Fraud Detection In Supply Chain: An AI And Blockchain-Based Approach

[1]Pratheek Rao MP, [2]Nihar Mandahas, [3]Rishabh Kumar Lal, [4]Prathik R S ,[5]Dr Manas M N
[1]Student, [2]Student, [3]Student ,[4]Student,[5]Associte Professor
R V College of Engineering

Abstract— Fraud in global supply chains—especially in the automotive industry—continues to be a major concern, causing massive financial losses, damaging reputations, and disrupting operations. In response to this growing threat, our research presents a smart and practical solution: an AI-powered fraud detection system built to spot and stop fraud before it spreads. Using a combination of machine learning techniques like Random Forest, XGBoost, SVM, and Logistic Regression, the system can quickly identify unusual behavior, flag suspicious transactions, and detect fraud in real time. But detecting fraud isn't enough—we also need to prevent it. That's where blockchain comes in. By recording every transaction on a secure, tamper-proof digital ledger, we ensure that supply chain data stays transparent and trustworthy. This approach helps block counterfeit parts from entering the system and protects everyone involved—from suppliers to end customers. We've made this system scalable and easy to integrate into real-world businesses by deploying it via Hugging Face APIs, so companies can plug it right into their existing workflows. More than just a technical project, this solution offers a powerful entrepreneurial opportunity. It addresses a real, growing market need in supply chain security and offers a clear value proposition: reduce losses, building trust, and streamline risk management, with strong potential for commercialization, this innovation brings together engineering know-how and business strategy. The system's components—including its fraud detection models and blockchain design—are also eligible for intellectual property protection through patents or trade secrets. This gives aspiring founders a unique edge in the competitive industrial tech space. With the right partnerships, funding, and go-to-market strategy, this solution could power the next generation of tech startups focused on supply chain integrity and cybersecurity.

Index Terms— Fraud Detection, Machine Learning, Supervised Learning, Blockchain, Supply Chain Security

I. INTRODUCTION

The global supply chain is a massive, interconnected web that brings together suppliers, manufacturers, logistics providers, and retailers—all working across borders to move goods and services efficiently. While this tightly woven system helps lower costs and improve delivery times, it also opens the door to serious risks: fraud, cyberattacks, and the spread of counterfeit products. As companies go digital and expand their global reach, fraudulent practices are becoming more sophisticated and harder to detect. In fact, the Association of Certified Fraud Examiners (ACFE) estimates that organizations worldwide lose about **$4.5 trillion every year** due to fraud, waste, and abuse within supply chains [1]. The 2024 PwC Global Economic Crime Survey echoes this concern, reporting that **47% of companies have faced supply chain fraud** in the past two years, much of it involving cyber-enabled threats, costing businesses over **$600 billion annually** [2].

Fraud in supply chains comes in many forms: procurement scams, counterfeit products, cargo theft, cyber fraud, and false compliance documentation. Each one can damage businesses, disrupt operations, and erode customer trust. According to the OECD, counterfeit goods alone now account for **3.3% of global trade**, totalling around **$509 billion** [3]. The automotive industry is especially vulnerable. Fake parts like airbags, brake pads, spark plugs, and other components not only lead to **$45 billion in global losses annually** but have also been tied to fatal accidents. These aren't just economic threats—they're safety hazards. Fraud is often facilitated by bribery, fake documents, and poor traceability systems that allow unverified or substandard products to slip through the cracks.

