iJCEM
International Journal of Core Engineering & Management

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

LEVERAGING MACHINE LEARNING AND AI TO PREVENT FRAUD IN MANUFACTURING WARRANTY PROCESSES: A PROACTIVE APPROACH FOR ENHANCED RISK MANAGEMENT

Praveen Kotholliparambil Haridasan
Independent Researcher
Frisco, TX, USA
PraveenKHari@gmail.com

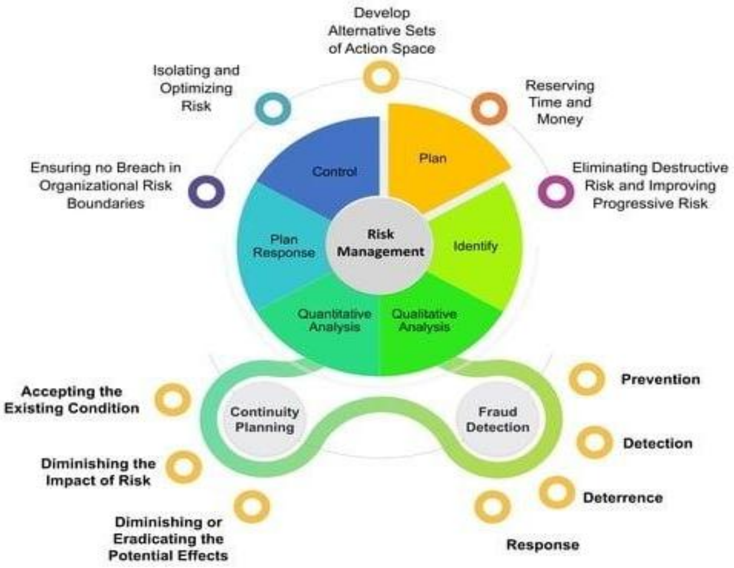
Abstract

From the development of expert systems to the widespread use of DL and ML in today's business, AI has been used successfully for decades. As computation and storage become more affordable, data-driven AI approaches have emerged as a viable option to bolster the ever-increasing complexity of industrial processes. Notwithstanding the recent popular enthusiasm, significant hurdles persist in the application of AI to smart manufacturing contexts. This study examines the utilisation of ML and AI for the identification and mitigation of fraud in manufacturing warranty processes. AI-driven solutions can save expenses, enhance risk management, and promote superior decision-making for manufacturers in the remanufacturing and consumer electronics sectors by identifying fraudulent claims and improving data accuracy. Many people have been talking about service industry fraud lately. Fraud protection and detection with remanufactured product warranties is an uncharted territory. Fraud can originate from various sources, each presenting distinct challenges. This research goal is to elucidate the principles of effective risk management and explore advanced algorithms that can mitigate the financial risks associated with warranty fraud, ensuring the integrity and reliability of warranty claims while promoting sustainable manufacturing practices.

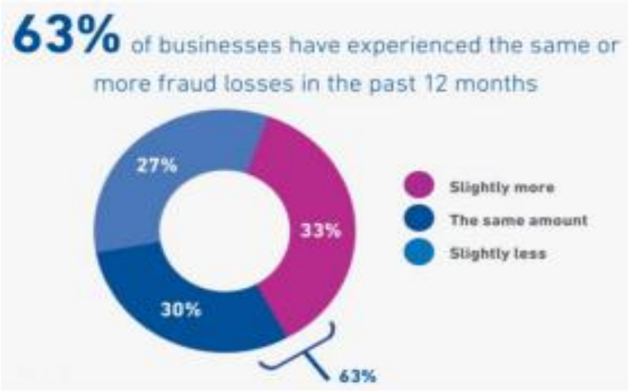
Keywords: Fraud, warranty, machine learning, AI, risk management, fraud prevention.

