%, although the fraud detection rate was not sufficiently high. The confusion matrix in the research indicated that the true positive value was not significantly high. Upon reviewing the table, it is evident that the proposed methods exhibit superior detection accuracy and fraud detection rates compared to previously conducted research.

Table 6

Comparison of the proposed approach to state-of-the-art

Study	DataSet	Method	Results
Baryannis et al. (2019)	Supply chain risk management Dataset	SVM	Recall-97.3%
Forough & Momtazi (2021)	European and Brazilian Credit Card data set	LSTM	Accuracy-88.47%
Wan (2021)	DataCo SMART SUPPLY CHAIN	Xgboost and RF	F1 Score- 99.45%
Zhou et al. (2020)	Supply Chain Finance (SCF) dataset	CNN	Accuracy-93%
Dong et al. (2021)	DataCo SMART SUPPLY CHAIN	SVM	Accuracy-98.61%
Lokanan & Maddhesia (2022)	DataCo SMART SUPPLY CHAIN	ANN	Accuracy-99%
Proposed Approach	DataCo SMART SUPPLY CHAIN	DNN	Accuracy/Recall/ F1 Score-99.35%

7. Conclusion and Future Work

Fraud in supply chain management is a serious and growing problem that can have a significant impact on businesses of all sizes. It can occur at any stage of the supply chain, from procurement to delivery, and can involve a wide variety of activities. The ability to detect the fraud transaction early on is crucial for preventing business from significant financial losses. Prior studies on fraud detection in supply chain management (SCM) have produced a significant amount of research, with most of these studies employing a rule-based method to identify fraud. But in recent years, the work which has been done by using machine learning approaches mostly uses conventional algorithms which have limitations to handling big data. The proposed methodology extends beyond the construction of a deep learning classifier for the purpose of identifying suspicious transactions to incorporate feature engineering. The computational procedure for evaluating real patterns may be jeopardized due to the high dimensionality of the data, which is prevalent in machine learning applications. Here, by using Principal Component Analysis, the number of components covers more than 90% cumulative explained variance, which reduced computing complexity and enhanced model performance.

In order to fulfill the research objectives, the proposed methodology aimed to utilize a deep learning classifier incorporating data standardization and dimensionality reduction. The final model was developed utilizing the "DataCo SMART SUPPLY CHAIN FOR BIG DATA ANALYSIS" dataset and four evaluation metrics, in addition to the rate of fraud detection and computation time. By employing PCA, the most favorable results were demonstrated, including an overall accuracy of 99.35%, a fraud detection rate of 87%, along with a reduction in computational time. Furthermore, performance of the model was compared with several conventional machine learning and deep learning classifiers along with relevant works focusing on fraud detection in SCM, which revealed that the proposed approach performs better with higher classification accuracy and detection rate. Moving forward, continued focus will be placed on improving the effectiveness and dependability of the detection model. By employing this enhancement in a comparable manner across diverse supply chain analytics datasets, the intended results are to be enhanced. Additionally, automating hyperparameter tuning with a sophisticated algorithm could further improve model performance while significantly simplifying its overall complexity.

References:

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

Abouloifa, H., & Bahaj, M. (2023). Fraud Detection in Supply Chain 4.0: A Machine Learning Model. International Conference on Advanced Intelligent Systems for Sustainable Development, 200–206. https://doi.org/10.1007/978-3-031-35245-4_19

Amarasinghe, T., Aponso, A., & Krishnarajah, N. (2018, May 19). Critical Analysis of Machine Learning Based Approaches for Fraud Detection in Financial Transactions. Proceedings of the 2018 International Conference on Machine Learning Technologies. https://doi.org/10.1145/3231884.3231894

Aziz, S., & Dowling, M. (2018, December 7). Machine Learning and AI for Risk Management. Palgrave Studies in Digital Business & Enabling Technologies, 33–50. https://doi.org/10.1007/978-3-030-02330-0_3

Baryannis, G., Dani, S., & Antoniou, G. (2019, December). Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. Future Generation Computer Systems, 101, 993–1004. https://doi.org/10.1016/j.future.2019.07.059

Cecchini, M., Aytug, H., Koehler, G. J., & Pathak, P. (2010). Detecting management fraud in public companies. Management Science, 56(7), 1146–1160. https://doi.org/10.1287/mnsc.1100.1174