Among all these challenges, counterfeit auto parts stand out as one of the most urgent issues. Beyond the financial damage, these fake components can—and have—cost lives. A U.S. Federal Trade Commission (FTC) report linked **counterfeit airbags** to fatal crashes, underscoring the need for more effective fraud detection. In response, forward-thinking manufacturers are now using a combination of **blockchain technology for traceability**, **AI-based anomaly detection**, and **RFID tracking** to keep fake parts out of the system

To address this growing threat head-on, our research proposes a hybrid solution that brings together **machine learning** and **blockchain technology**. By applying powerful models such as Random Forest, XGBoost, and SVM, our system can sift through large amounts of transactional data to detect irregularities and suspicious behavior in real time. The blockchain layer ensures that every component's journey through the supply chain is securely logged, tamper-proof, and fully transparent.
What makes this effort especially timely is the surge in **entrepreneurial interest** around AI and blockchain, particularly in sectors like automotive and logistics [31][32]. These technologies aren't just tools for detection—they're launching pads for innovation. Drawing inspiration from the **Lean Startup methodology** [33] and real-world examples of AI-powered ventures [34], this research positions fraud detection not just as a technical challenge, but as a business opportunity.

In short, this study doesn't just aim to prove how AI and blockchain can fight fraud—it also highlights how this approach can fuel the next wave of tech-driven entrepreneurship. The solution improves supply chain resilience, protects consumers, and opens the door for scalable, impactful ventures in one of the world's most critical industries.

II. LITERATURE REVIEW

The automotive supply chain is a vast, globally connected system involving manufacturers, suppliers, logistics partners, and retailers. With so many players in the mix, ensuring transparency, security, and the authenticity of parts is critical—not just for smooth operations, but for public safety too. Over the years, the industry has faced persistent issues like counterfeit components, rigged procurement processes, fake contracts, and violations of regulatory standards. While traditional tools like barcodes, ERP systems, and manual audits have helped, they simply haven't kept up with the pace and complexity of fraud in today's digitized world. This gap has created a strong opportunity for entrepreneurs to step in with newer technologies like **blockchain** and **AI** [31].

Blockchain stands out as a powerful tool for building trust and traceability in supply chains. Its decentralized, tamper-proof ledger records every transaction in real time, offering a clear, unchangeable trail of where each part comes from and how it moves through the system. Research by Esfandiari (2022) [6] shows how blockchain adoption in the Mexican automotive sector helped reduce fraud by strengthening transparency and safety between stakeholders. Platforms like Ethereum also bring in the use of **smart contracts**, which can automate supplier certification checks, enforce quality standards, and even process payments—minimizing the need for manual verification [7]. Of course, challenges remain. For startups and small companies especially, blockchain adoption can be expensive and technically demanding. Resistance to change from established players is another hurdle [32].

When it comes to detecting fraud in vehicle verification systems—like fake car registrations or tampered grant documents—rule-based logic systems have shown promise, especially when labelled data for training AI is hard to find [8]. These systems use preset rules to catch inconsistencies. But they work even better when combined with AI. Machine learning models, including decision trees, neural networks, and ensemble techniques, have proven more flexible and accurate in identifying shifting fraud patterns [11]. These AI tools don't just catch fraud after it happens—they predict and prevent it in real time, offering real value to businesses and innovators in the automotive space.

Blockchain's impact is also reaching beyond manufacturing and logistics into areas like **car-sharing, identity verification, and consumer vehicle services**. Technologies like Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs) allow for secure data exchanges between users, providers, and verifiers. This can help prevent identity-based fraud in systems like EV charging or vehicle rental platforms [9]. These cases

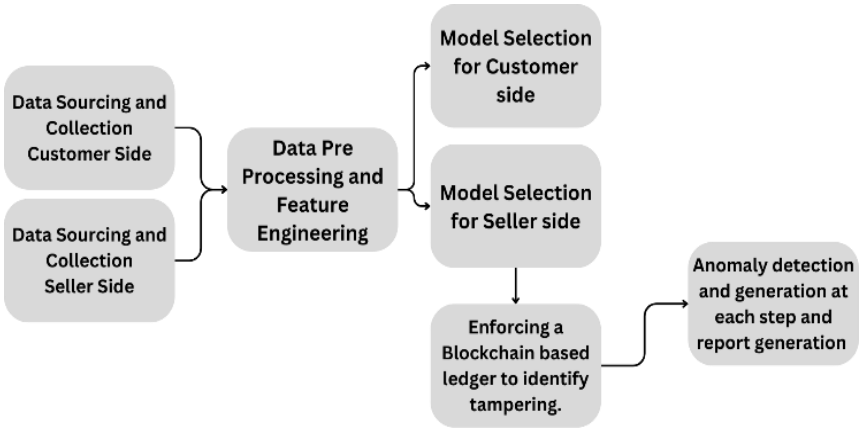
aren't just cool they represent real business opportunities, especially in the fast-growing B2B and B2C auto service markets.