I. INTRODUCTION

Progress in technology and innovation has sparked the rise in consumer electronics and has flooded the marketplace with low-cost, high-quality consumer goods. The abundance of low-cost options has subsequently also led to a shift in consumer behaviour. The most notable change is that now products, especially small-scale electronics, are most often disposed of before they reach their product EOL [1]. This has caused a tendency where items, even those with remaining life, become outdated in a considerably shorter amount of time. This has the unintended consequence of making product life cycles shorter for many different types of goods, which would eventually cause natural resources to erode as businesses try to meet consumers' ever-increasing demands while simultaneously adding to landfill waste. Over the last 50 years, there has been a steady rise in interest towards environmentally friendly practices both from the public as well as the government. This has resulted in a slew of new environmental legislation that has nudged even the largest corporations into moving away from age-old practices such as disposal and more toward EOL strategies. It is possible to include environmentally aware manufacturing practices into a product at any stage of its life cycle, from the design phase to the EOL. When it comes to getting a product to fulfil environmental regulations, this application flexibility is crucial. Reduced disposal costs and permit needs, environmental penalties, increased profitability, new business prospects, revitalised staff morale, and a better environment are all outcomes of the firm's commitment to waste minimisation [2]. Businesses encounter risks, vulnerabilities, and unexpected disruptions that impair productivity and market sustainability. A risk management system must identify and mitigate risks. An organisation must combine strict risk management methods and planning documentation[3]. To limit risks, vulnerabilities, and consequences, risk management needs continuity planning and fraud detection. To reduce human errors and hazards using smart algorithms, organisations need information systems. Figure 1 depicts the graphical figure of risk management in manufacturing warranty processes.


Develop Alternative Sets of Action Space
Isolating and Optimizing Risk
Reserving Time and Money
Ensuring no Breach in Organizational Risk Boundaries
Eliminating Destructive Risk and Improving Progressive Risk
Control
Plan
Plan Response
Risk Management
Identify
Quantitative Analysis
Qualitative Analysis
Accepting the Existing Condition
Continuity Planning
Fraud Detection
Prevention
Detection
Diminishing the Impact of Risk
Deterrence
Diminishing or Eradicating the Potential Effects
Response

Fraudulent activities have become increasingly complex and widespread in today's interconnected world. Fraud in the digital age has cost a lot of money, making it a complex issue. Fraud has increased with online financial transactions[4]. As more financial transactions move online, reliable fraud detection technologies are needed. Due to the COVID-19 epidemic and economic shutdown, which changed relative demands and organisational capital, fraud is projected to rise in the next years. As technologies and security systems change[5][6][7], fraudsters create new methods. This book describes the complexity of fraudulent activities and highlights the need to reduce financial risks. In the next sections, real-time fraud detection is shown to protect online financial transactions and restore Internet trust. Figure 2 shows the businesses experiencing fraud losses in the past 12 months.



Warranty fraud is expanding in manufacturing, notably remanufacturing and consumer electronics. Manufacturers face financial risks from deceptive activities, including component replacement and substitution fraud. These activities obscure product quality feedback, forcing producers to use inaccurate data, which can lead to unnecessary recalls, poor maintenance, and bad business decisions. When customers are unfairly denied warranty claims, unreliable data can tarnish a manufacturer's reputation. To solve this problem, ML and AI must be used to construct real-time fraud detection systems and improve risk management. This paper examines these issues and proposes methods to reduce warranty fraud's impact on production.

The aim of the paper is to explore innovative solutions for mitigating warranty fraud in the manufacturing sector, particularly within the consumer electronics industry. The motivation behind this research stems from the growing prevalence of warranty fraud, which not only results in significant financial losses for manufacturers but also undermines product quality and consumer trust. By integrating machine learning and artificial intelligence techniques into warranty risk management, the paper seeks to establish a robust framework that enhances fraud detection, promotes sustainable manufacturing practices, and ultimately contributes to improved customer satisfaction and loyalty.

- The paper systematically identifies and discusses the complexities associated with warranty fraud in the manufacturing sector, highlighting its implications on product quality feedback, financial losses, and brand reputation.
- It proposes the integration of advanced machine learning and artificial intelligence techniques to develop real-time fraud detection systems, offering a technological solution to enhance warranty risk management processes.
- The study outlines a comprehensive framework for effective risk management in warranty processes, emphasising the importance of mitigating financial risks associated with warranty fraud while maintaining product quality and consumer trust.
- The paper emphasises the necessity of incorporating environmentally conscious manufacturing practices, advocating for a shift towards sustainability to counteract the negative impacts of consumer electronics waste and resource depletion.
- It provides valuable insights and recommendations for future research directions, encouraging further exploration of advanced algorithms and their applications across various manufacturing contexts to improve warranty processes and sustainability initiatives.

1. Structure of the paper

The paper is structured as follows: Section I offers an introduction to a role of machine learning and artificial intelligence in preventing fraud within manufacturing warranty processes for enhanced risk management. Section II offers an overview of the various types of fraud that occur in warranty processes in the manufacturing sector. Section III discusses the principles and aims of risk management as they relate to warranty fraud. Section IV explores advanced algorithms employed in fraud detection specifically for warranty processes. Section V presents a literature review, highlighting existing research and methodologies in the field. Finally, Section VI concludes the paper and outlines potential future work to further advance the topic.