Constante-Nicolalde, F. V., Guerra-Terán, P., & Pérez-Medina, J. L. (2020). Fraud Prediction in Smart Supply Chains Using Machine Learning Techniques. Communications in Computer and Information Science, 145–159. https://doi.org/10.1007/978-3-030-42520-3_12

Constante-Nicolalde, F. V., Silva, F., & Pereira, A. (2019, March 12). DataCo SMART SUPPLY CHAIN FOR BIG DATA ANALYSIS. https://doi.org/10.17632/8gx2fvg2k6.5

Dong, Y., Xie, K., Bohan, Z., & Lin, L. (2021, January). A Machine Learning Model for Product Fraud Detection Based On SVM. 2021 2nd International Conference on Education, Knowledge and Information Management (ICEKIM). https://doi.org/10.1109/icekim52309.2021.00091

Edge, M. E., & Falcone Sampaio, P. R. (2012). The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams. Expert Systems with Applications, 39(11), 9966–9985. https://doi.org/10.1016/j.eswa.2012.01.143

Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 99(106883), 106883. https://doi.org/10.1016/j.asoc.2020.106883

Gao, Jiaxin, Zhou, Z., Ai, J., Xia, B., & Coggeshall, S. (2019). Predicting credit card transaction fraud using machine learning algorithms. Journal of Intelligent Learning Systems and Applications, 11(03), 33–63. https://doi.org/10.4236/jilsa.2019.113003

Gao, Jing, Sun, W., & Sui, X. (2021). Research on default prediction for credit card users based on XGBoost-LSTM model. Discrete Dynamics in Nature and Society, 2021, 1–13. https://doi.org/10.1155/2021/5080472

Lokanan, M., & Maddhesia, V. (2022). Supply chain fraud prediction with machine learning and artificial intelligence. In Research Square. https://doi.org/10.21203/rs.3.rs-1996324/v1

Mao, D., Wang, F., Hao, Z., & Li, H. (2018). Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. International Journal of Environmental Research and Public Health, 15(8), 1627. https://doi.org/10.3390/ijerph15081627

Maurya, A., Kumar, A., & Prakash, S. (2022). Credit Card Fraud Detection using XGBoost classifier with a threshold value. In Research Square. https://doi.org/10.21203/rs.3.rs-1722294/v1

Nguyen, H. D., Tran, K. P., Thomassey, S., & Hamad, M. (2021). Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management. International Journal of Information Management, 57(102282), 102282. https://doi.org/10.1016/j.ijinfomgt.2020.102282

Pradeep, G., Ravi, V., Nandan, K., Deekshatulu, B. L., Bose, I., & Aditya, A. (2015). Fraud Detection in Financial Statements Using Evolutionary Computation Based Rule Miners. Swarm, Evolutionary, and Memetic Computing, 239–250. https://doi.org/10.1007/978-3-319-20294-5_21

Roy, K. S., Ahmed, T., Udas, P. B., Karim, M. E., & Majumdar, S. (2023, November). MalHyStack: A hybrid stacked ensemble learning framework with feature engineering schemes for obfuscated malware analysis. Intelligent Systems With Applications, 20, 200283. https://doi.org/10.1016/j.iswa.2023.200283

Udas, P. B., Karim, M. E., & Roy, K. S. (2022, November). SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks. Journal of King Saud University - Computer and Information Sciences, 34(10), 10246–10272. https://doi.org/10.1016/j.jksuci.2022.10.019

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019, March). Credit Card Fraud Detection - Machine Learning methods. 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH). https://doi.org/10.1109/infoteh.2019.8717766

Vatsa, V., Sural, S., & Majumdar, A. K. (2007). A rule-based and game-theoretic approach to online credit card fraud detection. International journal of information security and privacy, 1(3), 26–46. https://doi.org/10.4018/jisp.2007070103

Wan, F. (2021, March 26). XGBoost Based Supply Chain Fraud Detection Model. 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). https://doi.org/10.1109/icbaie52039

Yan, J., Li, X., Shi, Y., Sun, S., & Wang, H. (2020). The effect of intention analysis-based fraud detection systems in repeated supply Chain quality inspection: A context of learning and contract. Information & Management, 57(3), 103177. https://doi.org/10.1016/j.im.2019.103177

Zhou, H., Sun, G., Fu, S., Fan, X., Jiang, W., Hu, S., & Li, L. (2020). A distributed approach of big data mining for financial fraud detection in a supply chain. Computers, Materials & Continua, 64(2), 1091–1105. https://doi.org/10.32604/cmc.2020.09834