With e-commerce and online procurement rising sharply, so too are fraud-related risks. That's why businesses are increasingly turning to **AI-driven fraud detection tools** that combine deep industry knowledge with smart algorithms. Research shows that blending supervised learning (which learns from past fraud cases) with unsupervised techniques (which catch new, unknown patterns) leads to better fraud detection overall [11, 34]. Still, developing sustainable business models around this tech isn't easy. According to [33], startups need to stay lean, test fast, and respond to user feedback quickly—especially in regulated sectors like automotive

Finally, several researchers [31, 34] stress the value of bringing together engineering, business, and technology disciplines to tackle fraud at scale. This kind of cross-disciplinary innovation opens doors for new ventures focused on AI-powered risk mitigation, SaaS fraud analytics, and blockchain-secured supply chain platforms. These solutions also offer strong potential for intellectual property protection, strategic partnerships, and large-scale market growth.

III. PROPOSED WORK

In this study, we propose a multi-faceted approach to detect fraud in global supply chains using AI and predictive analytics. Our methodology is structured into key stages, each addressing fraud detection at different points in the supply chain. The approach integrates data collection, machine learning techniques, blockchain-based ledger implementation, and anomaly detection mechanisms to ensure a robust fraud detection system



A. Data Pre-Processing

To develop an effective fraud detection system, data is collected from both customer and seller sides, focusing on behavioral patterns, transaction histories, and supply chain transparency.

On the customer side, data sources include transaction records (timestamps, payment methods, and pricing), return requests (frequency, reasons, and defects), customer complaints (refund requests due to false claims), and account metadata (historical transaction trends). These datasets are obtained through e-commerce platform integration, web scraping for external review analysis, historical customer interaction mining, and direct payment gateway data ingestion. This multi-faceted approach helps identify fraudulent activities such as return abuse, unauthorized chargebacks, and false refund claims.

On the seller and manufacturer side, data is gathered to ensure product authenticity and detect fraudulent practices like counterfeiting, price manipulation, and fake order fulfillment. Sources include inventory and shipping data (order fulfillment records, stock levels, and shipping logs), supplier reports (product origin and transaction details), product authenticity checks (batch numbers, certifications, and warranty claims), and pricing trends (sudden drops, abnormal discounts, and historical pricing). Collection methods involve ERP system integrations, blockchain-based verification, logistics and supply chain data ingestion, and crowdsourced validation from customers and auditors. By analyzing seller-side data, the system prevents fraudulent product listings and ensures supply chain integrity.

B. Data Pre-Processing

Once collected, the raw data undergoes extensive pre-processing to remove inconsistencies, enhance integrity, and extract meaningful features that improve the AI model's fraud detection capabilities. Missing values are handled using techniques such as mean or mode imputation and predictive modeling to ensure data completeness. Duplicate records are identified and removed to prevent biases that could affect model performance. Categorical variables, such as text-based data, are converted into numerical formats using one-hot encoding and word embeddings, making them compatible with machine learning algorithms. Additionally, scaling and normalization techniques, including Min-Max scaling and Z-score normalization, are applied to standardize data across different variables and maintain consistency. Feature engineering is then performed to extract relevant insights that enhance fraud detection accuracy. Behavioral features are derived by analyzing customer purchase and return habits to detect irregular patterns. Temporal features are extracted through time-series analysis, identifying trends such as sudden spikes in return requests that may indicate fraudulent activity. Transactional features, including order frequency, payment methods, and refund behaviors, are examined to uncover anomalies and suspicious activities. Finally, anomaly scores are assigned to transactions based on deviations from normal purchasing behaviors and past instances of fraudulent activity, allowing for a more robust fraud detection mechanism.

C. Implementation

The implementation of the fraud detection system involves the integration of multiple technologies, including machine learning, natural language processing, blockchain, and cloud-based solutions, to develop a robust and efficient fraud identification framework. The system leverages machine learning algorithms, such as Logistic Regression, Random Forest, XGBoost, and Support Vector Machines (SVM), trained on labeled datasets to differentiate between fraudulent and non-fraudulent transactions. These models analyze transaction records, return patterns, and behavioral anomalies to predict potential fraud with high accuracy. Additionally, deep learning frameworks like PyTorch and Hugging Face's transformer models are utilized for fraud-related text analysis, enabling the system to detect deceptive customer reviews and fraudulent claims using natural language processing techniques.

The system's model is built using Python-based machine learning libraries such as scikit-learn, XGBoost, and pandas for data manipulation and model training. These libraries facilitate efficient preprocessing, feature extraction, and model evaluation using tools like confusion matrices and classification reports. The fraud detection component also incorporates NumPy for numerical computations and Pickle for model serialization, ensuring seamless deployment and reuse of trained models. Visualization tools such as Matplotlib and WordCloud help represent fraud trends, feature distributions, and textual fraud patterns extracted from customer interactions.

For the cloud-based development environment, Jupyter Notebook and Google Colab are used to streamline interactive coding, model training, and real-time analysis. The system also integrates React for the front-end interface, enabling a user-friendly e-commerce prototype where fraud detection mechanisms are seamlessly embedded. The Hugging Face API and Gradio facilitate real-time fraud detection inference, allowing users to interact with the system and verify suspicious activities effectively.

Blockchain technology plays a critical role in ensuring product authenticity and preventing supply chain fraud. The implementation involves a permissioned blockchain network where manufacturers generate unique QR codes for each product. These QR codes are linked to immutable blockchain records containing product details such as serial numbers, manufacturer information, and historical transactions. Upon receiving a product, buyers can scan the QR code to retrieve the product’s blockchain data, verifying its authenticity and ensuring that no tampering has occurred during the supply chain process. This approach enhances transparency and security by preventing counterfeit products, price manipulation, and fraudulent order fulfillment.

The blockchain network is developed using Solidity smart contracts, deployed on a Ganache test network for safe and efficient prototyping. These smart contracts automate business rules and transactions, ensuring that only verified participants, such as manufacturers, sellers, and buyers, can interact with the system. The Ganache interface provides a visual representation of blockchain transactions, enabling real-time tracking of product movements and ensuring that all interactions are securely recorded.

Additionally, the fraud detection system incorporates a Generative AI-powered module to analyze customer reviews and detect fraudulent activities. Using advanced natural language processing models, the system can understand context, sentiment, and linguistic nuances to identify deceptive reviews and false claims. This component strengthens the fraud detection mechanism by flagging suspicious customer interactions that traditional rule-based methods might overlook.

Overall, the implementation of this fraud detection system combines machine learning, blockchain, cloud computing, and generative AI to provide a scalable, transparent, and highly accurate fraud identification framework. The integration of QR-based authentication, smart contracts, and AI-driven analysis ensures that both customers and sellers are protected from fraudulent activities, making e-commerce transactions more secure and trustworthy.

D. Prototype & Testing

The prototype provides distinct functionalities for both buyers and sellers, ensuring a secure and fraud-free transaction environment. Buyers can log in to their accounts, browse products, and place orders, with each transaction being evaluated for potential fraud using machine learning models. The seller fraud detection model assesses whether a product listing is fraudulent based on account metrics and past transaction behavior. Additionally, sentiment analysis is performed on customer reviews to detect manipulated or deceptive feedback, further improving fraud detection accuracy. Buyers are also provided with a QR code scanning feature that retrieves product authenticity details from the blockchain, ensuring that purchased items are genuine and have not been tampered with. Sellers, on the other hand, have access to a dashboard where they can manage their product listings and monitor incoming orders. The system uses a buyer fraud detection model to analyze metrics such as return-to-order ratios, VPN usage, account age, and transaction history, allowing sellers to make informed decisions about potential fraudulent buyers. This helps prevent abuse of return policies, fake claims, and unauthorized chargebacks. Blockchain authentication is a critical component of the prototype, ensuring the integrity of product listings. Each product is assigned a unique QR code linked to a blockchain ledger that contains manufacturer details and product history. This immutable ledger allows buyers to verify a product's authenticity simply by scanning the QR code, adding an additional layer of trust to online purchases.

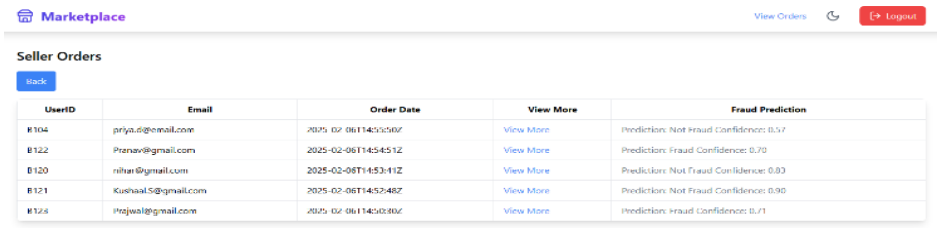
To ensure the reliability and efficiency of the fraud detection system, extensive testing was conducted at various stages of development. The testing process involved data validation, model accuracy assessments, integration testing, and blockchain verification.

The initial phase of testing focused on data preprocessing and model training. The dataset sourced from Deloitte was cleaned, normalized, and structured to eliminate inconsistencies and missing values. Key fraud detection metrics were identified for both buyer and seller fraud detection models. Feature engineering was performed to transform raw data into meaningful indicators, enhancing model performance. Multiple machine learning algorithms, including Logistic Regression, Decision Tree, Random Forest, SVM, XGBoost, and Gradient Boosting, were evaluated, with Random Forest emerging as the optimal choice due to its high accuracy and robustness against overfitting. Hyperparameter tuning was carried out to fine-tune the model's precision and recall, ensuring a balanced trade-off between false positives and false negatives.

The integration of machine learning models into the web application was tested through API calls to Hugging Face, verifying the models' ability to process real-time fraud detection requests. Functional tests were conducted to ensure that fraud detection predictions were accurate and provided timely feedback to users. The sentiment analysis model was validated using a dataset of authentic and fraudulent reviews, confirming its ability to detect manipulated sentiments that might indicate fraudulent activity.

Blockchain implementation was tested to verify the immutability and accessibility of product authentication records. The QR code functionality was examined to ensure seamless retrieval of product details from the blockchain ledger. Load testing was conducted to evaluate the scalability of the blockchain system under high transaction volumes, ensuring that product authentication remained efficient even with multiple concurrent verifications

Overall, the prototype and testing phase successfully demonstrated the system's ability to detect fraudulent



activities and verify product authenticity in real-time. By integrating machine learning for fraud detection and blockchain for transparency, the system offers a scalable and practical solution to combating fraud in e-commerce transactions.

Figure 2. Customer Side Fraud Detectio

IV. Results and Discussion

The experimental procedure includes the following steps: organizing the experiment, preparing the code, training the model, evaluating and testing it, and comparing the findings.

A. Experimental Setup

The training environment utilized Google Colab, leveraging its T4 GPU for training.
The performance of various machine learning models was evaluated to determine the most effective fraud detection algorithm. The models were assessed based on key performance metrics, including accuracy, precision, recall, and F1-score. Among the tested models—Random Forest, Logistic Regression, Gradient Boosting, XGBoost, and Support Vector Machine (SVM)—the Random Forest classifier demonstrated the highest overall performance, making it the optimal choice for fraud detection.

The Random Forest model achieved an accuracy of 95.41%, indicating its ability to correctly classify fraudulent and non-fraudulent transactions with high reliability. The precision of 95.77% highlights the model's effectiveness in minimizing false positives, ensuring that legitimate users are not mistakenly flagged as fraudulent. Additionally, the recall score of 89.86% reflects the model's ability to correctly identify fraudulent cases, reducing the likelihood of undetected fraud. The F1-score of 92.81% balances precision and recall, confirming the model's robustness and efficiency in handling fraud detection tasks.

Comparatively, while other models such as XGBoost (92.37% accuracy) and Gradient Boosting (91.40% accuracy) also performed well, they fell slightly behind Random Forest in terms of overall performance. Logistic Regression exhibited the lowest accuracy (89.13%) and recall (76.55%), making it less effective in identifying fraudulent transactions. SVM achieved a respectable accuracy of 92.1%, but its recall score (84.83%) was lower than that of Random Forest, indicating a higher risk of missing fraudulent cases.

The results suggest that ensemble-based models, particularly Random Forest, excel in fraud detection due to their ability to capture complex patterns and interactions within the data. The superior performance of Random Forest can be attributed to its robust feature selection process and ability to handle imbalanced datasets effectively.

Overall, the findings confirm that the proposed fraud detection system, powered by the Random Forest model, provides a highly accurate and efficient solution for identifying fraudulent activities in online transactions. The model's strong performance in precision and recall ensures a balanced approach, minimizing both false positives and false negatives, which is crucial for real-world fraud prevention applications.

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	95.41%	95.77%	89.86%	92.81%
Logistic Regression	89.13%	91.69%	76.55%	90.85%
Gradient Boosting	91.40%	95.74%	89.86%	92.70%
XGBoost	92.37%	95.71%	89.79%	92.60%
Support Vector Machine	92.1%	91.8%	84.83%	92.7%

Table 1. Seller Side Metrics

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	96%	95.6%	72.9%	83%
Neural Network	89.13%	91.69%	76.55%	90.85%
kNN	91.40%	95.74%	89.86%	92.70%

Table 2. Customer Side Metrics

GenAI-powered fraud detection leverages advanced natural language processing (NLP) techniques and cutting-edge generative AI models to identify fraudulent or deceptive customer reviews. This innovative approach goes beyond traditional rule-based or statistical methods by deeply understanding the nuances, context, and linguistic subtleties of written language. QR codes are generated to uniquely identify products, linking them to their blockchain records. This integration enhances traceability and user accessibility, allowing for easy verification of product authenticity.

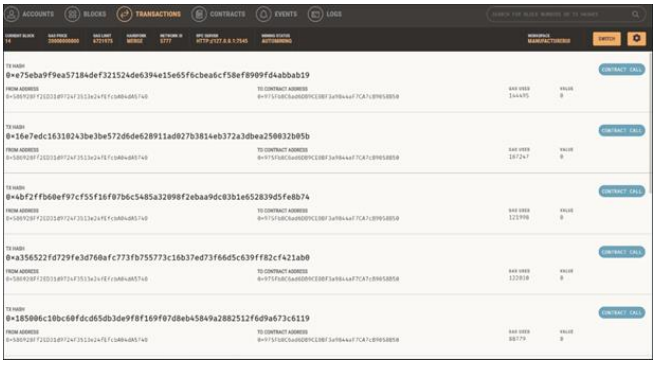


Figure 3. Ganache Based Blockchain Implementation

V. CONCLUSION

This study puts forward a powerful and timely solution to one of the biggest challenges facing the automotive industry today: fraud in the supply chain. By combining a **Random Forest-based machine learning model** with the security of **blockchain technology**, the system offers a smart, two-layered defense. On one hand, it uses AI to predict and detect fraudulent activity with high accuracy. On the other, it ensures that all transactions are recorded in a secure, tamper-proof way—critical in high-risk, tightly regulated industries like automotive manufacturing and logistics.

But this project isn't just technically impressive—it also has real **entrepreneurial promise**. The development of a working **e-commerce prototype** shows that the solution isn't just theoretical; it's ready to be used in real business environments. Its design is both holistic and practical, covering everything from fraud detection to traceability and scalable deployment. That makes it highly relevant in a world where companies are looking for smarter, safer ways to manage global supply chains.

What makes this even more exciting is how well it aligns with current trends in **AI entrepreneurship** [31], **lean innovation practices** [33], and **cross-disciplinary tech ventures** [34]. In short, this project isn't just solving a problem—it's opening the door to a new business opportunity. With its strong value proposition for manufacturers, suppliers, and logistics providers, this solution has the potential to scale, attract investment, and make a meaningful impact on global supply chain security.

VI. ACKNOWLEDGMENT

The authors would like to thank Dr K N Subramanya, Principal, R V College of Engineering, Bengaluru and Dr. Vishalakhsi Prabhu H, Associate Professor Department of Computer Science and Engineering, R V College of Engineering, Bengaluru for their timely help and constant support to complete this work

REFERENCES

[1] Organizations Worldwide Lose Trillions of Dollars to Occupational Fraud,https://www.acfe.com/about-the-acfe/newsroom-for-media/press-releases/press-release-detail?s=2022-RTTN-launch.

[2] Global Economic Crime Survey 2024 https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

[3] Global Trade in Fakes,https://www.oecd.org/en/publications/global-trade-in-fakes_74c81154-en.html

[4] 1 in 10 medical products in developing countries is substandard or falsified, https://www.who.int/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified

[5] Cybersecurity in automotive: Mastering the challenge, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge Available: https://arxiv.org/abs/2004.10934v1

[6] S. Esfandiari, "The effect of blockchain technology on supply chain management: its potential to prevent fraud ," 2022 IEEE Technology and Engineering Management Conference (TEMSCON EUROPE), Izmir, Turkey, 2022, pp. 179-183, doi: 10.1109/TEMSCONEUROPE54743.2022.9801908.

[7] M. A. Nasirudin, E. Abdullah, K. K. M. Shariff, M. S. A. M. Ali, M. K. Nordin and I. M. Yassin, "Car Grant Fraud Prevention using Ethereum Blockchain," 2023 IEEE Symposium on Computers & Informatics (ISCI), Shah Alam, Malaysia, 2023, pp. 48-52, doi: 10.1109/ISCI58771.2023.10391892.

[8] X. Wei et al., "Compliant Transport Vehicles Verification Fraud Detection of Based on Rule Inference," 2020 4th Annual International Conference on Data Science and Business Analytics (ICDSBA), Changsha, China, 2020, pp. 151-154, doi: 10.1109/ICDSBA51020.2020.00045.

[9] L. Cotugno, F. Mazzenga, A. Vizzarri and R. Giuliano, "The major opportunities of Blockchain for Automotive Industry: a Review," 2021 AEIT International Conference on Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE), Torino, Italy, 2021, pp. 1-6, doi: 10.23919/AEITAUTOMOTIVE52815.2021.9662907.

[10] Lokanan, Mark E., and Vikas Maddhesia. "Supply chain fraud prediction with machine learning and artificial intelligence." International Journal of Production Research 63.1 (2025): 286-313.

[11] Constante-Nicolalde, Fabián-Vinicio, Paulo Guerra-Terán, and Jorge-Luis Pérez-Medina. "Fraud prediction in smart supply chains using machine learning techniques." International Conference on Applied Technologies. Cham: Springer International Publishing, 2019.

[12] Kim, Bong-hyun. "Development of Online Fraud Detection and Sales Prediction Model using Supply Chain Dataset." Journal of System and Management Sciences 13.2 (2023): 501-514.

[13] Mohammed, Ahmed Farouk A. "Impact of Anti-Fraud Leadership on Fraud Detection in Saudi Private Automotive Sector in the Era of Artificial Intelligence." Tuijin Jishu/Journal of Propulsion Technology 45.3: 2024.

[14] Nguyen, H. Du, et al. "Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management." International Journal of Information Management 57 (2021): 102282.

[15] Ni, Du, Zhi Xiao, and Ming K. Lim. "A systematic review of the research trends of machine learning in supply chain management." International Journal of Machine Learning and Cybernetics 11 (2020): 1463-1482.

[16] DuHadway, Scott, Carlos Mena, and Lisa Marie Ellram. "Let the buyer beware: how network structure can enable (and prevent) supply chain fraud." International Journal of Operations & Production Management 42.2 (2022): 125-150.

[17] Shahriari, Hesam, et al. "The effect of automotive industry scandals on shareholder wealth: A supply chain perspective." Available at SSRN 4163849 (2022).

[18] Silvestre, Bruno S., Fernando Luiz E. Viana, and Marcelo de Sousa Monteiro. "Supply chain corruption practices circumventing sustainability standards: wolves in sheep's clothing." International Journal of Operations & Production Management 40.12 (2020): 1873-1907.

[19] Fraser, Iain J., Martin Müller, and Julia Schwarzkopf. "Transparency for multi-tier sustainable supply chain management: A case study of a multi-tier transparency approach for SSCM in the automotive industry." Sustainability 12.5 (2020): 1814.

[20] Schmitz, Peter. "The use of supply chains and supply chain management in the production of forensic maps using data from a fraud case." South African Journal of Geomatics 5.2 (2016): 156-174.

[21] Katz, Norman A. Detecting and reducing supply chain fraud. Routledge, 2016.

[22] Kraus, Cornelia, and Raul Valverde. "A data warehouse design for the detection of fraud in the supply chain by using the benford's law." American Journal of Applied Sciences 11.9 (2014): 1507-1518.

[23] Silvestre, Bruno S., Fernando Luiz E. Viana, and Marcelo de Sousa Monteiro. "Supply chain corruption practices circumventing sustainability standards: wolves in sheep's clothing." International Journal of Operations & Production Management 40.12 (2020): 1873-1907.

[24] [24] Beteto, Alinne, et al. "Anomaly and cyber fraud detection in pipelines and supply chains for liquid fuels." Environment Systems and Decisions 42.2 (2022): 306-324.

[25] Patterson, James L., Kimberly N. Goodwin, and Jennifer L. McGarry. "Understanding and Mitigating Supply Chain Fraud." Journal of Marketing Development & Competitiveness 12.1 (2018).

[26] Zhou, Hangjun, et al. "A distributed approach of big data mining for financial fraud detection in a supply chain." Comput Mater Continua 64.2 (2020): 1091-1105.

[27] Godwin, Benny J., N. Preethi, and Fr Jossy P. George. "Sustainable Supply Chain Analytics for Anomalously Potential Fraudulent Logistics." 2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies (TQCEBT). IEEE, 2022.

[28] Triepels, Ron, and Hennie Daniels. "Detecting shipping fraud in global supply chains using probabilistic trajectory classification." Doctoral Consortium on Enterprise Information Systems. Vol. 2. SCITEPRESS, 2015.

[29] Azzi, Rita, Rima Kilany Chamoun, and Maria Sokhn. "The power of a blockchain-based supply chain." Computers & industrial engineering 135 (2019): 582-592.

[30] [30] Cai, Yuanfeng, and Dan Zhu. "Fraud detections for online businesses: a perspective from blockchain technology." Financial Innovation 2 (2016): 1-10.

[31] [31] **Artificial Intelligence and Big Data in Entrepreneurship: A New Era Has Begun"** — Obschonka & Audretsch (2019) explore how AI and big data are reshaping entrepreneurial research and practice

[32] [32] **Critical Business Decision Making for Technology Startups – PerceptIn Case Study"** — Shows strategic decision-making in an autonomous driving startup

[33] [33] **Lean Startup in Corporations** — Edison et al. (2018) study internal innovation via lean startup methods for product development .

[34] **Automotive Innovation Case Studies** — Examples from Hyundai, Mercedes-Benz, and others illustrate open innovation models in the automotive industry