II. OVERVIEW OF FRAUD IN MANUFACTURING WARRANTY PROCESSES

Warranty fraud has various indirect costs that may be worse than revenue loss. Research and development often use repair service agent data. Manufacturers use field data to fix product quality issues. This notion works in theory, but if the data contains false information or questionable claims, differentiating quality issues from fraudulent billing may be difficult. Thus, poor product quality feedback may delay correction[8][9]. This rising issue may cause unnecessary and costly product recalls, reducing predictive maintenance's effectiveness. The manufacturer may abandon profitable products incorrectly considered unprofitable, affecting large-scale decision-making. Warranty fraud can damage a warranty provider's brand. This happens when clients are unfairly denied warranty coverage or obtain inadequate service due to fraud. This study examines how customers try to defraud others, challenging the idea that they are only victims[10]. Customer-driven fraud sometimes occurs after the warranty term has passed. Customers may file fraudulent warranty claims for products they have never purchased. Customer fraud occurs when a customer requests repairs or replacements without warranty coverage. Sometimes, the warranty expires, the consumer damages the product, or the servicing operation is not covered by the guarantee. Although large-scale fraud does happen, customers typically conduct one or two incidents of fraud per bought goods. Table 1 lists warranty fraud examples[11].

Victim of fraud	Aim	Methodology
Warranty provider	Refund replacement	Returning or exchanging an item without a valid reason because it is not defective or fake
	Service cost avoidance	Resolving warranty repairs for goods that are no longer covered
	Service level improvement	Taking advantage of a right to superior service by claiming

When consumers buy several identical items at different times, such as tablets or LED light bulbs, and then attempt to utilise the warranty of the current product to replace the older one, that is fraud. Likewise, items that are out of warranty may have broken components that may be claimed under warranty and swapped for ones that are covered. Without a serial number or tracked parts, it is difficult to determine if the equipment or evidence of purchase is related to the malfunctioning goods. This also applies to large installations with both in-warranty and out-of-warranty equipment installed at separate times. It is possible to offer service for items that are no longer covered by the warranty if there are holes in the provider's entitlement method or data.

A. Description of the system

Table 2 describes the three groups into which the various parties might be subdivided according to their respective significance (making a remanufacturer a principal warranty provider). In the warranty service chain, there are two types of participants: "primary parties" and "secondary parties." The former assists the latter with warranty operations, and both groups have a vested interest in the successful execution of the warranty service.

Table 2: Parties involved in a warranty servicing scenario

Category	Parties
Primary	Remanufacture, service agent, customers
Secondary	Parts manufacture, sales channel, warranty administrator.
Tertiary	Inspectors, logistic companies, leasers, underwriters & insurers, govt, shareholders

The consumer is the principal actor in component replacement fraud, while a service agents (and subsequently a remanufacturer) play a role of the victim [9]. Inspection to ascertain failure source is a standard procedure in most warranty servicing systems when a product becomes nonfunctional. As soon as a failure occurs, the relevant service professionals get the necessary failure details and carry out the necessary service activities, such as replacing the faulty component or components [9]. The servicing facility receives the defective items after this procedure. The goods are brought back to working order after the maintenance method. Customers get their things back when the maintenance service is finished. Figure 3 shows the standard procedure flow diagram for all warranty maintenance types.

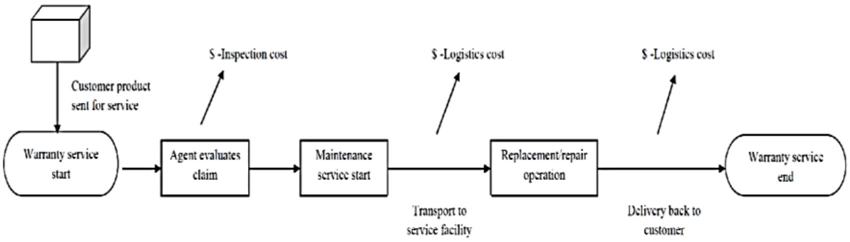


Figure 3: Warranty service operation for products

Consumers or customer service send claims to the SA after verifying warranty eligibility. When repair expenses exceed replacement prices, the product is replaced. They assume a random examination of a customer's service claim after entitlement, considering warning indications. The study assumes all claims, fraudulent or legitimate, pass through the RMA and entitlement systems without difficulties, focused on claim investigation. Table 3 lists parameters affecting embedded system customer claims and investigations. The example presupposes a valid claim and good faith from the consumer. With fraud, at least one component of the product requiring service may be non-warranty. This product would void the consumer-remanufacturer warranty. Inspection and logistics fees will increase service costs. The issue was simulated using two different situations.

