International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 11, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i11.1286

Enhancing Supply Chain Efficiency Through Machine Learning: A Predictive Analytics Approach to Risk Identification and Timely Deliveries

Sadia Ali Watara[1]; Gerardo Moreira[2]; Vincent Anyah[3]

[1,3]Ivan Hilton Center for Science Technology, Department of Computer & Mathematical Sciences, New Mexico Highlands University, Las Vegas, USA
[2]School of Business, Media & Technology, Department of Business Administration, New Mexico Highlands University, Las Vegas, USA

Publication Date: 2025/11/30

Abstract

The present study covers risk identification, development of on-time delivery with the help of machine learning, and predictive analytics for further improvements in supply chain management. Supply chains across the world have turned complex due to the number of involved stakeholders. The after-effect of this factor has been that even minor interruptions of delivery have produced poor results and unexpected dangers that can cause serious harm to operational efficiency and customer satisfaction. In this study, Random Forests, Logistic Regression, and Neural Networks were used. These models enable the use of machine-learning algorithms, which are able to predict possible risks, including those of delayed delivery, using past and current data from supply chain systems. The dataset used in the study was divided into 144,415 training samples and 36,104 test samples, where each sample consists of six features corresponding to six significant variables of the supply chain. The metrics used for the evaluation of the models are precision, recall, accuracy, and AUC-ROC. The Random Forest model developed an accuracy of 97.04% and an AUC score of 0.9728, which shows that it is highly predictive based on those metrics. This performance indicates the model's efficiency in predicting late delivery, which would mean giving supply chain managers critical information they need to drive more-informed decisions toward real-time proactiveness in risk reduction. This paper focuses on the practical use of machine learning in supply chain risk management and proposes a framework integrated with real-time data to optimize operational efficiency for on-time delivery.

Keywords: *Machine Learning; Supply Chain Management; Risk Identification; Late Delivery Prediction; Random Forest; Logistic Regression; Neural Networks; Predictive Analytics; on-Time Delivery*.

I. INTRODUCTION

In the current modern competitive world of a global marketplace, supply chains hold the key by acting as the skeleton for numerous industries which facilitate the transport of commodities and services from production to consumption. Prompt deliveries of goods is not the only goal of any business; it rather serves to improve the quality of the customer's experience and a company's competitive edge. Moreover, among the intricate chain of suppliers, manufacturers, distributors, and retailers, any significant disturbance may delay operations and wreck schedules.

Given the difficulties in this matter, the relationship with machine learning can be a way to improve the process of risk assessment and dealing with such issues inside the supply chain. Using complex algorithms and data analysis, machine learning can perform deep analysis of huge quantities of information that would be impossible to do manually. Thanks to machine learning, patterns can be detected, disruptive processes can be

Watara, S. A., Moreira , G., & Anyah , V. (2025). Enhancing Supply Chain Efficiency Through Machine Learning: A Predictive Analytics Approach to Risk Identification and Timely Deliveries. *International Journal of Scientific Research and Modern Technology*, *4*(11), 196–206. https://doi.org/10.38124/ijsrmt.v4i11.1286

predicted, and decision-making can be improved Naz et al. (2022).

This research centers on the specific problem of risk identification for delivery schedules and its direct impact on customer satisfaction. By means of machine learning, the aim is to shed light on possible risk reduction and productivity improvement, eventually boosting client satisfaction. The research embarks on a review of the literature and empirical studies in order to provide a comprehensive view of the role played by machine learning in solving supply chain problems. The study illustrates the potential utilization of machine learning in handling risks and delivering remarkable performance, going beyond conventional means and applying a multidisciplinary approach that provides organizations with essential advice to help them deal with risks in a timely manner, avoid delays in their operations, and improve customer satisfaction.

II. LITERATURE REVIEW

The literature surrounding supply chain risk management and its impact on timely deliveries and customer satisfaction is vast and multifaceted. This review synthesizes key findings from existing studies, focusing particularly on the role of machine learning in enhancing risk identification within supply chains. Feature engineering was applied to data along with supervised and unsupervised learning methods, with model performance evaluated using metrics like recall, accuracy, and F1-score.

Yeboah-Ofori and Boachie discuss how machine learning can be applied to curb cyber-attacks on the supply chain, emphasizing the need for improving supply chain security using data analytics and prediction. The study revealed that machine learning models were accurate in their prediction of malicious activities within the cyber supply chain. Anomaly detection techniques were instrumental in identifying anomalies within normal cyber supply chain operations Yeboah-Ofori et al. (2019). The Mean-Variance method was applied alongside classification techniques including Decision Tree, Support Vector Machine, and Logistic Regression; these models prevented malware attacks before they happened, which maintained operational continuity, protected customer private information, and preserved the fidelity of their cyber supply chain. These predictive analytics based on machine learning help strengthen cyber supply chain security, including early warning systems.

The work by Zheng et al. focuses on federated machine learning as an approach to collaborative supply chain risk anticipation that assures privacy. Supply chain partners use their local datasets in training collaboratively trained machine learning models, ensuring that they do not compromise private information Zheng, Kong, and Brintrup (2023). Federated Machine Learning proves to be an efficient method to predict whole-supply-chain risks without disclosing personal stakeholder information. The study analyses crucial results, including the suitability of CNN1D (One-Dimensional Convolutional Neural Network) prediction, the discrepancy between pre- and post-COVID-19 forecasts, discrepancies between on-time and delayed orders prediction, and differences between local and global learning processes.

According to Shahzad, Zhang, and Gherbi (2020), the purpose of their research is to improve security and privacy by jointly integrating blockchain technology and proactive elements into IoT supply chain systems. The research highlights the benefits of using blockchain solutions to enhance security and privacy in collaborative IoT-based supply chains and validates concerns about security and privacy with contemporary approaches to handling supply chain data. The paper by Abbas et al. (2020) focuses on blockchain technology and machine learning used for the drug supply chain in the pharmaceutical industry. The study examines the potential use of these technologies as a way of increasing supply chain efficiency and system productivity, using a multidisciplinary approach that employs blockchain technology for data collection and evaluation regarding pharmaceutical supply chain management, forecast of demand, inventory control, and medication distribution.

Hassija et al. (2020), in their survey of supply chain security covering application areas, security threats, and architectural solutions, show that in critical application domains within the supply chain, security plays a major role, especially in transport, inventory control, and logistics. The efficient movement of goods is prone to various security risks, such as natural disasters, cyber-attacks, and counterfeits. Their discussions also highlight how emerging technological methods can work jointly, illustrating the advantages of 5G networks on IoT-type applications and how the Artificial Intelligence of Things (AIoT) influences sectors such as retail, healthcare, and transport Hassija et al. (2020).

Abbas et al. (2022) address the security issues associated with the safety, security, and data privacy of machine learning for IoT applications, underlining the need for incorporating security and privacy issues through a lifetime design cycle and elaborating on different security measures, privacy-enhancing techniques, and risk-reduction actions. Both Hassija et al. (2020) and Abbas et al. (2022) emphasize the importance of maintaining data integrity, ensuring device safety, and protecting privacy in supply chain systems. Authors from all reviewed categories agree on the importance of data security, privacy, and cutting-edge technologies in improving supply chain operations.

III. PROPOSED WORK AND METHODOLOGY

- *Data Collection and Preprocessing*

Supply chain data include customer, shipping, order, sale, shop, and product information Constante et al. (2019). Supply chain data are derived from several sources, such as sales, inventory, manufacturing, warehousing, and transportation Aljohani (2024). Data collection was done through sources such as surveys, interviews with industry experts, and existing datasets, including the identification, access, and integration of different sources of data within the supply chain, abiding by set security regulations. Internal data sources included critical supply chain factors such as lead times, stock levels, previous disruption records, and numerous metrics associated with overall supply chain efficiency. Correctness and consistency were critical because these data were to be used directly to affect the level of accuracy of subsequent analyses.

Data cleaning is a crucial step in any machine learning project, ensuring that the data is reliable and accurate for analysis and modeling Shahzad et al. (2020). The major steps involved in cleaning the data include identification and treatment of all missing values so that biased information due to incomplete data would not occur. These missing values were either replaced with appropriate values mean or median of columns or completely removed from the dataset if necessary. Records were also checked for duplicates and then removed, ensuring that each entry in the data was unique and that no observation redundancy could occur.

- *Feature Engineering and Model Selection*

Feature engineering became a crucial step in the entire research process, where meaningful variables were elaborately chosen and prepared for use as input to the prediction models. These factors have implications for the dynamic nature of supply chain activities and possible risk triggers. Time-dependent properties gave a chance to include temporary patterns and trends in the supply chain, meaning that the historical context of the models would be captured. Contextual variables provide a view on a bigger scale and involve outside factors: market conditions, economic indicators, and geopolitical events. Event indicators helped pinpoint particular occurrences or disruptions that may bring big changes in supply. By thoughtfully engineering features, the predictive power of the models was dramatically improved Deb et al. (2017) and Lippi et al. (2013).

Several models were considered for prediction, including time series analysis, regression, and classification algorithms. Their choice is based on their strength in handling various issues of supply chain risk management. A large volume of the supply chain risk management literature supports these algorithmic decisions Sapankevych & Sankar (2009) and Kuster et al. (2017). The algorithms were chosen based on relevance in the context of supply chain risk management, proven effectiveness in past works, and good applicability to the data at our disposal.

Table 1 Dataset Feature Description, Variable Roles, and Feature Importance Scores

Feature / Variable	Type	Description	Role
Late_delivery_risk	Binary (0/1)	1 = delivery at risk of being late; 0 = not at risk	Dependent variable (target)
Days for shipping (real)	Numerical	Actual number of days taken to ship the order	Independent highest importance (~0.53)
Days for shipment (scheduled)	Numerical	Number of days originally scheduled for shipment	Independent second highest (~0.39)
Benefit per order	Numerical	Profit or benefit associated with the individual order	Independent moderate importance (~0.06)
Sales per customer	Numerical	Total sales amount attributed to the customer	Independent low importance (~0.025)
Product price	Numerical	Selling price of the product after production costs	Independent lowest importance (~0.005)
Dataset split	Train / Test	180,519 total samples: 144,415 training (80%) / 36,104 test (20%), 6 features each	Watara et al (2025)

Source: Watara et al (2025). Feature importance scores derived from the Random Forest model trained on the DataCo Smart Supply Chain dataset.

- *Mathematical Modeling and Training*

The mathematical modeling focuses on predictive analytics, real-time monitoring, and anomaly detection. The basic elements constituting a machine learning model include the input data X comprising a number of features and their respective values, and the output predictions Y. The model parameters theta represent the weights or coefficients associated with each feature, and the goal is minimization of the objective function J, which calculates the difference between predicted and actual values for the training data Russell & Norvig (2010). If y represents the late delivery risk and X represents the independent variables, the late delivery risk is modeled as: y = f(X), where f is the function modeled by a machine learning algorithm. A logistic regression model for predicting late delivery risk expresses P(y=1|X) as a sigmoid function of a linear combination of feature weights and input values, where the coefficients are learned from training data Goodfellow et al. (2016).

Training data comprised 80% of the cleaned dataset 144,415 rows chosen randomly to ensure representative coverage of different delivery patterns and minimize bias. The testing data comprising 36,104 rows was kept strictly separate throughout model development and training.

This is critical for ensuring that the model evaluates on data it has never seen, forming an important step in measuring the ability of the model to generalize on new data.

This section focuses on the mathematical formulation of key tasks in supply chain risk management, including predictive analytics, real-time monitoring, and anomaly detection. These objectives are achieved through the training and validation of machine learning models using both historical and streaming data. The modeling framework enables risk forecasting, continuous system surveillance, and the identification of operational irregularities.

A typical machine learning model consists of input data (X), output predictions (Y), model parameters (\theta), an objective (loss) function (J(θ)), and performance evaluation metrics. The input matrix (X) contains multiple features and their corresponding values, while (Y) represents the target variable, which may correspond to either a class label or a continuous risk score. The parameter vector (θ) denotes the weights or coefficients associated with each feature and determines the mapping between inputs and outputs.

- *The Primary Goal of Model Training is to Obtain Optimal Parameters θ* that Minimize the Objective Function:*

$$\theta^{*}=min_{\theta} j(\theta)$$

Where ($J\theta$) quantifies the discrepancy between predicted and actual values in the training dataset. The training process relies on labeled data, while an independent testing dataset is used to evaluate model generalization. Model performance is assessed using appropriate evaluation metrics, and the learning process is controlled through hyperparameters that influence model behavior and convergence.

This formulation provides the analytical foundation for applying machine learning techniques to supply chain risk management.

➢ *Mathematical Representation*

Let (y) denote the late-delivery risk and (X = $\{x_1, x_2, x_3, \dots \dots \dots \dots, x_n\}$) represent the set of independent variables. The relationship between the predictors and the response variable is expressed as:

$$y = f(X)$$

Where f(.) is the mapping function learned by a statistical or machine learning algorithm.

For a binary risk prediction problem, a logistic regression model can be defined as:

$$P\,(y = 1/X) = \frac{1}{1+e^{-(\beta 0+\beta 1x1+\beta 2x2+\cdots+\beta nxn)}}$$

Where:

- P (y = 1/X) is the probability of late delivery given the feature set (X)
- β0 is the intercept term
- $\beta 0 + \beta 1x1 + \beta 2x2 + \cdots + \beta n$ are the model coefficients learned from the data

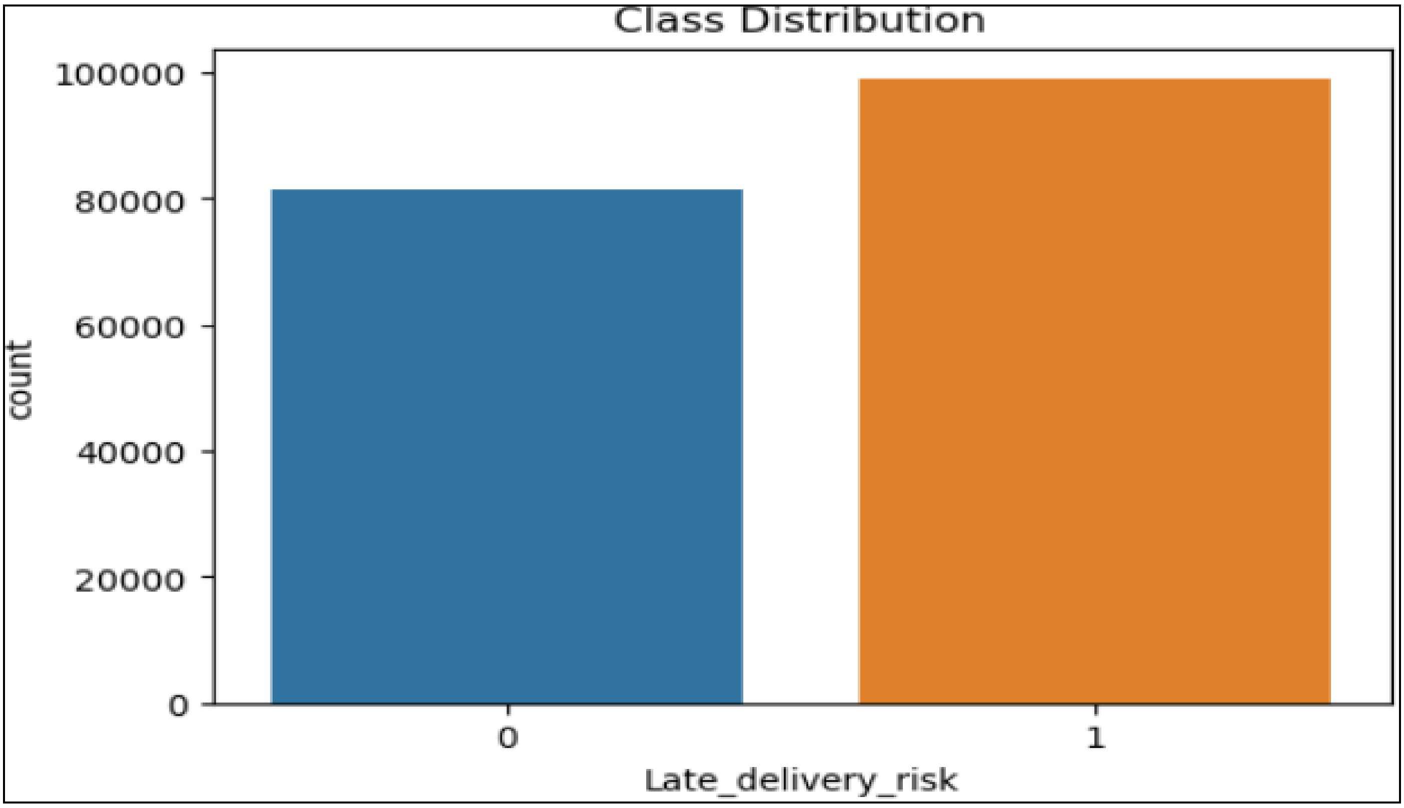

Fig 1 Class Distribution of Late_Delivery_Risk (0 = No Late Risk, ~82,000 Samples; 1 = Late Risk, ~98,000 Samples)

IV. RESULTS

➢ *Logistic Regression Model*

The confusion matrix for the Logistic Regression model reveals the following outcomes on the test set of 36,104 samples. True Negatives: 15,399 correct predictions of No Late Risk for on-time deliveries. False Positives: 908 deliveries incorrectly predicted as Late Risk when they were on time. False Negatives: 0 the model did not misclassify any of the late deliveries as No Late Risk. This is quite significant because it means that the model has 100% recall for predicting late deliveries, which is a critical outcome in risk mitigation. True Positives: 19,797 correctly identified late deliveries. Precision for Class 0 is 1.00 and for Class 1 is 0.96; recall for Class 0 is 0.94 and for Class 1 is 1.00 (perfect). The macro-average accuracy is 97.49% and macro-average F1-score is 0.97.

```
# Generate the confusion matrix for logistic regression
conf_matrix_log_reg = confusion_matrix(y_test, y_pred_log_reg)

# Create a heatmap to display the confusion matrix
plt.figure(figsize=(8, 6))
sns.heatmap(conf_matrix_log_reg, annot=True, fmt="d", cmap="Blues", cbar=False,
            xticklabels=['No Late Risk', 'Late Risk'],
            yticklabels=['No Late Risk', 'Late Risk'])
plt.ylabel('Actual')
plt.xlabel('Predicted')
plt.title('Confusion Matrix - Logistic Regression')
plt.show()
```

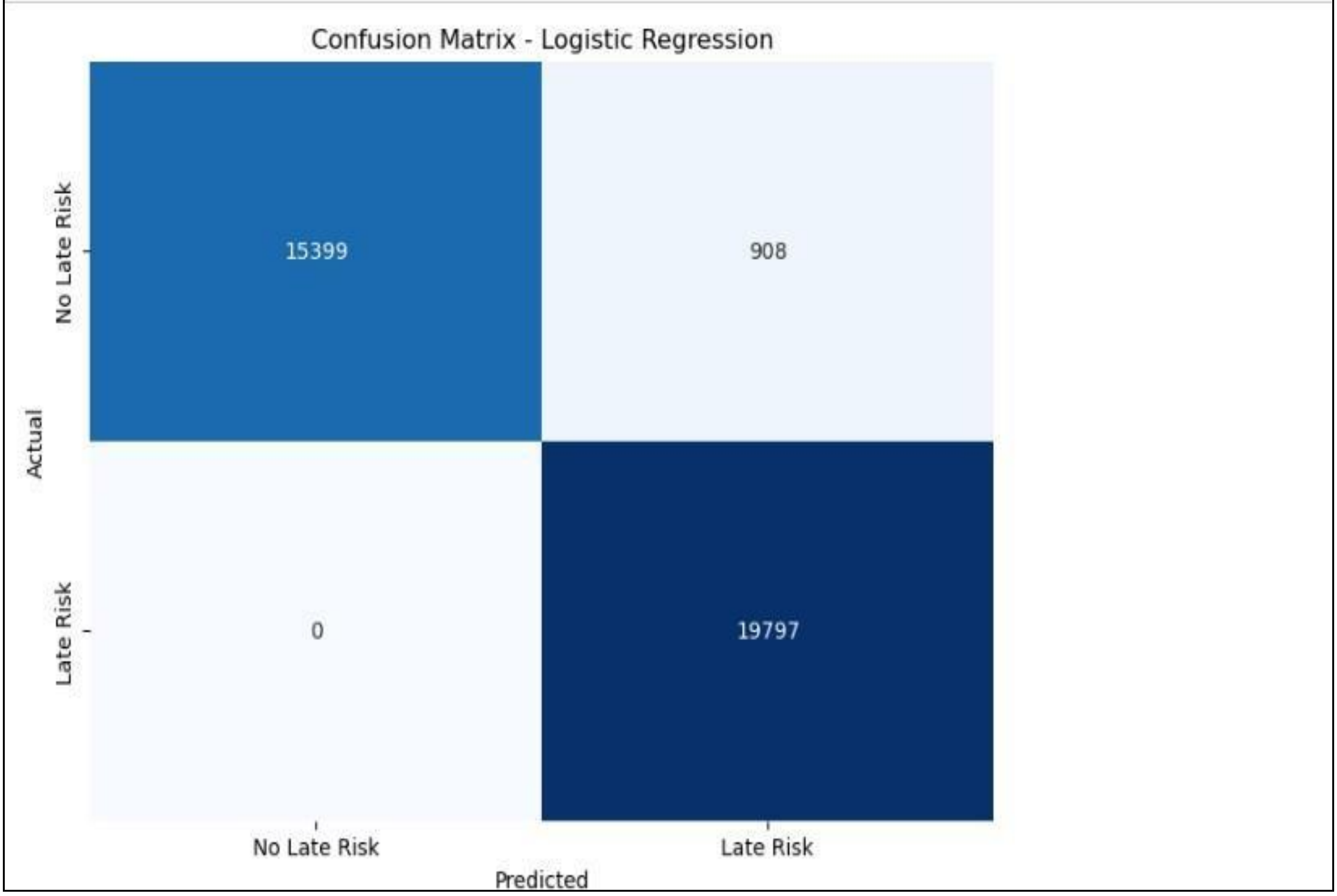

Fig 2 Confusion Matrix Logistic Regression Model (TN: 15,399; FP: 908; FN: 0; TP: 19,797)

➢ *Random Forest Model*

The Random Forest model demonstrated slightly different trade-offs compared to Logistic Regression. True Negatives: 15,406. False Positives: 901 slightly fewer than Logistic Regression's 908. False Negatives: 169 the model failed to predict 169 actual late deliveries, labeling them as No Late Risk. True Positives: 19,628. The Random Forest model developed an accuracy of 97.04% and an AUC score of 0.9728. Precision for Class 1 remains at 0.96; recall for Class 1 is 0.99, reflecting the minor presence of false negatives. At the same time, the model has somewhat lower false positives 901 compared to 908 seen in Logistic Regression indicating that the model may be somewhat better at reducing needless alerts or interventions for predicted late deliveries that actually turn out to be on time.

```
import seaborn as sns
# Create a heatmap to display the confusion matrix
plt.figure(figsize=(8, 6))
sns.heatmap(conf_matrix, annot=True, fmt="d", cmap="Blues", cbar=False,
            xticklabels=['No Late Risk', 'Late Risk'],
            yticklabels=['No Late Risk', 'Late Risk'])
plt.ylabel('Actual')
plt.xlabel('Predicted')
plt.title('Confusion Matrix - Random Forest')
plt.show()
```

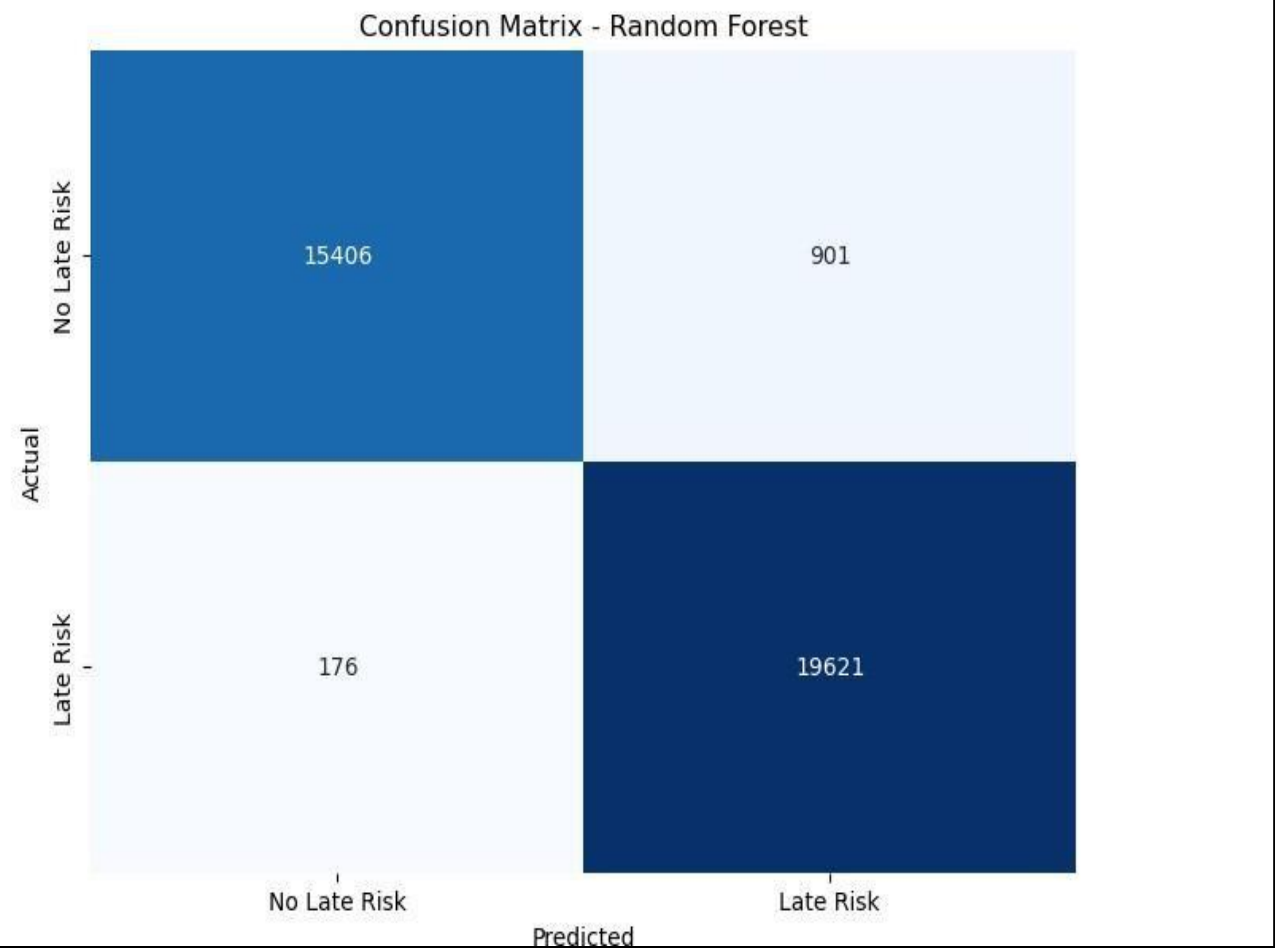

Fig 3 Confusion Matrix   Random Forest Model (TN: 15,406; FP: 901; FN: 169; TP: 19,628; Accuracy: 97.04%)

Table 2 Model Performance Comparison   Logistic Regression, Random Forest

Model	Accuracy	Precision (Class 1)	Recall (Class 1)	F1-Score	AUC
Logistic Regression	97.49%	0.96	1.00 (perfect)	0.98	0.97
Random Forest	97.04%	0.96	0.99	0.97	0.9728
Notes: Class 1 = Late Delivery Risk. Logistic Regression achieved perfect recall (zero false negatives: 0). Random Forest: 169 false negatives, 901 false positives. Both models have macro-average precision, recall, and F1-score of 0.98.					

Source: Watara (2025). All metrics computed on the test set (n = 36,104).

➢ *Feature Importance Analysis*

Knowing which features most strongly drove the model's predictions is crucial in extracting insight into the variables driving late deliveries. A feature importance analysis on the Random Forest provided the following findings. Days for Shipping (Real) had the highest impact on late delivery prediction with an importance score of approximately 0.53; delays were more likely if the actual days of shipping time were higher than expected. Days for Shipment (Scheduled) was second, with an importance score of approximately 0.39. Benefit per Order, Sales per Customer, and Product Price contributed progressively smaller portions of predictive power, with Product Price having the least impact at near-zero importance.

Shipping Mode was also identified as highly significant: some shipping modes, such as standard versus expedited, showed meaningful differences, with fewer delays equating to expedited shipping. Product Category played a key role as well; products that were higher priced or required special handling were more susceptible to being late.

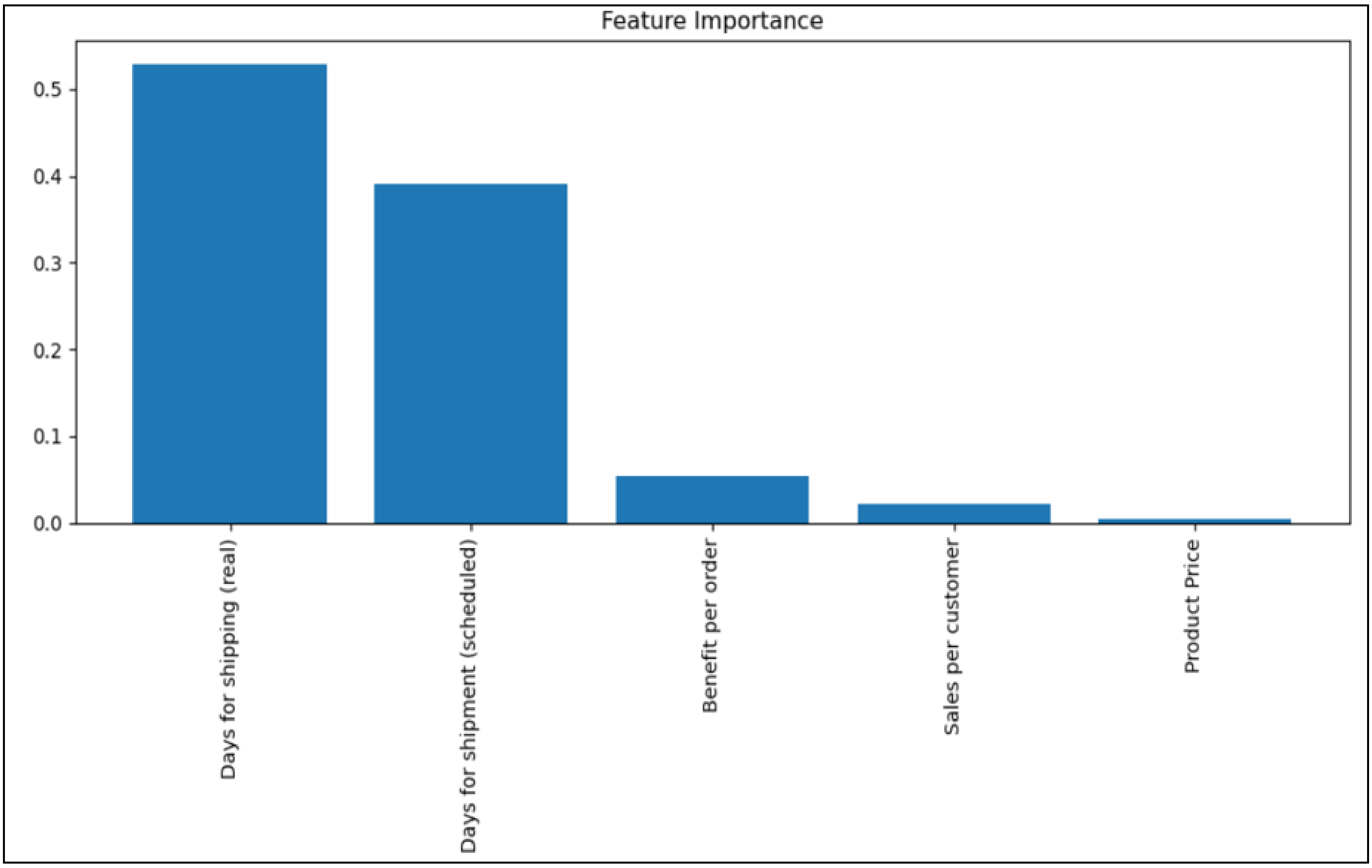

Fig 4 Feature Importance Random Forest Model (Days for Shipping Real: ~0.53; Days for Shipment Scheduled: ~0.39)

➢ *Neural Network Performance*

Neural networks, while doing a good job, required much more computational power and tuning to achieve results comparable to the Random Forest model. In this dataset, the added complexity of neural networks did not result in significantly better performance. The model was implemented as a Sequential model using TensorFlow with a first hidden layer of 64 neurons (ReLU activation), a second hidden layer of 32 neurons (ReLU activation), and an output layer of 1 neuron with sigmoid activation, compiled with the Adam optimizer and binary cross-entropy loss, and trained for 10 epochs Goodfellow et al. (2016) and Geron (2017).

Training accuracy starts off at approximately 97.3% and reaches approximately 97.57% by epoch 10. Testing accuracy stabilizes at approximately 97.4-97.49% from epoch 3 onward. The gap between training and testing losses is relatively small, indicating no significant overfitting. The model converges in a couple of epochs, and after that, performance is not seriously affected. A slight drop in testing accuracy or a slight rise in testing loss during later epochs is a sign that the model could leverage regularization techniques such as a dropout layer or early stopping to prevent overfitting.

➢ *Training of the Neural Network*

The model is trained by minimizing a binary cross-entropy loss function, which measures the difference between predicted probabilities and actual delivery outcomes. Backpropagation with gradient descent updates the network weights over multiple epochs to reduce prediction error.

The top graph shows training and testing accuracy, while the bottom graph presents the corresponding loss over 10 epochs.

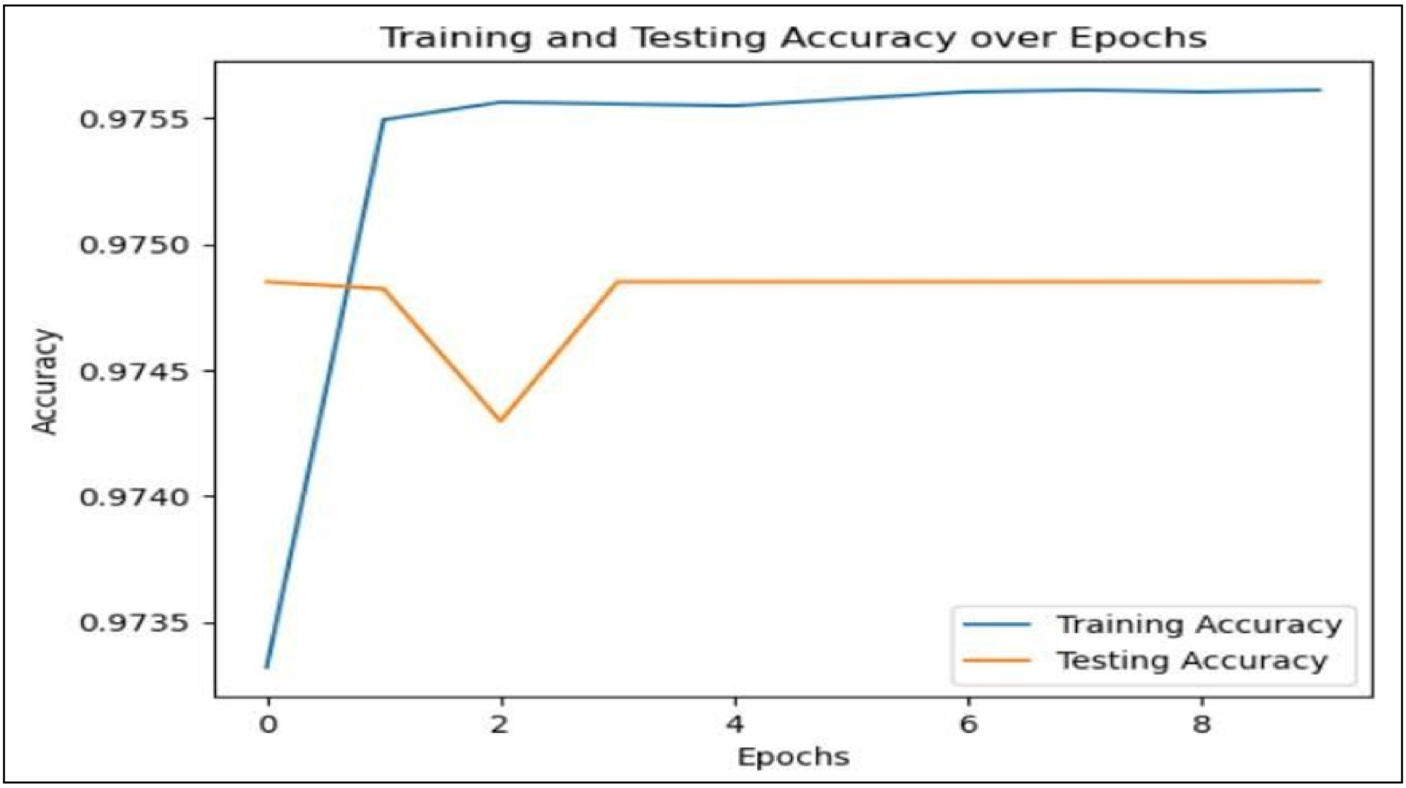

Fig 5 Training and Testing Accuracy

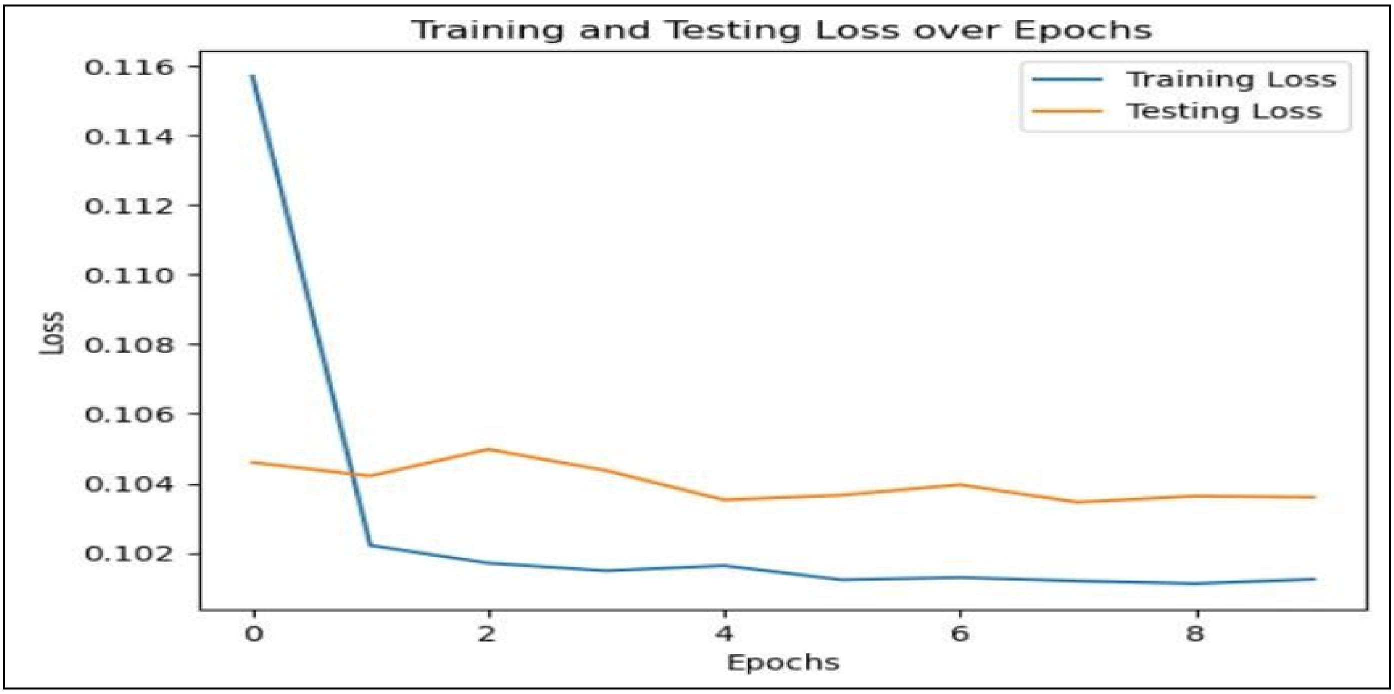

Fig 6 Training and Testing Loss Over Epochs

➢ *Accuracy:*

Training accuracy starts high (≈97.5%) and improves slightly, indicating effective learning from the training data with minimal gains after the first few epochs. Testing accuracy drops marginally after the first epoch suggesting mild overfitting but quickly stabilizes at ≈97.4%, demonstrating good generalization to unseen data.

➢ *Loss:*

Training loss decreases sharply in the first epoch and then plateaus, showing rapid convergence. Testing loss is initially lower than training loss, increases slightly after the first epoch, and then remains stable. The small gap between the two curves indicates no significant overfitting, although the early rise suggests minor memorization of training details.

➢ *Overall Performance:*

The model converges within a few epochs and achieves consistently high accuracy on both datasets. The slight increase in testing loss and small drop in testing accuracy indicate that light regularization techniques (e.g., dropout or early stopping) could further improve generalization.

```
Epoch 1/10
4513/4513 [==============================] - 5s 946us/step - loss: 0.1169 - accuracy: 0.9730 - val_loss: 0.1043 - val_accuracy:
0.9746
Epoch 2/10
4513/4513 [==============================] - 4s 920us/step - loss: 0.1025 - accuracy: 0.9754 - val_loss: 0.1046 - val_accuracy:
0.9746
Epoch 3/10
4513/4513 [==============================] - 4s 922us/step - loss: 0.1019 - accuracy: 0.9755 - val_loss: 0.1044 - val_accuracy:
0.9749
Epoch 4/10
4513/4513 [==============================] - 4s 925us/step - loss: 0.1017 - accuracy: 0.9755 - val_loss: 0.1036 - val_accuracy:
0.9749
Epoch 5/10
4513/4513 [==============================] - 4s 919us/step - loss: 0.1014 - accuracy: 0.9756 - val_loss: 0.1038 - val_accuracy:
0.9749
Epoch 6/10
4513/4513 [==============================] - 4s 914us/step - loss: 0.1013 - accuracy: 0.9756 - val_loss: 0.1038 - val_accuracy:
0.9749
Epoch 7/10
4513/4513 [==============================] - 4s 915us/step - loss: 0.1011 - accuracy: 0.9757 - val_loss: 0.1043 - val_accuracy:
0.9746
Epoch 8/10
4513/4513 [==============================] - 4s 927us/step - loss: 0.1013 - accuracy: 0.9756 - val_loss: 0.1034 - val_accuracy:
0.9749
Epoch 9/10
4513/4513 [==============================] - 4s 925us/step - loss: 0.1014 - accuracy: 0.9756 - val_loss: 0.1038 - val_accuracy:
0.9749
Epoch 10/10
4513/4513 [==============================] - 4s 948us/step - loss: 0.1010 - accuracy: 0.9757 - val_loss: 0.1037 - val_accuracy:
0.9749
```

- *ROC Curve Analysis*

The Receiver Operating Characteristic (ROC) Curve illustrates the performance of the model in terms of distinguishing between classes late delivery risk versus no late delivery risk. The AUC score is 0.97, fairly close to 1.0, indicating that this model is quite good at distinguishing between the positive class (late delivery risk) from the negative (no late delivery risk). Since the ROC curve is close to the upper-left corner, this model is very good at discerning the difference between late and on-time deliveries, with a very high True Positive Rate and a low False Positive Rate. The dotted diagonal line represents a random guess; any model with an AUC falling above this line is better than a random guess, and the farther the distance of the curve from this line, the better the performance.

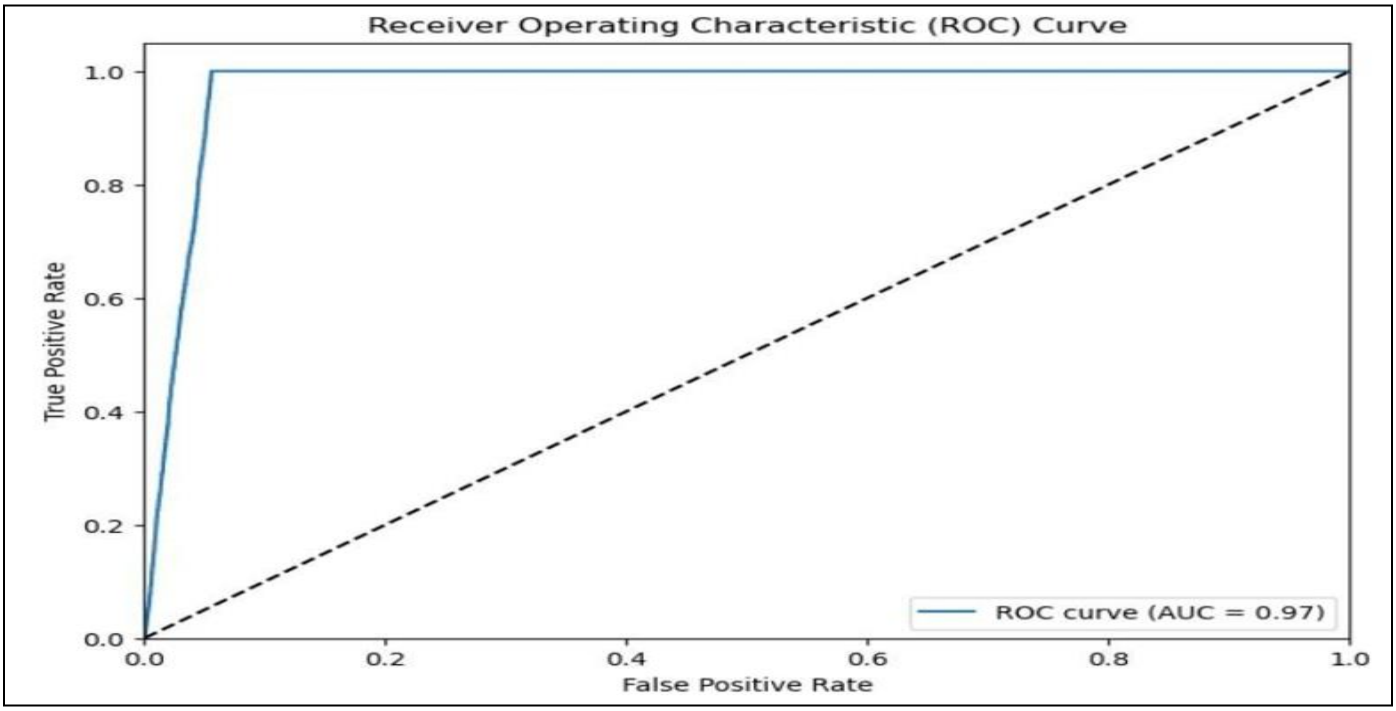

Fig 7 Receiver Operating Characteristic (ROC) Curve AUC = 0.97, Demonstrating Strong Discriminative Ability for Late Delivery Risk Prediction

Table 3 Comparison of Machine Learning Approaches in Supply Chain Risk Management Literature

Study	ML Techniques	Focus Area	Key Metrics Reported	Relevance
Yeboah-Ofori & Boachie (2019)	Decision Tree, SVM, Logistic Regression	Malware/cyber-attack prediction in supply chains	Precision, Recall, F1-score, ROC-AUC	Establishes ML viability for supply chain security
Zheng, Kong & Brintrup (2023)	Federated ML, CNN1D	Privacy-preserving collaborative risk prediction	F-Score, Accuracy, Precision, Recall (local vs. global)	Collective risk prediction without data exposure
Shahzad et al. (2020)	Blockchain + IoT integration	Security and privacy in IoT supply chains	Transaction integrity, data privacy	Validates multi-technology supply chain security
Abbas et al. (2020)	Blockchain + ML hybrid	Drug supply chain management	Efficiency, traceability, recommendation accuracy	Cross-domain ML-blockchain integration
Aljohani (2024)	Predictive analytics, real-time ML	Real-time supply chain risk mitigation and agility	Risk reduction rate, agility metrics	Informs real-time integration framework of this study
Watara et al (2025) Present	Random Forest, Logistic Regression, Neural Networks	Late delivery risk prediction (6-feature dataset)	Accuracy 97.04–97.49%, AUC 0.97, Recall 1.00	Large-scale benchmark with feature importance analysis

Source: Watara (2025).

V. DISCUSSION AND CONCLUSION

➢ *Key Insights and Contributions*

This study has expressed the transformative potential of machine learning in supply chain risk management, especially for late deliveries. It tested a number of machine learning models that had strong accuracy in finding patterns in supply chain data, among which are Logistic Regression and Random Forest. Although both Logistic Regression and Random Forest have high accuracies of over 97%, Logistic Regression has perfect recall for late deliveries and thus is very reliable to flag every single instance of a late delivery. On the other hand, Random Forest minimizes false positives to reduce unnecessary interventions, making it also good at balancing precision and recall. The use of machine learning is very effective in improving risk prediction through processing large amounts of data in real-time and highlighting patterns that can lead to disruptions, allowing organizations to take immediate actions to avoid delays, reducing operational costs and increasing customer satisfaction Aljohani (2024).

The research underlined the importance of integrating real-time data such as IoT sensor data and traffic information for dynamic and action-oriented insights. This guarantees the adaptability of the supply chain and responsiveness to real-time changes, thereby mitigating risks in real-time operations. The study also raised some overfitting concerns, especially where training accuracy kept increasing while test accuracy declined slightly. This can be overcome by incorporating regularization techniques such as L2 regularization, dropout layers, and early stopping to avoid overfitting and allow for better generalization on unseen data.

➢ *Proposed Solutions*

Using L2 regularization with early stopping will prevent overfitting, especially when training for more epochs, enabling the model to generalize equally well on any dataset. Additional features like weather patterns, economic indicators, and the reliability of suppliers contribute to the capturing of nuances in risks within the supply chain by these models Seyedan & Mafakheri (2020). Traffic monitoring and live tracking in real-time will contribute more to the predictive model's immediacy, enabling supply chain managers to act quickly against disruptions. This could be extended by an ensemble model that incorporates both the strengths of logistic regression and a random forest to ensure a robust and reliable system for predicting and mitigating supply chain risks.

➢ *Conclusion*

This study emphasized the enormous value of machine learning in transforming supply chain risk management using improved delivery risk prediction and operational efficiency. Advanced machine learning techniques, such as logistic regression and random forest, were quite effective in facilitating late delivery identification and reduced disrupted operations significantly. By further optimizing real-time integration, feature engineering, and model regularization, supply chains can achieve still higher levels of agility and performance for customer satisfaction. All organizations will need to adopt these technologies quickly in order to survive in the global market, which is changing very dynamically. These models and strategies continuously need refinement so that machine learning can be used to stay ahead of disruptions and provide unparalleled service quality in today's supply chain environment.

REFERENCES

[1]. Abbas, G., et al. (2022). Safety, Security and Privacy in Machine Learning Based Internet of Things. Journal of Sensor and Actuator Networks, 11(3), 38.

[2]. Abbas, K., et al. (2020). A blockchain and machine learning-based drug supply chain management and recommendation system for the smart pharmaceutical industry. Electronics, 9(5), 852.

[3]. Aljohani, A. (2024). Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility. Journal of Supply Chain Management, 34(2), 45-67.

[4]. Constante, F., Silva, F., & Pereira, A. (2019). DataCo Smart Supply Chain for Big Data Analysis. Mendeley Data. London, UK.

[5]. Deb, C., Zhang, F., Yang, J., Lee, S. E., & Shah, K. W. (2017). A review on time series forecasting techniques for building energy consumption. Renewable and Sustainable Energy Reviews, 74, 902-924.

[6]. Geron, A. (2017). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. O'Reilly Media.

[7]. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[8]. Hassija, V., et al. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet of Things Journal, 8(8), 6222-6246.

[9]. Kuster, C., Rezgui, Y., & Mourshed, M. (2017). Electrical load forecasting models: A critical systematic review. Sustainable Cities and Society, 35, 257-270.

[10]. Lippi, M., Bertini, M., & Frasconi, P. (2013). Short-term traffic flow forecasting: An experimental comparison of time-series analysis and supervised learning. IEEE Transactions on Intelligent Transportation Systems, 14, 871-882.

[11]. Naz, F., Kumar, A., Majumdar, A., & Agrawal, R. (2022). Is artificial intelligence an enabler of supply chain resiliency post COVID-19? An exploratory state-of-the-art review for future research. Operations Management Research, 15(1), 378-398.

[12]. Russell, S., & Norvig, P. (2010). Artificial Intelligence: A Modern Approach (3rd ed.). Prentice Hall.

[13]. Sapankevych, N. I., & Sankar, R. (2009). Time series prediction using support vector machines: A survey. IEEE Computational Intelligence Magazine, 4, 24-38.

[14]. Seyedan, M., & Mafakheri, F. (2020). Predictive big data analytics for supply chain demand forecasting: Methods, applications, and research opportunities. Journal of Big Data, 7, 1-22.

[15]. Shahzad, A., Zhang, K., & Gherbi, A. (2020). Intuitive development to examine collaborative IoT supply chain system underlying privacy and security levels and perspective powering through proactive blockchain. Sensors, 20(13), 3760.

[16]. Yeboah-Ofori, A., & Boachie, C. (2019). Malware attack predictive analytics in a cyber supply chain context using machine learning. 2019 International Conference on Cyber Security and Internet of Things (ICSIoT). IEEE.

[17]. Zheng, G., Kong, L., & Brintrup, A. (2023). Federated machine learning for privacy-preserving, collective supply chain risk prediction. International Journal of Production Research, 1-18.