Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 6s (2025)

An Integrated Approach to Optimize Risk in SCM using Blockchain and Machine Learning Techniques

Ritesh Kumar Singh[1], Udai Shanker[2]

[1]Research Scholar, [2]Professor, Department of CSE, M. M. M. University of Technology, Gorakhpur, UP, India

E-mail: [1]riteshvns53@gmail.com, [2]udaigkp@gmail.com

Article History:

Received: *23-10-2024*

Revised: *07-12-2024*

Accepted: *15-12-2024*

Abstract:

In the dynamic field of supply chain management (SCM), identifying and mitigating risks is crucial for sustaining resilience and efficiency. Conventional risk management strategies frequently inadequately handle the complexities and uncertainties intrinsic to contemporary supply networks. This study investigates a hybrid approach that combines blockchain technology with machine learning to improve risk detection and management in supply chain management. Blockchain provides a decentralised and transparent system for monitoring supply chain operations, guaranteeing data integrity and transparency. Machine learning enhances this process by examining extensive amounts of past and present information to discern trends, forecast future dangers, and propose mitigation solutions. The suggested system utilises blockchain's inviolability and machine learning's predictive powers to tackle significant difficulties including identifying fraud, demand forecasting, supplier assessment, and disruption prediction. Case studies and quantitative assessments illustrate the efficacy of the hybrid method in mitigating vulnerabilities and enhancing decision-making. This research enhances current understanding in digital supply chain management and offers practical insights for practitioners aiming to implement novel technology to alleviate supply chain hazards. This hybrid system utilises the immutable characteristics of blockchain to provide safe and open data storage, while machine learning models derive actionable insights, hence improving productivity and making decisions. The experiment demonstrates four machine learning models and we achieved 97% accuracy for two model for Random Forest and Support Vector Machine that outperform from other models.

Keywords: Supply Chain Management, Blockchain, Machine Learning, Risk Management, Privacy Preserving

1. Introduction

In the contemporary era of globalisation, several organisations are establishing dependable supply chains to secure a competitive edge by providing the greatest value to their clients. Supply Chain Management (SCM) has grown essential for managing risk, dynamism, and the intricacies of global sourcing [1]. Consequently, the organisation must have a fully interconnected supply chain for maximum benefits.

Supply Chain Management (SCM) has become a primary priority for top firms seeking to enhance market share, profitability, competitive advantage, and shareholder value. Indeed, during the last few decades, the word SCM has transitioned from "Distribution" to "Logistics" and ultimately to "Supply Chain Management" [2]. Contemporary industrial civilisation relies on globalisation, specialisation, and mass production. Virtually no firm or industrial unit manufactures the entire product anymore. A supply chain is an association of distinct companies that cooperate to produce a product that satisfies customer requirements. SCM encompasses the strategic planning and management of commodities movement to accelerate time to market, minimise inventory levels, reduce overall costs, and enhance client service and experience.

1.1 Risk Management in SCM

Risk refers to the possibility of encountering harm or loss. Exposure to the risk of damage or loss, a hazard or peril, likelihood of loss, and the degree of probability associated with such loss. Risks arise from ambiguity regarding the future, and since precise outcomes are unattainable, risk is perpetually present. The phrases 'risk' and 'uncertainty' are sometimes used interchangeably; however, there exists a fundamental distinction between both. Uncertainty denotes the ability to enumerate potential future occurrences but lacking knowledge on which it will transpire or their respective probabilities. Risk refers to the capacity to enumerate potential future occurrences and assigns a probability to occurrence [3]. When managers engage with uncertainty, risk, certainty, and ignorance, the discourse typically revolves on risk management. Risk management is a systematic technique of detecting, reducing, and evaluating risks to minimize losses resulting from inadequate risk management [4][5]. The risk management process encompasses the subsequent phases that can be seen in figure 1-

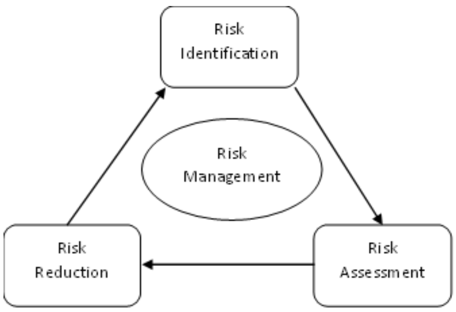

Figure 1: Risk Management Process cycle in Supply Chain

- **Recognition of Risks** – It assists in recognizing potential hazards to the system.
- **Risk Analysis and Evaluation -** It facilitates the prioritization, evaluation, and implementation of the recommended control measures inside the system.
- **Risk reduction -** It assesses and determines the applicability of the existing control procedure to the system.

Supply chain risk manifests as any occurrence that might impact transportation and interrupt the intended flow of materials. The assumption is that the anticipated, standard supply chain flow yields a conventional outcome, and that any disturbance in this flow may diminish the result.

1.2 Use of Blockchain and Machine Learning Techniques

Machine learning algorithms provide exceptional learning capabilities. They possess several elements that enhance the blockchain's functionality compared to its prior state. Several of these enhance the security of the apps. Machine learning diminishes the computing time required to answer the challenge and enhances data sharing methodologies. Machine learning algorithms can utilize data stored on the blockchain for predictive analytics or data analysis. Intelligent blockchain-based apps aggregate data from many sources including smart devices, sensors, and more apparatus. The blockchain is an integral component of the application where a machine learning model is utilized for data analysis or predictions [6]. Errors in machine learning models may be mitigated by utilizing blockchain for data storage. It is devoid of missing data, duplication, and noise, all of which are essential for a machine learning model to achieve enhanced accuracy. Potential applications of machine learning in conjunction with blockchain include improved customer service, data trade, product production etc.

1.3 Need for Blockchain Technology in SCM

The applications of blockchain are numerous. In addition to its application in industrial industries, the healthcare industry has effectively utilized blockchain for communication and other critical functions. Various sectors have heightened their awareness of the myriad cyber hazards that products encounter throughout the SCM process [7].

Ensuring the integrity and traceability of products and processes within a multi-stakeholder supply chain system is a significant challenge. Product safety and protection is a burgeoning domain within supply chain management that has garnered significant research interest in the past year. In figure 2, we focused that product safety refers to the reduction of the probability that a product may induce disease, injury, or other detrimental effects to individuals. Blockchain is a superior solution for addressing supply chain management concerns. Current blockchain-based systems encounter several security issues, such as scalability, confidentiality, anonymity, and privacy. Supply chains utilizing blockchain are always susceptible to many forms of attacks including tag cloning, key leakage, eavesdropping, and block withholding attacks [8][9]. Despite the availability of many countermeasures, assaults and attackers remain active in disrupting the blockchain process for their personal profit. These conditions delineate a gap that necessitates a framework to address all forms of current and future threats.

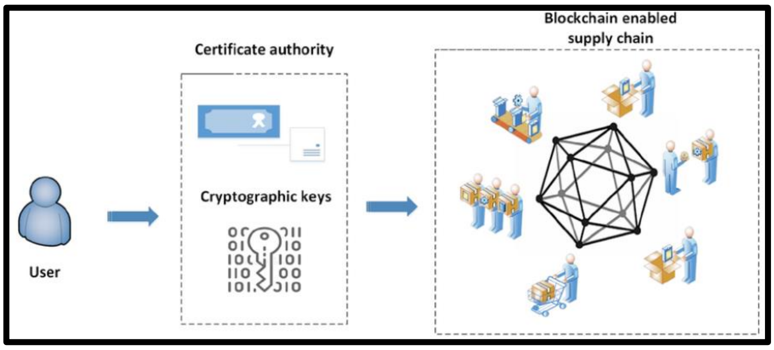

Figure 2: Blockchain Based SCM Architecture [10]

It is crucial to priorities strategies for effectively responding to attacks and confronting assailants. In accordance with the aforementioned, it became essential to create appropriate modules to maintain blockchain as a safe technology, impervious to manipulation or disruption of the actual process flow [11]. Due to the rise of unethical practices in the supply chain, such as counterfeit goods, misleading product labelling, inappropriate components and materials, and trademark infringement, the origin of these issues remains undetectable with current centralized anti-counterfeit solutions. Moreover, the proposed modules may instill genuine confidence in the blockchain process among participants and further entice new individuals to join by mitigating concerns over potential assaults. The advantages derived from a secure blockchain entice additional parties and may facilitate its advancement and broader use.

1.4 Machine Learning Techniques

Organizations possess substantial amounts of organized and unstructured data; yet improper management may diminish the advantages. Data mining facilitates the identification of patterns and trends that might benefit the organization [12]. A variety of strategies can be employed to transform raw data into valuable information. This encompasses both sophisticated artificial intelligence [13] and essential data strategy, which are vital for maximizing the value of data investments.

The use of machine learning is a fundamental component in the constantly changing discipline of data science. In data extraction endeavors, algorithms are instructed using statistical methodologies to provide predictions or categories and to reveal valuable insights. These insights subsequently impact the decision-making of apps and companies., ideally impacting essential growth KPIs. With the proliferation of big data, the need for data scientists will increase. They will be tasked with assisting in the selection of the most relevant business queries and the corresponding data [14].

Data serves as the catalyst that drives an organisation. Through data-driven analytics, a corporation may ascertain if it is maintaining competitiveness or lagging. Machine learning is essential for realising the true value of corporate and consumer data and facilitating optimal decision-making.

Machine learning encompasses several sorts of models that utilise distinct algorithmic techniques. One of the following four learning models may be utilised: supervised, unsupervised, semi-supervised, or reinforced [15]. Each model may incorporate one or more algorithmic procedures, contingent upon the used data sets and the intended results. The primary objective of machine learning algorithms is to categorise things, discern patterns, predict outcomes, and provide educated decisions. In the context of complex and unforeseen data, algorithms may be employed individually or collectively to achieve optimal accuracy.

1.5 Challenges of Machine Learning

The subsequent are notable issues associated with machine learning [16][25][26]:

- **Substandard Data Quality:** Developers have difficulties in obtaining quality data while always striving to enhance machine learning algorithms. The difficulty of data quality is complex due to its diversity, speed, and magnitude. Diverse sources and categories of data require distinct methodologies. Machine learning may assist with particular aspects of data quality like addressing data gaps, detecting abnormalities, finding and eliminating duplicates, and verifying data.
- **Insufficient Skilled Personnel:** Oversight of the machine learning process, encompassing coding and maintenance, is conducted by machine learning specialists. The sector is nascent, making it challenging to find experienced personnel. Consequently, there is a deficiency of proficient representatives to formulate and oversee scientific components for machine learning (Moraffah R et al., 2020; Tran S. et al., 2021).
- **Inadequate Comprehension of the Issue:** In the contemporary landscape of machine learning, distinguishing reality from fiction is getting ever more difficult. Daily manual procedures with consistent output are the simplest to automate. Prior to automating complex operations, they must

undergo meticulous examination. It is essential to identify the platforms to be utilized and the problems associated with them prior to addressing the problem. Although machine learning can facilitate the automation of certain processes, it is not essential for all automation challenges.

- **Implementation Challenges:** By the time, organizations opt to transition to machine learning, the majority already own established analytical engines. Integrating contemporary machine learning methodologies into existing processes is a challenging endeavor. Accurate interpretation and recording of primary training can facilitate implementation significantly. Engaging an implementation partner may significantly simplify the development of services such as anomaly detection, forecasting, and ensemble simulation.

1.6 Motivation

Today supply chains are growing progressively intricate regarding the individuals involved, resources utilized, and overall complexity. Due to the extensive nature of these supply chains involving several enterprises, the exchange of products, personnel, and information among critical stakeholders is imperative. This presents many supply chain security issues. Security risks must be promptly handled, since a system breach might lead to the loss of trade secrets, revenue, and wasteful shipping. Providing unauthorized or altered merchandise may jeopardize consumer safety and lead to undesirable arguments. Inspired by these findings, this paper presents a secure blockchain-based system for SCM.

Additionally, forecast risks in SCM via a predictive model is designed to function as a risk management tool. Anticipating future risks allows the firm to implement measures to mitigate them. This study aims to assess the causal impact on risk, so offering the organization further insight into mitigating its effects.

1.7 Objective of Research

This would be helpful to the industry professionals in making a secure framework and classifying the risk. The primary purpose of this study is given below.

- Determine principal risks and inadequacies in supply chain through gathering of dataset.
- Investigate ways in which blockchain improves confidence, and data security inside supply chains.
- Examine machine learning methodologies to forecast risks and enhance supply chain efficiency.

This section provides a comprehensive introduction to risk management in SCM, the need of blockchain, uses of machine learning techniques, and research objectives. The next part will examine the previous researchers' efforts to identify risk management in SCM.

2. Literature Survey

The supply chain, comprising of multiple participants such as manufacturers, stockiest, distributors, physical sellers, and buyers, is quite intricate. When a disruption occurs in a supply chain, it necessitates extra time and effort to ascertain the location and nature of the delivery failure. The discourse has been organized into many headings and subheadings. This research study emphasizes the security of blockchain technology and associated topics such as authentication; subsequently, examines the applications of machine learning improvements for mitigating risk in supply chain management. Here, we have discussed some technical papers to reduce the risk using blockchain and machine learning techniques under the head supply chain, Blockchain in supply chain and machine learning technique for supply chain.

SCM emphasises the coordination and optimisation of operations to guarantee the effective movement of products, services, and information. Today, global supply networks are especially susceptible to interruptions caused by natural catastrophes, geopolitical conflicts, and cyberattacks due to their complexity. Recent studies underscore the necessity for flexibility and adaptive risk management to guarantee durability in supply chains. Aljohani (2023) [17] highlighted the use of analytical models and real-time tracking systems to proactively detect hazards, hence improving agility and quickness in supply chains. This strategy enhances readiness and flexibility in an unpredictable global landscape.

Blockchain technology has been used as a revolutionary instrument for enhancing transparency, accountability, and trust inside supply chains. It provides decentralised and irreversible record-keeping, ensuring accountability and mitigating the danger of fraud, infringement, and data tampering. Recent improvements have shown its significance in mitigating disruption risks, including those stemming from unstable geopolitical circumstances or pandemic-related shocks. Etemadi et al. (2023) [18] investigated the role of blockchain in augmenting supply chain resilience via secure traceability and real-time disruption surveillance. R. Tan et al. (2023) [19] illustrated the application of blockchain in vaccination supply chains ensuring authenticity and accountability while tackling significant issues including counterfeit prevention and logistical efficiency.

The integration of blockchain and machine learning is becoming effective in thoroughly mitigating supply chain risks. Blockchain guarantees data integrity and traceability, whilst machine learning provides predictive and prescriptive analytics to enhance decision-making. Wu et al. (2023) [20] presented frameworks that amalgamate blockchain with machine learning for green supply chains, enhancing visibility and environmental sustainability. Zhang et al. (2023) [21] emphasised the efficacy of blockchain-enabled platforms in reverse supply chains, especially for the management of high-value resources such as power batteries.

Machine learning (ML) is progressively utilised in SCM for predictive analytics, anomaly identification, and demand forecasting. Machine learning approaches enable organisations to discern patterns and possible dangers within complicated information, facilitating proactive risk mitigation tactics.

Kayikci et al. (2024) [22] conducted comprehensive research on the function of machine learning in examining intricate blockchain data structures, offering insights into overcoming problems such as sparse data and real-time volatile modifications in blockchain settings. Paramesha et al. (2024) [23] demonstrated the use of blockchain for safe data management and machine learning for modelling and prediction to reduce financial risks in supply chains, showcasing practical applications and outcomes.

Although blockchain guarantees accountability and tracking, while machine learning offers predictive analytics, limited research addresses the cohesive integration of both technologies into a singular framework for holistic risk management. Much research investigates these technologies in isolation, resulting in a deficiency of integrated application solutions. To address these gaps, it is essential to design scalable, sustainable, and experimentally verified frameworks that include blockchain and machine learning, taking into account different uses and real-world limitations.

3. Methodology

Effective SCM is essential for facilitating the uninterrupted movement of goods, services, and information throughout different phases of production and distribution. Nonetheless, irregularities in the supply chain may result in interruptions, inefficiencies, and monetary losses. These abnormalities may arise from data input mistakes, operational problems, or possible fraudulent activity. This article utilises blockchain and machine learning approaches to secure and identify anomalies throughout a SCM dataset to tackle these difficulties.

3.1 Dataset Collection

This study illustrates the capability of machine learning in tackling significant difficulties in supply chain management through the automation of anomaly detection and classification by providing a pragmatic solution for enhancing efficiency in operations and decision-making. The dataset is obtained from Kaggle (https://www.kaggle.com/datasets/lastman0800/supply-chain-management) [24].

The methodology encompasses a sequential procedure, commencing with data exploration and pre-processing, succeeded by anomaly identification, model training, and optimisation. Every step is formulated to guarantee effective and precise anomaly identification inside the SCM dataset. The dataset includes data types, column count, and missing values. The dataset initially had 1000 rows and 23 columns represented as a shape of (1000, 23) evaluated each column to determine its significance to the analysis, eliminated superfluous or unnecessary columns, including those exhibiting consistent values across rows or minimal fluctuation. Upon eliminating unimportant columns or those containing excessive NULL values, we are left with 20 columns, including:

▪	SCM Practices	1000 non-null	object
▪	Supplier Count	1000 non-null	int64
▪	Inventory Turnover Ratio	1000 non-null	float64
▪	Lead Time (days)	1000 non-null	float64
▪	Order Fulfilment Rate (%)	1000 non-null	float64
▪	Customer Satisfaction (%)	1000 non-null	int64
▪	Technology Utilized	1000 non-null	object
▪	Supply Chain Agility	1000 non-null	object
▪	Supplier Lead Time Variability (days)	1000 non-null	float64
▪	Inventory Accuracy (%)	1000 non-null	float64
▪	Transportation Cost Efficiency (%)	1000 non-null	float64
▪	Supply Chain Integration Level	1000 non-null	object
▪	Supply Chain Complexity Index	1000 non-null	object

▪	Cost of Goods Sold (COGS)	1000 non-null	float64
▪	Operational Efficiency Score	1000 non-null	float64
▪	Revenue Growth Rate out of (15)	1000 non-null	float64
▪	Supply Chain Risk (%)	1000 non-null	float64
▪	Supplier Collaboration Level	1000 non-null	object
▪	Supply Chain Resilience Score	1000 non-null	float64
▪	Supplier Relationship Score	1000 non-null	float64

And then saved the cleaned and updated dataset to a new file for ease of use in later stages.

3.2 Blockchain framework for SCM

Blockchain was first introduced as a framework for facilitating bitcoin and other cryptocurrencies Subsequently, it was developed via smart contracts, including distributed programs based on blockchain that can be executed and validated autonomously, and commenced use in SCM. The majority of blockchain attributes have encouraged producers to adopt this technology for the conveyance of their goods to customers. While blockchain technology facilitates transportation (supply) by reducing processing time and costs, it also presents drawbacks including susceptibility to many assaults, and the management framework remains largely undefined. This section delineates the technological methodology for employing blockchain to safely store and monitor critical transactions inside a supply chain network. The algorithm utilises the immutable and decentralised characteristics of blockchain to improve transparency, reliability, and confidence among every party involved.

Algorithm: Blockchain to Store Key Transactions

Step 1: Initialise Blockchain Network

- Specify Blockchain Category, set up Blockchain Nodes, Choose Agreement Protocol

Step 2: Establish Data Framework for Transactions

- Develop a transaction structure:

{‘transactionID': ‘bigint',

'productID': 'varchar',

'timestamp': datetime',

'supplierID': 'varchar',

'location': ‘geography',

'status': 'char',

'metadata': ‘Char’}

- Hash Sensitive Information:

Implement SHA-3 hashing on highly sensitive information to ensure data privacy and indestructibility.

For instance: hashed_productID = SHA-3(productID).

Step 3: Verification of Transactions

- Confirm Transaction Validity:

Employ digital signatures to authenticate the sender's identity.For Example: -

Sender's signature: signature = sign(privateKey, transactionData).

The receiver authenticates: verify(publicKey, signature, transactionData).

- Verify Adherence to Smart Agreements:

Enforce business regulations within smart contracts (e.g., 'Only authenticated suppliers are permitted to initiate transactions'). Confirm data integrity and assure compliance prior to documenting the transaction.

Step 4: Incorporate Transaction into Blockchain

Disseminate transaction (T) to blockchain nodes and implement the consensus procedure to authenticate the transaction. Add Block to the Blockchain. Authenticate transaction authenticity by recalculating the Merkle root and comparing it with the root provided in the block header.

Step 5: Augmentation of Security Measures

- Implement Access Control Mechanisms:

Establish role-based authorisation using smart agreements to avert unauthorised access.

- Employ encryption for crucial data:

Encrypt fields such as agreements with suppliers and customer information prior to hashing and storage.

Step 6: Scaling and Effectiveness

- Archive obsolete blocks off-chain to facilitate expedited retrieval of current transactions while preserving inviolability.

This section was constructed utilising the blockchain and smart contracts to identify counterfeit items, provide traceability without intermediaries, and eliminate a single point of failure in SCM. Subsequently, machine learning (ML) may be amalgamated with blockchain for examining the archived supply chain data for insights and risk forecasts.

3.3 Integration of Machine Learning in SCM

Effective SCM is essential for facilitating the uninterrupted movement of products, services, and data throughout different phases of production and distribution. Nonetheless, risk in the supply chain may result in interruptions, inefficiencies, and monetary losses. These risks may arise from data input mistakes, operational deficiencies, or even fraudulent activity. This study uses machine learning approaches to identify and detect risks in a SCM dataset. In figure 3, we can see the flow of integration.

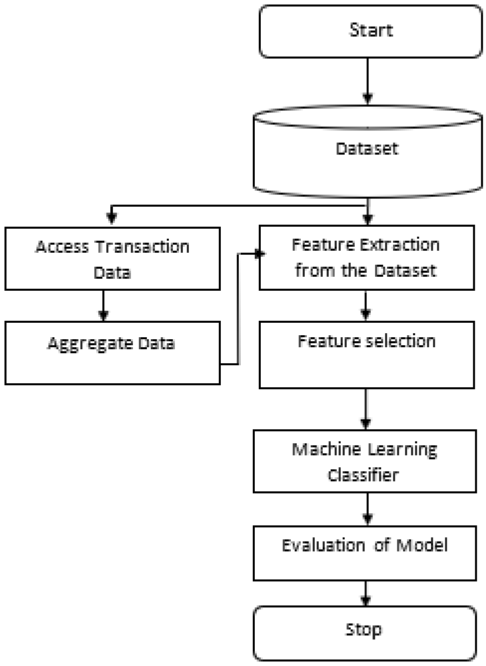

Figure 3: Working Principle for Proposed Study

The paper incorporates a thorough pipeline of data preparation and risk detection using machine learning classification to deliver a fully automated and adaptable solution. Initially, exploratory data analysis (EDA) was performed to comprehend the dataset's structure and detect significant aspects. Subsequent phases involved data preparation, which encompassed encoding categorical variable, scaling numerical values, and eliminating unnecessary or constant-value fields to enhance model precision and effectiveness.

An essential phase in the workflow was risk identification accomplished by the Local Outlier Factor (LOF) method. LOF assesses the local density variation of a certain information point with relation to its neighbours; therefore, successfully detecting outliers within the sample. LOF operates by contrasting the density of a data point with that of its neighbouring points. A point is deemed an outlier if its density is markedly inferior to that of its surrounding points. This is the sequential operation of LOF:

- **Identifying Neighbours:** For each data point, LOF determines the nearest neighbours (k-nearest neighbours or k-NN) utilizing distance measures.
- **Reachability Distance:** The Local Outlier Factor (LOF) computes the reachability distance, which quantifies the separation between two places while accounting for the density of adjacent points. This assists in determining if a point is segregated from its adjacent points.
- **Local Reachability Density (LRD):** Subsequently, LOF calculates the Local Reachability Density (LRD) of a point, serving as an approximation of the density in the vicinity of that point. If a point is encircled by a reduced density of points relative to its neighbours, its Local Reachability Density (LRD) will be diminished.
- **LOF Score Calculation:** The LOF score for every point is ultimately determined by the ratio of the Local Reachability Density (LRD) of the point to the LRDs of its neighbours, as defined by

LOF. The occurrence is an aberration, as its local density is significantly lower than that of its neighbours, as indicated by an elevated LOF score.

Therefore, equation (1), (2) and (3) that describe the identification of outlier as follows.

$$Reach\_Distance_{(p,o)} = \max\left(k - distance(o), distance(p,o)\right) \quad (1)$$

$$LRD(p) = \frac{1}{\frac{1}{k}\sum_{o \in n_{k(p)}}\left(Reach\_Distance_{(p,o)}\right)} \quad (2)$$

$$LOF_{(p)} = \frac{\sum_{o \in n_{k(p)}} \frac{LRD_{(o)}}{LRD_{(p)}}}{\frac{1}{k}\sum_{o \in n_{k(p)}}\left(Reach_{Distance_{(p,o)}}\right)} \quad (3)$$

Where, p is point and o is neighbour, distance (p, o) represents the actual distance across points p and o. k-distance(o) represents the k-distance of points.

LRD(p) denotes the local reachability density of neighbour o, whereas LOF(p) represents the reachability density of point p.

We employed the Elbow Method to determine the optimal number of neighbours (k) identifying the optimum value for k as 20 for the LOF method. The objective is to calculate the LOF scores for different values of k and identify the point at which the average LOF score stabilizes. This assists us in selecting the ideal number of neighbours that achieves an optimal equilibrium between identifying genuine outliers and minimizing false positives.

Following the acquisition of predictions from LOF, the outlier values -1 (indicating risk) and 1 (indicating inliers) were transformed into a binary format. This binary field signifies whether a data point is classified as risk or not.

3.4 Classification Algorithm

After data preparation through preprocessing, risk identification, and partitioning into training and test sets, we advanced to model training utilising several machine learning methods. This method enables us to evaluate the efficacy of many models and choose the most effective one for risk detection. The algorithms include Random Forest, Support Vector Machine, Logistic Regression, and Naive Bayes.

4. Results and Discussions

After the training and testing of several machine learning methods, we assessed their performance utilising essential measures such as the confusion matrix, recall, F1-score, accuracy, and precision. The purpose of training numerous algorithms is to investigate various methods for addressing the anomaly detection issue and determine which algorithm is most effective for this specific dataset. Through comparison of the findings, we may evaluate which model achieves an optimal equilibrium between under fitting and over fitting; hence, yielding the most dependable predictions. The outcome can be seen in Table1 and Table 2.

Table 1: Comparison between Different Machine Learning Classifier for (a) Random Forest (b) Support Vector Machine (c) Logistic Regression and (d) Naïve Bayes

Model	Parameter	Values (%)
Random Forest	Accuracy	97.0
	Precision	97.0
	Recall	99.0
	F1-Score	98.0
Support Vector Machine	Accuracy	97.0
	Precision	98.0
	Recall	99.0
	F1-Score	98.0
Logistic Regression	Accuracy	96.5
	Precision	97.0
	Recall	98.0
	F1-Score	99.0
Naive Bayes	Accuracy	92.0
	Precision	94.0
	Recall	95.0
	F1-Score	94.0

Table 2: Comparison of Training Time for Different Machine Learning Classifier for (a) Random Forest (b) Support Vector Machine (c) Logistic Regression and (d) Naïve Bayes

ML Algorithm	Training Time (ms)
Random Forest	123.1
Support Vector Machine	13.5
Logistic Regression	34.2
Naive Bayes	10.0

This part involves hyper parameters tweaking with Optuna, a renowned optimisation package for machine learning. Optuna is engineered to automate the identification of optimal hyper parameters by effectively navigating the hyper parameter space and reducing the computational expense of tuning. It employs advanced optimisation algorithms to enhance model performance more efficiently than conventional grid or random search techniques. Optuna's hyper parameter tuning procedure enables the enhancement of model performance by the adjustment of parameters like tree depth, number of estimators, regularisation terms, learning rate, and others in accordance with a specified optimisation objective. The optimal hyperparameters are determined through the assessment of several trials, guaranteeing that the models function at their peak capability. Figure 4 and figure 5 provide a graphical illustration of above outcome.

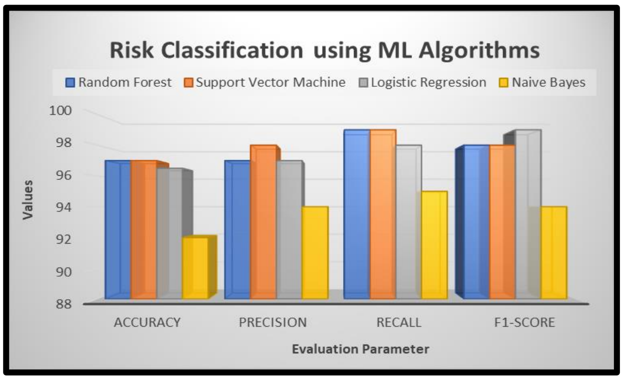

Figure 4: Comparison of Outcome for Proposed Model using SCM Dataset

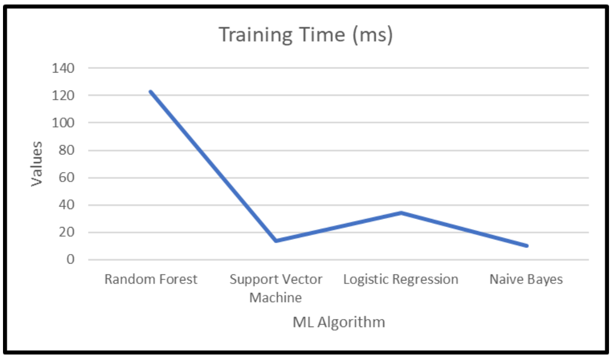

Figure 5: Comparison of Training Time for Proposed Algorithms

5. Conclusions and Future Scope

This project has concentrated on creating a secure connection utilising a blockchain foundation and identifying a risk detection system through various machine learning methodologies. The blockchain framework delineates a methodical strategy for utilising blockchain to privately archive critical transactions. The process begins with the initialisation of the blockchain network and the establishment of an organised system for transaction data that includes hashed private data. Transactions are authenticated using digital signatures and adherence to intelligent contracts prior to their inclusion in the blockchain through a consensus method. Security is fortified by role-based access restrictions and encryption, but scalability is attained by archiving obsolete blocks off-chain to boost performance. The hyper parameter tuning method indicated that models such as Random Forest and Support Vector Machine attained optimal outcomes, achieving accuracies of 97% along with elevated accuracy, recall, and F1 scores. Although Naive Bayes was efficient and rapid, its performance was inferior to that of the other models. The amalgamation of blockchain technology with machine learning presents a revolutionary method for SCM, tackling enduring issues such as privacy protection, risk assessment, and disruption prediction. Future research may be broadened to incorporate supplementary alternative or optimisation methodologies for parameter management and investigate categorisation using deep neural networks.

References

[1] Sahoo, S., Kumar, S., Sivarajah, U., Lim, W. M., Westland, J. C., & Kumar, A. (2024). Blockchain for sustainable supply chain management: trends and ways forward. Electronic Commerce Research, 24(3), 1563-1618.

[2] Islam, R., Ansari, M. E., Dewan, M. A., Sultana, S., & Rivin, M. A. H. (2024). Supply Chain Management Analysis and Design for a Variety of Economic Scenarios, Including Data and System Administration. Journal of Software Engineering and Applications, 17(10), 770-785.

[3] Ngo, V. M., Quang, H. T., Hoang, T. G., & Binh, A. D. T. (2024). Sustainability-related supply chain risks and supply chain performances: The moderating effects of dynamic supply chain management practices. Business Strategy and the Environment, 33(2), 839-857.

[4] Okoye, C. C., Ofodile, O. C., Tula, S. T., Nifise, A. O. A., Falaiye, T., Ejairu, E., & Addy, W. A. (2024). Risk management in international supply chains: A review with USA and African Cases. Magna Scientia Advanced Research and Reviews, 10(1), 256-264.

[5] Shahid, M. I., Hashim, M., Baig, S. A., Manzoor, U., Rehman, H. U., & Fatima, F. (2024, January). Managing supply chain risk through supply chain integration and quality management culture. In Supply Chain Forum: An International Journal (Vol. 25, No. 1, pp. 62-74). Taylor & Francis.

[6] Whig, P., Remala, R., Mudunuru, K. R., & Quraishi, S. J. (2024). Integrating AI and quantum technologies for sustainable supply chain management. In Quantum Computing and Supply Chain Management: A New Era of Optimization (pp. 267-283). IGI Global.
[7] Moosavi, J., Naeni, L. M., Fathollahi-Fard, A. M., & Fiore, U. (2021). Blockchain in supply chain management: a review, bibliometric, and network analysis. Environmental Science and Pollution Research, 1-15.
[8] Tezel, A., Febrero, P., Papadonikolaki, E., & Yitmen, I. (2021). Insights into blockchain implementation in construction: models for supply chain management. Journal of management in engineering, 37(4), 04021038.
[9] Chowdhury, R. H. (2024). Automating supply chain management with blockchain technology. World Journal of Advanced Research and Reviews, 22(3), 1568-1574.
[10] Sarfaraz, A., Chakrabortty, R., & Essam, D. L. (2023). RPoC: An efficient and scalable consensus algorithm for SCM applications. Authorea Preprints.
[11] Meier, O., Gruchmann, T., & Ivanov, D. (2023). Circular supply chain management with blockchain technology: A dynamic capabilities view. Transportation Research Part E: Logistics and Transportation Review, 176, 103177.
[12] Alshurideh, M. T., Hamadneh, S., Alzoubi, H. M., Al Kurdi, B., Nuseir, M. T., & Al Hamad, A. (2024). Empowering Supply Chain Management System with Machine Learning and Blockchain Technology. In Cyber Security Impact on Digitalization and Business Intelligence: Big Cyber Security for Information Management: Opportunities and Challenges (pp. 335-349). Cham: Springer International Publishing.
[13] Sodiya, E. O., Jacks, B. S., Ugwuanyi, E. D., Adeyinka, M. A., Umoga, U. J., Daraojimba, A. I., & Lottu, O. A. (2024). Reviewing the role of AI and machine learning in supply chain analytics. GSC Advanced Research and Reviews, 18(2), 312-320.
[14] Tirkolaee, E. B., Sadeghi, S., Mooseloo, F. M., Vandchali, H. R., & Aeini, S. (2021). Application of machine learning in supply chain management: a comprehensive overview of the main areas. Mathematical problems in engineering, 2021(1), 1476043.
[15] Ghazal, T. M., & Alzoubi, H. M. (2021). Modelling supply chain information collaboration empowered with machine learning technique. Intelligent Automation & Soft Computing, 29(3), 243-257.
[16] Barzizza, E., Biasetton, N., Ceccato, R., & Salmaso, L. (2023). Big Data Analytics and Machine Learning in Supply Chain 4.0: A Literature Review. Stats, 6(2), 596-616.
[17] Aljohani, A. (2023). Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. Sustainability, 15(20), 15088. https://doi.org/10.3390/su152015088.
[18] Etemadi, N., Borbon-Galvez, Y., Strozzi, F., & Etemadi, T. (2023). Supply chain disruption risk management with blockchain: A dynamic literature review. Information, 12(2), 70. https://doi.org/10.3390/info12020070.
[19] R., Tan, C., Wu, D. D., & Zhao, C. (2023). Strategies choice for blockchain construction and coordination in vaccine supply chain. Computers & Industrial Engineering, 182, 109346. https://doi.org/10.1016/j.cie.2023.109346.
[20] Wu, C., Xu, C., & Zhao, Q. (2023). Research on financing strategy under the integration of green supply chain and blockchain technology. Computers & Industrial Engineering, 182, 109598. https://doi.org/10.1016/j.cie.2023.109598.
[21] Zhang, X., Feng, X., Jiang, Z., & Gong, Q. (2023). A blockchain-enabled framework for reverse supply chain management of power batteries. Journal of Cleaner Production, 415, 137823. https://doi.org/10.1016/j.jclepro.2023.137823.
[22] Kayikci, S., & Khoshgoftaar, T. M. (2024). Blockchain meets machine learning: a survey. Journal of Big Data, 11(1), 9.
[23] Paramesha, M., Rane, N. L., & Rane, J. (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review. Partners Universal Multidisciplinary Research Journal, 1(2), 51-67.
[24] Xiong, T. (2024). The analysis of the impact of different supply chain factors using statistical perspective. Applied and Computational Engineering, 87, 241-249.
[25] Kamal Kant, Sarvesh Pandey & Udai Shanker (2024). Addressing Blockchain Efficiency: A study on Super Node-Based Consensus Mechanism" Proceedings of the 1st International conference on Advanced Computing and Emerging Technologies (ACET), 23-24 August 2024 organized by the Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, India.
[26] Kamal Kant under the supervision of Sarvesh Pandey & Udai Shanker (2022). A Journey from Commit Processing in Distributed Databases to Consensus in Blockchain" Proceedings of the 38th International Conference on Data Engineering (ICDE 2022), Virtual Event, PhD Symposium, May 9-12, 2022