Category	Subcategory	Assumption and justification
Factors that push the customer into committing fraud	Prior fraud history	It is also expected that a consumer would be biased towards or away from fraud based on their past interactions with the investigative process. For instance, there is a greater chance that a consumer would conduct fraud again if they manage to get away with it the first time. On the other hand, the likelihood of a consumer being discovered for fraud is also decreased.
	Confidence in the investigation process	Assuming the customer manages to evade detection in subsequent audits or secondary inspections, the probability of fraud grows with each successful heist.
Factors that affect claim processing	Prior criminal record	An investigator's decision to accept the allegations as accurate will be influenced by the customer's past record, which only includes detected fraud and not committed fraud.
	Warning flags	The examination of a claim may reveal red flags due to certain indications. (a high demand for claims within a certain time frame).
	Inspection error	Reasons abound for why inspection claims might be flawed. Unfortunately, inexperience or carelessness are the most common causes of human mistakes.
Factors that affect Sensor behavior	Claim data on record	Better records (including times, dates, and location data) provided by the sensor increase the likelihood that it will correctly ascertain the veracity of the claims presented.
	Sensor damage	Accidental or intentional sensor failure is always a possibility, and it's not always simple to tell which is which, especially when it comes to situations involving fraud.

III. PRINCIPLES AND AIMS OF RISK MANAGEMENT

Effective risk management requires companies to coordinate a wide range of hazards [12]. The traditional approach to risk management treats each risk independently. The three concepts of risk—partially unknown, changing over time, and changed by human actions—define it [13][14]. These aspects of risk motivate the development of particular approaches, models, and guidelines that compel managers to channel concentrated efforts into project risk management and organisational architecture in order to accomplish particular goals, such as:

Isolating risks that are economically, energetically, and temporally viable for investment;

Isolating and optimising risks;

- Reducing or eliminating harmful risks while enhancing those that are progressive;
- Developing alternative sets of action spaces;
- Reserving time and resources for unavoidable dangers;
- Ensuring that the organisational risk boundaries are not crossed.

The same principles in risk management have been defined and structured differently throughout time (e.g., Octave Allegro at Education Institution methodology [15]), which has been identified as a cause of ongoing uncertainty. Figure 4 below depicts a prominent risk management framework; most risk management textbooks also endorse this layout [16].

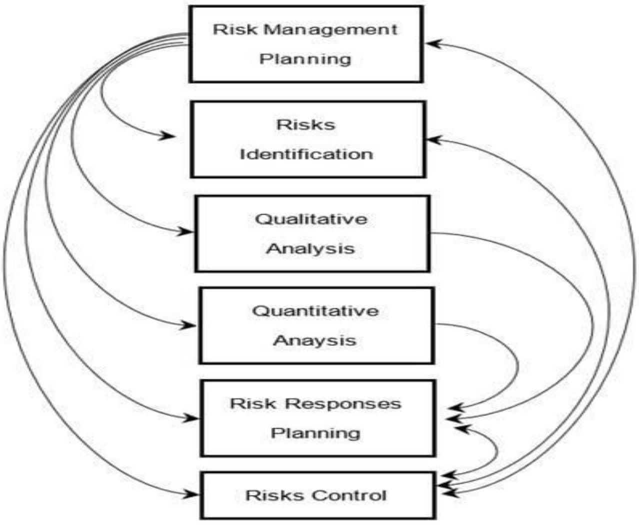


Figure 4: Main structures attributed to risk management [17]

A. Risk Management Planning

The primary goals and evaluation criteria for risk management are laid forth in the risk management strategy. Projects have detailed blueprints that explain their execution. Leading strategies should contain the risk management plan's status. Unlike other plans and initiatives, risk management plans lack a clear substance or structure to help managers organise frameworks and paperwork. Thus, businesses approach risk management plan content differently. Project overview, risk environment, application issues and problems, risk management strategy, process approaches, risk governance, etc. may be in a risk management plan.

B. Risk Identification

Every risk strategy must identify risks. An organised method for identifying real threats to project goals and activities. The assessment and management of risks, hazards, and opportunities require visibility. This is done by defining risk and vulnerability. Risk actors exploit system vulnerabilities. Lack of vulnerabilities prevents risk events. Susceptibility mostly depends on risk probability[18][19]. All important risk sources must estimate organisational dangers. Risk and system characterisation are linked to comprehending the circumstance. System data must be organised for associated managers. Details:

- Software development, implementation, and postimplementation;
- System interfaces (e.g., internal and external connectivity);
- Data and information within a system;
- People who support and use IT systems;
- System and data criticality (e.g., the value of the system or importance to an organisation);
- System and data sensitivity;

Humans with malicious intent, particularly when involved in fraudulent activities, might also constitute a risk source, in addition to the aforementioned possible risk sources.

C. Qualitative Analysis

In order to categories and ascertain the ultimate risk effect on the organization, it is necessary to examine the well-organized project risk documentation that is generated by the risk identification process. For classification and impact determination, information systems need data sensitivity and criticality. Qualitative or quantitative risk identification data analysis. During identification, qualitative analysis precedes quantitative [20]. There are several steps to risk qualification. Start with risk baseline. Qualitative analysis organizes project risks. Starting a risk among absolute uncertainty (zero and 100 likelihood) is the greatest technique to stratify its probabilities and ramifications. Absolute success and failure simplify the process and explain all options.

D. Quantitative Analysis

Assigning numeric values to project-related risks from qualitative data allows for further quantification. Risk quantification increases project success, evaluates "what-if" scenarios, and validates contingency reserves. Managers use numerous approaches to quantify risk quantitative analysis, including risk qualification and organisational statistics data:

Conducting quantitative risk assessments via interviews with technical specialists;

Calculating an innovative quantitative parameter from the predicted monetary value (the product of the likelihood and effect of risk);

- Decision trees that provide abundant information in an understandable way;
- The program evaluation: Implementing network systems with embedded multi-data-point duration estimations to provide schedule-specific risk levels;
- Tools for Simulating Risk, such as the Monte Carlo Method.

E. Planning Risk Response

Risk response development is crucial to risk management because it outlines how to address risks recognised, qualified, and quantified in prior processes. Risk thresholds and causes should be defined in this step. Risk thresholds can eliminate uncomfortable methods, saving time. Managers can also identify common hazards by defining the risk. It's evident that risk can mean threats or opportunities. Responses to both risk factors should be linked. The reaction strategies are in Figure 5.

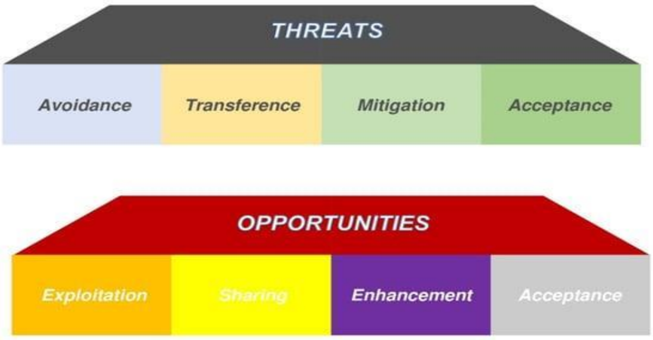


Figure 5: Aspects of risk

F. Risk Control

Risk management concludes with implementing identified, qualified, quantified, and specified responses. Implementing and validating risk plans are two main obstacles in this area. Integration of strategies and plans should make risk plans self-fulfilling. Ensuring plan validation requires thorough and sustainable risk and environmental tracking, which is mostly done through enquiries. Assist the process with well-organized and helpful documentation. This step uses earned value analysis and other approaches to assess risk monitoring's delicate needs [13].

IV. ADVANCE ALGORITHMS IN FRAUD DETECTION FOR WARRANTY PROCESSES

This section discusses advanced techniques to utilise Machine Learning and AI for fraud prevention in manufacturing warranty processes.

A. Machine Learning

Learning algorithms are studied in ML. Learning is the state in which experience helps a computer program judge by a performance criterion to perform better itself. The trained computer software is referred to as a model. ML models, therefore, are statistical methods and computational algorithms created to let computers learn and make judgements or predictions without having to be explicitly programmed. The concepts of pattern recognition and data-driven learning form the basis of these models. Figure 6 shows that there are four distinct kinds of ML. Classifying learning methods as either supervised or unsupervised, semi-supervised or reinforced. The following provides a concise explanation of various types:

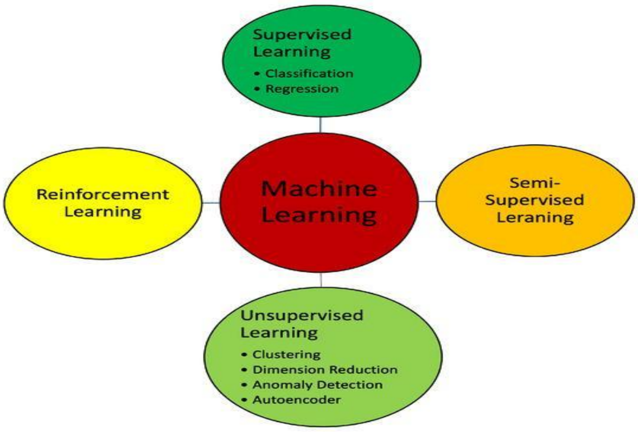


Figure 6: machine learning in fraud detection

1) Supervised Learning:

The model learns to classify or make predictions in supervised learning by being trained on data that has labels. In features-based classification and regression, the input data is coupled with the associated output labels.

2) Unsupervised Learning:

Unsupervised learning uses ML to understand data patterns, structures, and relationships without labelled examples. It discovers data patterns or clusters to enable grouping, dimensionality reduction, and anomaly detection. Unsupervised learning is suitable for examining and interpreting un-labelled data because it lacks target labels:

- Clustering: The algorithm uses similarities and patterns in the input data to group data points together. Machines with comparable performance characteristics might be grouped together in this way.
- Dimensionality Reduction: For this task, the algorithm's goal is to minimise the amount of input characteristics while keeping all the relevant data. It may be used as a first stage in the processing of other ML tasks, and it helps to see and comprehend high-dimensional data.
- Anomaly Detection (AD): This is where the computer discovers normal patterns in the data and marks as outliers or anomalies any data points that deviate significantly from those patterns. Among the many potential applications of this technique is the detection of wear in process equipment by use of anomalies in transmission signals.
- Autoencoder (AE): For dimensionality reduction and unsupervised learning, AE neural networks are particularly useful as they are able to both encode and decode input. Encoder networks compress the input data into a lower-dimensional representation known as latent space, from which decoder networks recreate the original data. In order to train the model to learn a condensed representation that emphasizes the important parts of the input data, it is necessary to minimize reconstruction errors using an AE [21].

3) Semi-supervised Learning:

The training method in this learning paradigm makes use of both labelled and unlabelled data. By combining a greater amount of unlabelled data with a smaller amount of labelled data, the model performs better. Labelling data may be a time-consuming and costly ordeal, but this serves its purpose well.

4) Reinforcement Learning:

In this kind of learning, an agent engages in interactions with its surroundings. In order for the agent to maximise a reward signal, it learns to manipulate its surroundings in a certain way. The agent learns to attain its long-term objectives by making optimum judgements in diverse environmental situations via a process of trial and error. Applications of reinforcement learning include visual navigation, robotics, and video games that need many steps to make a choice.

B. Artificial Intelligence Methods

This section examines AI methodologies that can be employed to mitigate fraud through a proactive approach to enhanced risk management.

- Identity: Identical items should have corresponding explanations, according to the identity principle. The amount of inherent nondeterminism in the procedure is estimated by doing this.
- Separability: Nonidentical objects cannot be explained similarly. Two samples that differ only in a non-essential attribute will predict the same. Even though the samples are different, the explanation approach might explain them. This proxy assumes that every attribute has a minimal positive or negative importance in predictions for simplicity.
- Stability: There must be comparable explanations for analogous things. This is predicated on the notion that an explanation technique ought to limit its output to comparable explanations for marginally dissimilar items.

- Selectivity: The forecast must be adversely impacted by the removal of relevant factors. In order to calculate selectivity, the characteristics are ranked from most to least significant. The remaining mistakes are then computed to get the AUC after each characteristic is removed one at a time, for example, by setting it to zero.
- Coherence: Computing the result is as simple as subtracting the old signal's prediction error from the new signal's prediction error after all the unnecessary features have been eliminated.
- Completeness: It takes each prediction mistake and divides it by the percentage of explanation error.
- Congruence: The congruence proxy is given by the standard deviation of the coherence. The fluctuation of the coherence may be better captured by this measure.
- Acumen: According to the authors' original proposal for this novel proxy is based on the premise that a characteristic that is considered critical by the XAI technique should actually become one of the least important features once it has been disturbed. Whether the XAI approach is feature-position dependent is what this proxy is trying to identify. A comparison of the ranking position of each essential characteristic after perturbation is used to calculate it.

C. AI to prevent fraud in manufacturing warranty processes

Table 4 summarises key areas for using AI to prevent fraud in manufacturing warranty processes, including fraud detection, risk assessment, and data management. It highlights tools like machine learning algorithms, predictive analytics, and automation to streamline operations. Important considerations include data integrity, employee engagement, regulatory compliance, and ethical practices, emphasising a comprehensive approach to enhancing warranty processes through AI.

Table 4: AI techniques for fraud prevention in manufacturing warranty processes

Key Areas	Description	Tools/Techniques	Considerations
Fraud Detection	Identifying and analysing suspicious warranty claims.	Machine Learning (ML) Algorithms	Data quality and integrity
		Anomaly Detection Techniques	Continuous monitoring and updating of models
		Natural Language Processing (NLP) for text analysis	Establishing thresholds for alerts
Risk Assessment	Evaluating the likelihood and impact of potential warranty fraud.	Risk Scoring Models	Developing comprehensive risk matrices
		Predictive Analytics	Regularly updating risk assessments based on new data.
		Simulation Techniques (e.g., Monte Carlo Simulation)	Stakeholder involvement in risk assessment
Data Management	Ensuring access to accurate and complete data for analysis.	Data Lakes for storage	Data governance frameworks
		ETL (Extract, Transform, Load) Tools	Compliance with data protection regulations
		Cloud-based Data Warehousing	Ensuring data accuracy and timeliness

Automation	Streamlining warranty claim processing to reduce human error.	Robotic Process Automation (RPA)	Balancing automation with Human Oversight
		Intelligent Document Processing (IDP)	Change management during automation implementation
		Workflow Automation Tools	Impact on employee roles and responsibilities
Monitoring and Reporting	Ongoing tracking of warranty claims and reporting of anomalies.	Business Intelligence (BI) Tools	Defining KPIs for performance monitoring
		Dashboards and Visual Analytics	Establishing reporting frequency and audience
		Real-time Data Analytics	Ensuring timely responses to detected issues
Collaboration and Training	Engaging employees and stakeholders in fraud prevention efforts.	Training Programs for Staff	Fostering a culture of accountability and transparency
		Cross-Department Collaboration Tools	Ensuring ongoing training and updates
		Knowledge Sharing Platforms	Measuring training effectiveness
Regulatory Compliance	Adhering to legal requirements in warranty processes.	Compliance Management Systems	Understanding regional regulations and standards
		Audit Trail Tools	Regular audits and reviews of compliance
		AI-Driven Compliance Monitoring	Staying updated with changing regulations
Feedback Mechanism	Gathering feedback to improve the warranty process.	Customer Feedback Tools	Analysing feedback for continuous improvement
		Surveys and Feedback Forms	Incorporating feedback into risk management strategies
		Sentiment Analysis	Timeliness of feedback collection

V. LITERATURE REVIEW

This section summarises the existing literature on utilising machine learning and artificial intelligence to mitigate manufacturing fraud in warranty operations to improve risk management. Table 5 depicts the summary of the various literature review as discussed below.

This study, Cantarelli et al. (2018) evaluates the main fraud-fighting methods and their pros and downsides. This describes how these methods could be changed to handle remanufacturing warranty fraud. Big data and new technology enable fraud detection[22].

This, Pandit and Gupta, (2021) article focuses only on the problem of customer-initiated warranty frauds involving remanufactured products, particularly those involving the remanufacturing of consumer electronics. This article discusses the options open to the remanufacturer for dealing with this kind of fraud. The potential utility of a sensor-embedded product in reducing component replacement fraud is investigated in a case study that employs a discrete event simulation model. This case study demonstrates how to detect and prevent fraud in advance[23].

The existing, Srinivasan et al. (2016) burden of dealing with complicated and costly procedures to identify warranty fraud falls on manufacturers due to the fact that these approaches deal with data that is erroneous and unclear. Due to the massive amount of data, they suggest a model to detect anomalies in warranty records by combining information on component failures with patterns extracted from past warranty claims that are pertinent to a certain location and component. The claim date, type of failure, and failure date were all effectively identified as indicators of a claim, including a high probability of fraud. They also found patterns of failure and connected data with claims processing, reporting, and business processes, all while keeping current systems as unchanged as possible[24].

This paper, Bhatia, (2022) to aid financial organizations in evaluating risk before to issuing credit cards by suggesting a new practical approach to customer segmentation based on estimated likelihood of payment default. To showcase our methodology and outcomes, we have harnessed the credit card default information from Taiwan. However, the method has been made more generic so it may be used with credit card default information from any country [25].

This paper, Attanayake and Ratnayake, (2022) proposed method allows asset managers and inspection and maintenance engineers to identify DTs that are eligible for comprehensive risk assessments. In order to demonstrate the proposed method, a power distribution network situated in a densely populated region is used to conduct a risk screening using 40 DT units. This study's methodology allows for improved electric power distribution system asset management by applying the same methodology to other critical components of such systems [26].

Study	Methodology	Performance	Limitation	Future work
[22]	Evaluation of main fraud-fighting methods and suggestions for adapting them to remanufacturing warranty fraud detection.	The study describes how fraud-fighting methods could be improved but lacks quantitative performance.	The study lacks a focus on specific technologies like AI or big data analytics for remanufacturing.	Integrate AI and big data analytics to improve fraud detection in remanufacturing processes.
[23]	Focus on remanufactured product warranty fraud in consumer electronics, using a sensor-embedded product to mitigate part substitution fraud.	The case study shows preemptive identification and mitigation of fraud, demonstrating effectiveness through discrete event simulation.	Limited to the consumer electronics sector; relies heavily on the case study example.	Extend strategies to other sectors and explore additional sensor-based methods for fraud mitigation.
[24]	Use of a model to detect abnormalities in warranty data, leveraging historical warranty claims and component failure patterns.	Successfully isolates fraudulent elements in warranty claims, integrating business rules while maintaining system continuity.	High complexity and expense due to the reliance on large volumes of data and inaccuracies in historical	Develop more cost-effective methods to handle large datasets and enhance accuracy in identifying fraudulent patterns.
[25]	Proposed a novel technique for segmenting customers by their predicted probability of defaulting on payments using a credit card default dataset (Taiwan).	Demonstrated effectiveness in assessing risk before issuing credit cards; generalised for application across other countries.	Performance limited to dataset used (Taiwan dataset); potential model overfitting to specific dataset characteristics.	Apply and test the proposed approach on credit card default datasets from other countries.

[26]	Suggested a risk screening method for 40 units of distribution transformers (DTs) in a power distribution network.	Enhances asset management in power distribution by identifying DTs for detailed risk analysis.	Focuses on a specific network type in a dense area; may not fully generalise to less dense or differently structured power networks.	Extend approach to other key components in power distribution systems for improved asset management.

VI. CONCLUSION AND FUTURE WORK

Though AI fraud detection is becoming more popular, its future must be considered. AI can identify fraud better due to machine learning and data mining. AI can detect suspicious behaviour, so companies must use it. AI can foresee risks. AI-powered fraud detection solutions can use predictive analytics to assess detected and undiscovered fraud. Thus, companies can reduce risk and prepare for attacks. Strange customer conversions can indicate suspect conduct or purpose with AI. Many companies will utilise AI in security networks to understand financial crime networks. AI aids companies against thieves. AI technology is effective, precise, and better than manual fraud detection, making its use commendable. The rise in warranty fraud not only threatens manufacturers' financial stability but also undermines consumer trust in warranty systems. By implementing advanced machine learning and artificial intelligence techniques, organisations can improve their fraud detection capabilities, thereby mitigating risks and fostering a more transparent warranty ecosystem. Moreover, integrating environmentally conscious manufacturing practices is crucial for addressing the broader implications of consumer electronics waste and resource depletion.

The goal of future research should be to improve these technologies and find more ways to use them in different production settings so that we can create a more sustainable future that is both economically and environmentally responsible. Preventing malevolent actors from leveraging AI requires security. Due to its cost-effectiveness and efficiency, AI may help companies reduce fraud risk. Soon, AI will be popular. AI and machine learning research should use deep reinforcement learning and federated learning to combat industrial warranty fraud. Continuous learning and decentralised data sources improve fraud detection methods. Blockchain and AI decrease warranty fraud with tamper-proof claims (EUDL). IoT devices recording product consumption in real-time could help manufacturers avoid fraud. Finally, explainable AI (XAI) should increase transparency and help human reviewers believe warranty fraud detection results. ML and AI can detect and prevent warranty fraud better than rules. Anomaly detection, deep learning, and automated machine learning reduce fraud and save manufacturers money. AI-driven solutions with human experience improve fraud detection and response to emerging fraud schemes. