Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1 (2025)

Predicting Supply Chain Fraud with Artificial Intelligence and Machine Learning Models: Enhancing Operational Security and Integrity

[1]**Mohd. Asif Gandhi,**
Associate Professor, Department of Mechanical Engineering,
School of Engineering and Technology,
Anjuman-I-Islam's Kalsekar Technical Campus, Raigad, Panvel.
masifigandhi@gmail.com
[2]**P K Sudhakar,**
Assistant Professor, Department of Mathematics,
Rajalakshmi Institute of Technology, Tamilnadu, India.
sudhakarpk_susila@yahoo.com
[3]**Bommaraju Srinivasa Rao,**
Professor and HOD,
Department of Computer Science and Engineering (Data Science),
Geethanjali College of Engineering and Technology, Hyderabad, Telangana, India.
drbsrinivasarao.cse@gcet.edu.in
[4]**Aditya Bommaraju,**
Sr. Data and Analytics Platform Engineer, BCBSNC, North Carolina.
adityabommaraju97@gmail.com
[5]**.Dr Sandeep Kumar,**
Professor in Management,
Tecnia Institute of Advanced Studies, Affiliated to GGSIP University, Delhi, India.
sandeeprk1969@gmail.com
[6]**Mohamadi Ghousiya Kousar,**
Assistant Professor, Department of CSE,
Vijaya Vittala Institute of Technology, Bengaluru, Karnataka, India.
kousarmvit@gmail.com

ABSTRACT:

Companies are under increasing pressure to discover novel approaches to optimizing efficiency and reducing costs as a result of the growing complexity of supply networks. The use of machine learning (ML) and artificial intelligence (AI) in supply chain management is one area that has witnessed significant growth in recent years. This proposed uses AI and machine learning techniques to foretell instances of supply chain fraud. Actual company transactions provided the supply chain data used in this project. It turns out that AI and ML classifiers were very good at predicting fraud in the supply chain. Specifically, after looking at all performance metrics, the AI model emerged as the top predictor. According to these findings, AI has the potential to be an effective weapon in the fight against supply chain fraud. When it comes to analysing large datasets, ML and AI classifiers can find patterns that humans might miss. This paper's findings can be applied to optimize supply chain management (SCM) and to anticipate fraudulent transactions. Machine learning and artificial intelligence classifiers may change supply chain management for the better, but they are still in their infancy.

Keywords—Supply Chain Fraud Prediction, Principal Component Analysis (PCA), Graphical Convolutional Neural Network (GCNN).

I. INTRODUCTION

There has been a surge in supply chain fraud due to the proliferation of online shopping and other types of digital business. Supply chain fraud comes in many forms, and it always has negative consequences for businesses. In some cases, it could cause the loss of valuable possessions or the theft of confidential information. A number of situations can lead to resource waste and disruptions in supply chains. Because of the worldwide web of middlemen, companies run the danger of supply chain fraud more often in countries with lax or nonexistent regulations[1]. With an increase in cross-border transactions comes a greater risk of criminals using fraudulent invoices or other materials to commit fraud. The supply chain is vulnerable while the company's higher management deals with critical operational issues. The idea of a supply chain extends well beyond the simple conveyance of goods. It includes the flow of money, services, and data. Even when thinking about a single factory on a single site interacting with a limited number of suppliers, the supply chain process is complex and requires excellent communication as well as a supportive company culture. Without it, the consumer-centric modern world we live in today would not exist. The end product of any consumable good is the product of a lengthy series of interconnected processes that involve numerous stakeholders. The supply chain is vital to numerous businesses, including those dealing with pharmaceuticals, agricultural products, gemstones, and electrical appliances. Consequently, a number of security measures must be put in place to keep the supply chain functioning properly. The problem is that the variables in the existing system are growing exponentially, which makes this procedure very challenging. Due to certain inefficiencies in the current supply chain ecosystem, products often suffer substantial quality degradation before they reach customers[2]. Supply chain security flaws have persisted for a long time, adding to the problem of pirated and counterfeit goods. As a result, manufacturers' reputations suffer along with consumers' wallets. It is infamously difficult to trace the beginnings of the supply chain because of its complexity. Some bad actors take advantage of this vulnerability by committing financial crimes like piracy. People who choose to mislead others about food have a long and storied past1, and they can earn a substantial living doing it. Following a series of high-profile food fraud cases, customers, authorities, and the economy are all concerned about the potential consequences of food-related crime on public health, consumer trust, and the economy. A growing body of research, together with domestic regulatory authorities, international and intergovernmental networks and organizations, and other initiatives, is aiming to curb and avoid food fraud[3]. Companies in the food industry must ensure the safety and quality of their products and must not use misleading or false labeling according to legislation. However, they must also have enough measures in place to protect their supply chain. While numerous studies have looked at how globalization affected economies around the world, supply chain management researchers have just recently begun to investigate how globalization lowered supply chain transparency. One source of increased risk for shipments that cannot be tracked is the practice of customs brokerage by freight forwarders. New ideas and technical developments have also led to a precipitous decline in the price of transportation. When it comes to logistics, containerization is revolutionary. Because of the uniform design, shippers may exchange containers at ports quickly and easily without opening them[4]. The improvement in efficiency is outweighed by the unexpected consequence of reducing supply chain visibility due to the invisibility of contents inside specific containers. The freight forwarder is mostly at risk when it comes to customs declarations made to the importing country. A bill of lading is all that is needed to confirm the services of multiple intermediary shippers involved in a single shipment. The problem here is that you can't tell from these documents if the containers actually contain the items listed. Due to the significant operational costs, it would be impracticable and inconvenient to open every container indicated for clearing. Instead, freight forwarders must rely solely on third-party shipping paperwork to report products they have rarely seen in person.

II. LITERATURE SURVEY

One new method for spotting supply chain fraud is machine learning (ML). Supply chain management (SCM) is increasingly relying on artificial intelligence (AI) to identify and prevent fraudulent activities through the use of big data [5]. Significant losses and system-wide effects can result from supply chain disruptions. By analyzing transactional data with machine learning and AI, trends that could indicate fraud could be uncovered. Things could be shifted if, for instance, a supplier has an unexpectedly high amount of orders or if there is a discernible delay in distribution.

If you use ML to monitor your data in real-time, you can detect any unusual activity with your transactions or shipments. The use of ML intelligence in supply chain management is anticipated to grow in the next years [6]. ML intelligence is a powerful tool for detecting fraud warning indicators in general. Analysis of data is a crucial component of supply chain management. Computational intelligence has a notable influence in the prediction of smart supply chain fraud, and ML is applicable to numerous areas of SCM, including transportation, warehousing, procurement, and inventory management. The use of predictive analytics powered by ML to decrease supply chain fraud has recently increased. One potential use of ML for reducing supply chain fraud is its ability to spot anomalies in large data sets, as shown in previous research [7]. Early findings from commercial applications imply that computational technology could be utilized more extensively for managing supply chain fraud, however studies in this area are still in their early stages. Examining and studying the risks is essential for identifying the components of Internet finance that pose a threat. The weighted KNN algorithm is an expert in volatile accuracy, and the coarseness set is a tool for managing financial risk in the digital realm [8]. Data from credit card transactions can be classified as fraudulent or valid using supervised machine learning, and supply chain risks related to credit card fraud can be identified using artificial neural networks (ANN), according to some researchers [9]. A 99.96% accuracy rate is within the realm of possibility for the trained model. Experts in the field recommend using the XG-Boost algorithm for optimizing data imbalance, the diferential evolution method for detecting credit card fraud, and the optimized XG-Boost algorithm for classifying fraudulent transactions. The model is highly accurate, according to the results [10]. Using genetic algorithms, one may refine the super specifications of illicit transactions and compare and contrast the results of studies on credit card fraud with network search algorithms in terms of accuracy. Decision trees (DT), logistic regression (LR), and random forests (RF) aren't even close to genetic algorithms when it comes to overall performance and prediction accuracy, according to results from real-world applications [11]. Using a genetic algorithm, GA-K-means Businesses may swiftly evaluate their exposure to different risks and react appropriately with K-means clustering analysis, which employs objective gamma to segregate the elements with the highest and lowest risk levels, respectively [12]. Bankruptcy, counterfeit, application, and behavioral fraud are the four categories of credit card fraud listed by [13]. Some of the machine learning methods used to identify fraudulent transactions in various nations include LR, Naive Bayes (NB), RF, K Nearest Neighbour, Gradient Boosting, Support Vector Machines, and neural network algorithms. An approach to credit card fraud detection that is based on machine learning was developed by [14] and makes use of hybrid models using Ada Boost and majority voting algorithms. In order to understand what is considered normal and abnormal behavior in terms of transactions, two types of random forests were proposed in [15]. In this study, we examine two random forests' classifier performance to see which one can identify credit card fraud better. Their study looked on practical methods for detecting credit card theft that affects banking institutions[16]. The best algorithm for predicting fraudulent transactions was found by comparing several machine learning techniques. Two types of resampling were used—under sampling and over sampling—during algorithm training. Among the trained algorithms, Decision Tree, Random Forest, and Xgboost were the most accurate models for predicting instances of credit card theft. Every one of them had an area under the curve (AUC) of 1.00%, 0.99%, or 0.99%. Using machine learning techniques to identify and categorize fraudulent transactions can be incredibly helpful. According to [17], supervised ML systems utilize a common set of tools called classifiers, algorithms, and data mining To begin, a large body of research has demonstrated that support vector machines (SVMs) are capable of detecting fraud. Consequently, SVMs are widely used for fraud detection, as stated by [18]. Random forests are used as an additional classifier for fraud detection. The ability and adaptability of random forests, a type of classifier model that can be likened to aggregated decision tree models, make them stand out when faced with complex data [19]. Decision trees are a powerful tool for fraud detection systems because they are both easy to use and able to employ ensembles and nodes to generate prediction outputs (ibid.). Thirdly, three studies have used logistic regression (LR) as a classifier for fraud detection [20]. One mathematical tool for processing ML prediction tasks before knowing the outcome is the LR technique. It provides a percentage of the possibility of having a fraud case, which is valuable for anticipating fraud instances. The predictive powers of this approach are also critical in the battle against fraud, as stated in their study.

III. METHODOLOGY

An unethical supplier could deceive a buyer in a supply chain due to the information asymmetry on product quality. In order to deter and punish quality fraud, buyers frequently undertake shipping quality inspections and establish supply contracts. Buyers, mindful of budgetary constraints, must assess the likelihood of fraud on the part of suppliers and select suitable testing procedures and intervals. It may model suppliers' profit-seeking behaviour appropriately to understand their fraud intentions, since these intentions are based on suppliers' cost-benefit analyses. What impact, if any, fraud intention analysis might have on quality inspections is the focus of this study. It is worth noting that quality inspection can be iterative, with buyers and suppliers engaging in numerous rounds of transactions (including fraudulent ones) and gaining a better understanding of one another in the process.

a. Preprocessing:

After the data has been pre-processed, it can be analysed using machine learning models to get better results. It was aware that data biases could exist, especially if the dataset had an unfairly high number of instances of a specific kind of spare part or provider[21]. As a result, we looked for opportunities for bias in the data. To solve this, we used visualization tools like density plots and histograms to look at the data distribution, studying the patterns and frequencies of data values in each dataset variable and feature.It employed extra data preprocessing techniques to get the data ready for machine learning models after identifying possible biases and picked the right features. Here are some of the techniques:

i. Data Coding:

Information encoding of categorical variables into numeric values for utilization by machine learning algorithms. Some methods used in this process include binary encoding, one-hot encoding, and label encoding, which transform text input into numerical data. End products will be integer variables with 32 or 64 bits of data.

ii. Data Normalization:

Data normalization is the process of bringing all available data to a consistent scale. A method for standardizing data by converting it to a range of 0 to 1 is Min-Max normalization, which is also called feature scaling. The data is averaged by taking the minimum value from each observation and dividing it by the difference between the maximum and minimum values. As a result, the average is obtained. The Min-Max normalization formula (1) is as follows:

$$z_{max} = \frac{z - z_{min}}{z_{max} - z_{min}} \qquad (1)$$

iii. Sampling:

Data sampling has the purpose of dividing the dataset into two subsets: training and testing. A training sample and a test sample are created from the data. To train machine learning models, one uses the training sample, and to test their performance, one uses the test sample. Here, there are 10,230 samples used for testing and 40,860 samples for training.

b. Feature Selection:

PCA has seen extensive use in real-world process control and serves as a foundation for multivariate data analysis. To account for correlation between variables and to project the high-dimensional data into a lower-dimensional space that contains the original data's variance, principal component analysis (PCA) can be used[22]. As a second-order method, PCA can only take into account the mean and variance of the input data; as a result, it cannot provide high-order representations for data that is not normally distributed according to the normal distribution, which is generally the situation in industrial settings in the real world. The PCA breaks down the data matrix $z \in \mathbb{R}^{m \times f}$(where m is the sample size and f is the number of variables) into its component scores and loadings by employing either the singular values decomposition technique or the nonlinear iterative partial least squares; the process is described below:

$$Z = VQ^{T} + H \tag{2}$$

The score matrix, denoted as $V \in \mathbb{R}^{m \times c}$, and the loading matrix, denoted as $Q \in \mathbb{R}^{m \times f}$ are respectively equal to the residual matrix, H. By projecting onto PC space, the original collection of variables is reduced to a set of latent variables. The variables linked to the variables with the highest eigenvalues are contained in the covariance or correlation matrix, and the columns of Q represent these eigenvectors. The PCA score, prediction, and residual vectors are provided for a new sample vector z in the following way:

$$score: v = Q^{T}z \tag{3}$$

$$prediction: z' = QQ^{T}z \tag{4}$$

$$Residual: h = (B - QQ^{T})z \tag{5}$$

A news sample vector$z$ is frequently analyzed using V^{2} and SPE for aberrant detection. It is defined as V^{2}, which is a measure of the variation in PC space and the sum of the normalized squared scores.

$$V^{2} = v^{T}F^{-1}v = z^{T}QF^{-1}Q^{T}z \tag{6}$$

The SPE, on the other hand, can be used to track a measure of variation that the PCA model misses. By projecting the sample vector onto the residual space, the SPE statistics show how well each sample fits the model.

$$SPE = h^{T}h = z^{T}(B - QQ^{T})z \tag{7}$$

The sum of squares of the residuals, denoted as$h$, is the SPE.

c. Model Training

i. **GNN*:***

Introduced initially, graph neural networks (GNNs) allow deep neural networks, particularly convolutional networks, to handle graph-structured data, which is geographically distributed around the world and not limited to Europe[23]. Most graph convolutional neural networks fall into one of two broad types: spectral domain or spatial domain. For graph convolution operations, the former turns to Spectral Graph Theory. Convolution on generic graphs was defined using the matching Fourier basis. We used K-order Chebyshev polynomials to approximatively estimate the convolution operator in order to circumvent processing costs. In the end, they created a GCN using a first-order approximation of spectral graph convolutions, which sparked scientists' enthusiasm for

GNN. As it pertains to geographical methods, convolutions are defined by the adjacency on the graph itself. They used GraphSAGE, an aggregator based on neural networks, to process data from neighbours with a fixed number of nodes. GraphSAGE learns a function to create embeddings by combining neighbours' attributes. Then, GNN like Graph Attention Network (HAN) are trained to automatically learn the relevance of various neighbours. GNNs have found usefulness in many different fields, including text classification, computer vision, and social networks.To set ourselves apart from the aforementioned research, itpresents a new model for heterogeneous graph attention networks that takes into account the diversity and significance of individual nodes within the network to classify semi-supervised short texts, and it suggest building an HIN for such texts that can adaptably incorporate any extra information.

ii. CNN:

One deep-learning system that has broken new ground in picture classification is convolutional neural networks (CNNs). In order for CNN to extract features from images, the convolutional layer performs convolution operations[24]. Convolution creates feature maps by multiplying and adding matrices that have been dragged across the input image in a filtering operation. This convolution layer is usually iterated many times. The fully-connected layer takes a vector input from the feature map that was derived from the last convolutional layer and uses it for classification. High translation invariance, or the capacity to recognize individual objects in a picture regardless of changes to their locations, is one of CNN's strongest suits.Experts in fields focused on images, such as time-series transactions' cadence, find a home in the embrace of sequential data. Using transactional data as a stage, CNNs perform a spatial and temporal symphony in the big theatre of fraud detection. CNNs demonstrate their expertise in learning hierarchical representations in the context of order and relationships. Their intricate choreography of preprocessing and data shaping is required to navigate spatial dependencies. An enormous stage is necessary for this performance since massive datasets are necessary for maximal brilliance.

iii. GCNN:

It is presumed that CNN receives data in a grid format, like images, with a meaningful layout and order of pixels. The reason behind this is that when convolutional operations are performed among nearby pixels in the convolutional layer, a square filter matrix is usually utilized. On the other hand, GCNN makes it possible to use similarity relationships to perform convolution operations on items that aren't nearby. GCNN use similarity relationships to convert convolved items into data that is graph-structured. Nodes in this study stood in for elements, or audio features, and edges for similarity relationships between nodes. A number of GCNNs have been suggested, each using a unique approach to calculating feature similarity. This research made use of the GCNN method, which calculates feature-to-feature correlations by averaging their absolute values.

iv. RNN-LSTM:

For time-series or sequential transactions, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) Networks are great choices because of their ability to manage sequential dependencies. When it comes to detecting fraud, RNNs and LSTMs dance through the complexities of time, revealing patterns that develop over several transaction sequences. They are experts at detecting complex webs of interdependencies and flourish in fast-paced fraud situations. But being stable requires a journey through computational domains, where tackling the disappearing and growing gradient problems becomes paramount.

IV. Results and Discussion

Supply chain risk management is an emerging discipline that aims to safeguard supply chains from disruptions by identifying, assessing, and reducing possible risks. The current spike in interest in AI has also spurred study into machine learning approaches and how they could be used to supply chain risk management. The importance of interpretability has been under-researched compared to prediction performance, despite the fact that it is critical for supply chain practitioners to comprehend the findings and take actions to mitigate or eliminate risks. The proposed methodology for predicting risks in the supply chain is the principal new contribution of this research. Implemented using AI and supply chain experts' complimentary abilities, it is based on data-driven methods. Then, we probe the compromise between prediction accuracy and interpretability by applying the framework to the actual issue of forecasting delivery delays in a multi-tiered industrial supply chain.

TABLE I. PERFORMANCE PREDICTION(%)

Model	GNN	CNN	GCNN	RNN-LSTM
Accuracy	89.76	90.36	92.29	91.64
Precision	87.54	88.12	90.42	89.06
Sensitivity	95.48	93.54	96.90	94.80
Specificity	89.21	87.60	88.43	88.43
F1-Score	88.20	89.68	91.12	90.49
AUC	96.54	96.49	97.35	97.12
Recall	86.28	87.04	89.56	88.25

Table 1 shows the results of comparing four models' performance on different measures. These models are GNN, CNN, GCNN, and RNN-LSTM. In terms of overall effectiveness, GCNN outperforms all other methods with the best accuracy (92.29%), precision (90.42%), sensitivity (96.90%), and area under the curve (97.35%). Although both RNN-LSTM and CNN perform similarly, RNN-LSTM achieves better recall (88.25%). With the exception of sensitivity (95.48%), GNN has the worst results across the board. Based on these results, it's clear that GCNN performed better than the other options.

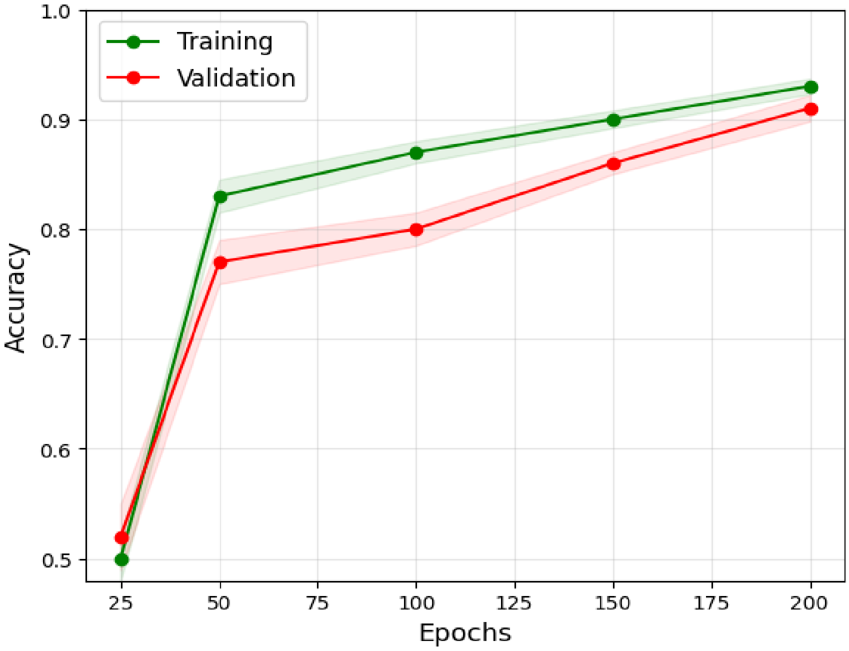

Fig. 1. Training and Validation Accuracy for Predicting Supply Chain Fraud

Figure 1 shows the number of training and validation epochs needed to determine the accuracy of a model in identifying supply chain fraud. The accuracy of both training and validation increases over time, with validation accuracy closely tracking training accuracy, suggesting that there is little overfitting. That the model is learning and able to generalize to new data is supported by this. With these results, the model has proven it can accurately detect fraud in supply chain.

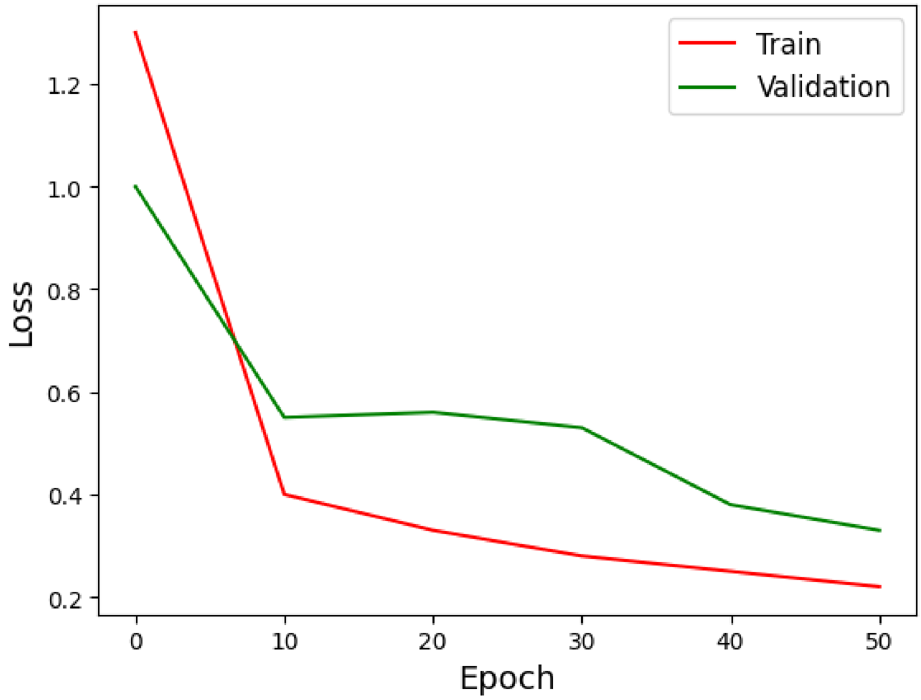

Fig. 2. Training and Validation Accuracy for Predicting Supply Chain Fraud

Figure 2 shows the training and validation loss of a model that can detect supply chain fraud over the course of 50 epochs. Both losses come down considerably, but the training loss comes down more quickly than the validation loss, which means that the model is being optimized well.

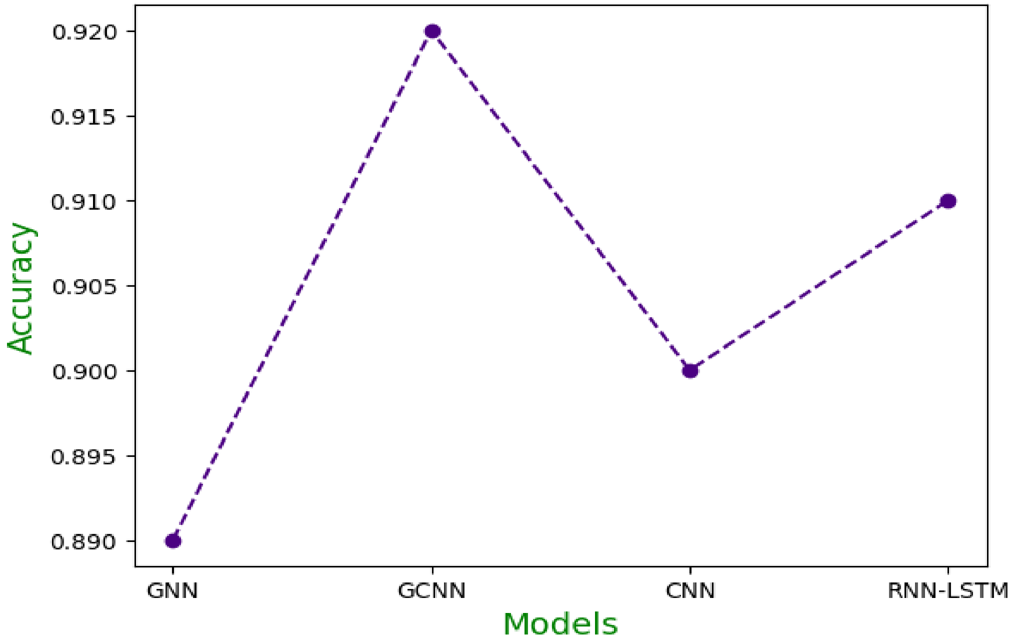

Fig. 3. Accuracy Comparison of Various Models

Machine learning models' ability to identify supply chain fraud is compared in Figure 3. When compared to the other models, GCNN's superior accuracy suggests it can detect intricate patterns of fraud. CNN lagged behind, although GNN and RNN-LSTM both did well.

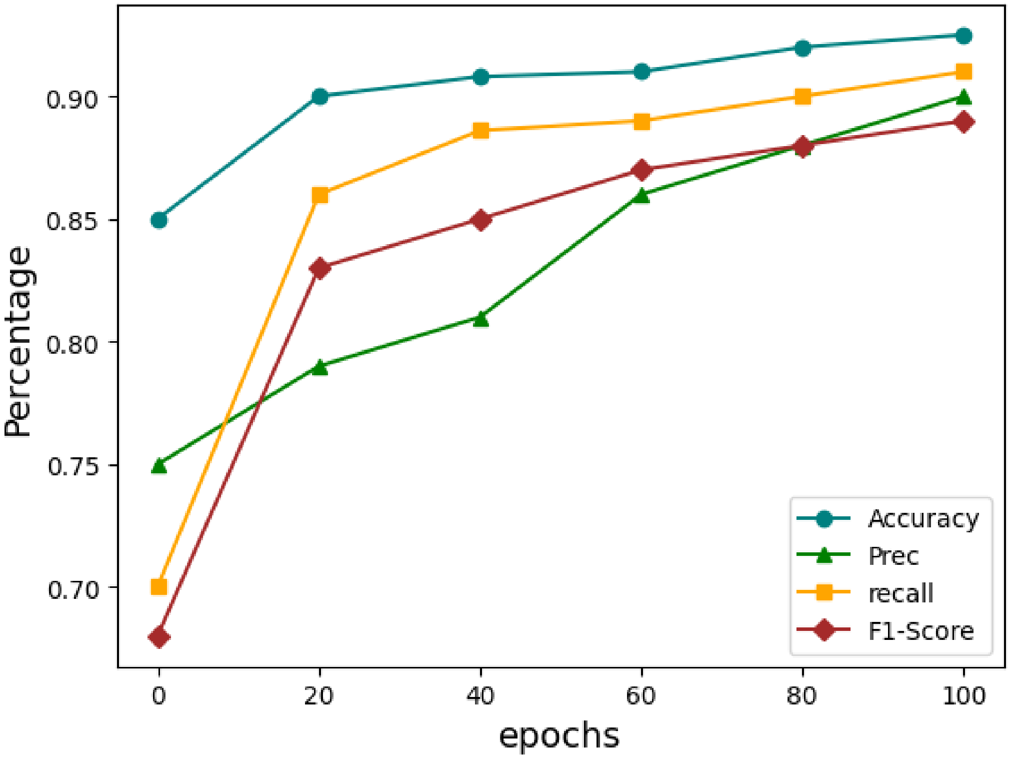

Fig. 4. Performance Evaluation for Proposed Model to Predicting Supply Chain Fraud

Figure 4 shows the evolution of an recall, F1-score, accuracy, and precision as well as a supply chain fraud detection model's performance metrics during the course of its training epochs. Every statistic shows steady improvement as the epoch count rises, reaching a plateau after 60 epochs.

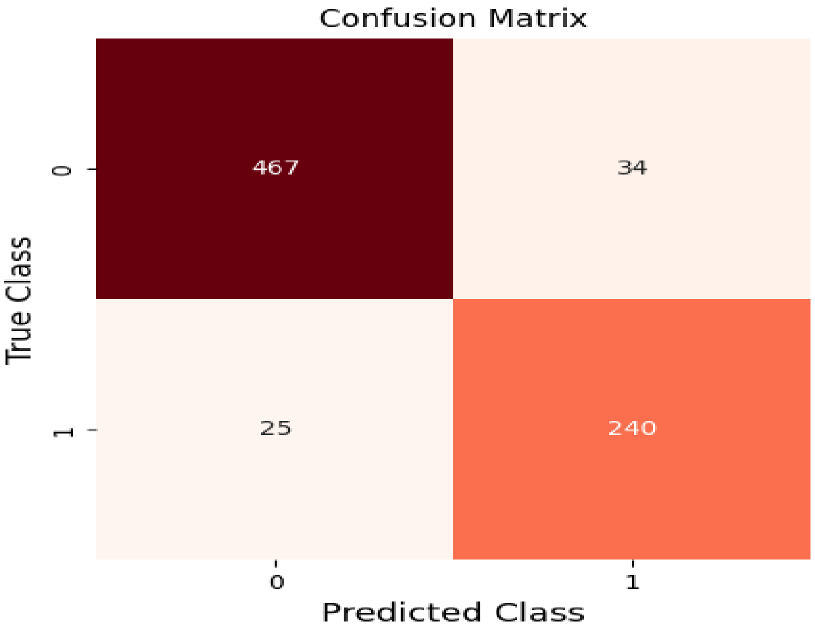

Fig. 5. Confusion Matrix for GCNN Model for Predicting Supply Chain Fraud

Figure 5 shows a confusion matrix that assesses a classification model for detecting fraud in the supply chain. There were 467 cases of successful non-fraud detection and 240 cases of successful fraud detection. There have been 25 missed fraud instances and 34 non-fraud cases that were mistakenly marked as fraud. The majority of the model's predictions match up with the actual class labels, indicating strong performance.

V. CONCLUSION AND FUTURE DIRECTIONS

AI is driving innovation in financial technology and is proving critical in today's fast-paced world. Everything from day-to-day operations to future developments in the supply chain relies heavily on ML algorithms, a subfield of artificial intelligence research. Organizational decision-makers can benefit greatly from the scientific and logical decision-making capabilities offered by machine learning algorithms, such as data mining and deductive reasoning, when applied to the current financial index data. Companies in the supply chain are now at increased danger of bankruptcy as globalization uncertainties grow. There must be practical tools in the operation process to detect and react to supply chain operation threats in a timely manner, to forecast the likelihood of company failure, and to take scientific and realistic steps to avoid a financial crisis during good season.Using GCNN for training, the model achieved an accuracy of 92.29%.

REFERENCES

[1] V. Hassija, V. Chamola, S. Member, V. Gupta, S. Jain, and N. Guizani, “A Survey on Supply Chain Security : Application Areas , Security Threats , and Solution Architectures,” vol. 333031, no. c, pp. 1–25, 2020, doi: 10.1109/JIOT.2020.3025775.

[2] R. Triepels and H. Daniels, “Detecting shipping fraud in global supply chains using probabilistic trajectory classification,” *Dr. Consort. Enterp. Inf. Syst.*, pp. 12–19, 2015.

[3] Y. Bouzembrak and H. J. P. Marvin, “Prediction of food fraud type using data from Rapid Alert System for Food and Feed (RASFF) and Bayesian network modelling,” *Food Control*, vol. 61, pp. 180–187, 2016, doi: 10.1016/j.foodcont.2015.09.026.

[4] Y. Dong, K. Xie, Z. Bohan, and L. Lin, “A Machine Learning Model for Product Fraud Detection Based on SVM,” *Proc. - 2021 2nd Int. Conf. Educ. Knowl. Inf. Manag. ICEKIM 2021*, pp. 385–388, 2021, doi: 10.1109/ICEKIM52309.2021.00091.

[5] K. Yamini, V. Anitha, S. Polepaka, R. Chauhan, Y. Varshney, and M. Singh, “An Intelligent Method for Credit Card Fraud Detection using Improved CNN and Extreme Learning Machine,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Jun. 2023, pp. 810–815. doi: 10.1109/ICCES57224.2023.10192774.

[6] N. M. Reddy, K. A. Sharada, D. Pilli, R. N. Paranthaman, K. S. Reddy, and A. Chauhan, “CNN-Bidirectional LSTM based Approach for Financial Fraud Detection and Prevention System,” in *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, IEEE, Jun. 2023, pp. 541–546. doi: 10.1109/ICSCSS57650.2023.10169800.

[7] R. Rajkumar, N. Kogila, S. Rajesh, and A. R. Begum, “Intelligent System for Fraud Detection in Online Banking using Improved Particle Swarm Optimization and Support Vector Machine,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Jun. 2023, pp. 644–649. doi: 10.1109/ICCES57224.2023.10192690.

[8] K. Rathor, S. Vidya, M. Jeeva, M. Karthivel, S. N. Ghate, and V. Malathy, “Intelligent System for ATM Fraud Detection System using C-LSTM Approach,” in *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, IEEE, Jul. 2023, pp. 1439–1444. doi: 10.1109/ICESC57686.2023.10193398.

[9] S. Kakkar, “Analysis of Discovering Fraud in Master Card based on Bidirectional GRU and CNN based Model,” *2023 Int. Conf. Self Sustain. Artif. Intell. Syst.*, no. Icssas, pp. 50–55, 2023, doi: 10.1109/ICSSAS57918.2023.10331770.

[10] S. Yadav, D. Pilli, M. K. Senthil Kumar, D. Kaushal, S. Kaliappan, and R. Maranan, “Managing and Assessing the Risk Management of Supply Chain Using the A-BiGRU-CNN Approach,” *7th Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2023 - Proc.*, no. Iceca, pp. 553–558, 2023, doi: 10.1109/ICECA58529.2023.10395063.

[11] K. Prabhakar, M. S. Giridhar, A. Tatia, T. M. Joshi, S. Pal, and U. S. Aswal, “Comparative Evaluation of Fraud Detection in Online Payments Using CNN-BiGRU-A Approach,” *Int. Conf. Self Sustain. Artif. Intell. Syst. ICSSAS 2023 - Proc.*, no. Icssas, pp. 105–110, 2023, doi: 10.1109/ICSSAS57918.2023.10331745.

[12] T. Porkodi, “An Automatic ATM Card Fraud Detection Using Advanced Security Model Based on AOA-CNN- XGBoost Approach,” *2024 Int. Conf. Electron. Comput. Commun. Control Technol.*, pp. 1–7, 2024, doi: 10.1109/ICECCC61767.2024.10593851.

[13] B. A. Reddy, G. V. Kumar, M. D. Kumar, S. Veena, A. Chauhan, and H. A. Basha, “Towards a Framework for Supply Chain Financing for Order-Level Risk Prediction : An Innovative Stacked A-GRU Based Technique,” *2024 Int. Conf. Electron. Comput. Commun. Control Technol.*, pp. 1–6, 2024, doi: 10.1109/ICECCC61767.2024.10593920.

[14] K. Rathor, B. V. Dhananjayamurthy, D. Abdul Jaleel, S. Pal, P. Bhavani, and N. Nishant, “Temporal Threat Recognition in Supply Chains: Integrating Hidden Markov Models for Proactive Security with AI-Driven Automated Threat Hunting,” *2024 Int. Conf. Adv. Mod. Age Technol. Heal. Eng. Sci. AMATHE 2024*, pp. 1–6, 2024, doi: 10.1109/AMATHE61652.2024.10582202.

[15] N. Pol and S. Agarwal, “Online Transaction Fraud Detection : Exploring the Hybrid SSA-TCN-BiGRU Approach,” *2024 2nd World Conf. Commun. &amp; Comput.*, pp. 1–6, 2024, doi: 10.1109/WCONF61366.2024.10692254.

[16] L. Saha, S. Birajdar, D. Uike, M. D. Kumar, G. Sivakumar, and U. A. Nayak, “LSSVM Analysis of Competency Effects on Supply Chain Management from Individual and Collaborative Perspectives,” *2024 Int. Conf. Data Sci. Netw. Secur.*, pp. 1–6, 2024, doi: 10.1109/ICDSNS62112.2024.10691117.

[17] S. Vii, G. D. Rede, P. Ramesh, R. Kumar A, A. Bharathi, and M. C. J. Anand, “Optimizing E-Commerce Fraud Detection with BiGRU and Capsule Network Architectures,” in *2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024*, 2024, pp. 1–6. doi: 10.1109/ICDSNS62112.2024.10691229.

[18] Y. Zhou, X. Song, and M. Zhou, “Supply Chain Fraud Prediction Based on XGBoost Method,” *2021 IEEE 2nd Int. Conf. Big Data, Artif. Intell. Internet Things Eng. ICBAIE 2021*, no. Icbaie, pp. 539–542, 2021, doi: 10.1109/ICBAIE52039.2021.9389949.

[19] H. Wang, F. Yang, and S. Shen, “Supply Fraud Forecasting using Decision Tree Algorithm,” *2021 IEEE Int. Conf. Consum. Electron. Comput. Eng. ICCECE 2021*, no. Iccece, pp. 344–347, 2021, doi: 10.1109/ICCECE51280.2021.9342556.

[20] Y. Zhang, J. Tong, Z. Wang, and F. Gao, “Customer Transaction Fraud Detection Using Xgboost Model,” *Proc. - 2020 Int. Conf. Comput. Eng. Appl. ICCEA 2020*, pp. 554–558, 2020, doi: 10.1109/ICCEA50009.2020.00122.

[21] A. Amellal, I. Amellal, H. Seghiouer, and M. R. Ech-Charrat, “Improving Lead Time Forecasting and Anomaly Detection for Automotive Spare Parts with A Combined CNN-LSTM Approach,” *Oper. Supply Chain Manag.*, vol. 16, no. 2, pp. 265–278, 2023, doi: 10.31387/oscm0530388.

[22] J. Yu, “Fault detection using principal components-based gaussian mixture model for semiconductor manufacturing processes,” *IEEE Trans. Semicond. Manuf.*, vol. 24, no. 3, pp. 432–444, 2011, doi: 10.1109/TSM.2011.2154850.

[23] M. Ishimaru, Y. Okada, R. Uchiyama, R. Horiguchi, and I. Toyoshima, “Classification of Depression and Its Severity Based on Multiple Audio Features Using a Graphical Convolutional Neural Network,” *Int. J. Environ. Res. Public Health*, vol. 20, no. 2, 2023, doi: 10.3390/ijerph20021588.

[24] P. Kamuangu, “A Review on Financial Fraud Detection using AI and Machine Learning,” *J. Econ. Financ. Account. Stud.*, vol. 6, no. 1, pp. 67–77, Feb. 2024, doi: 10.32996/jefas.2024.6.1.7.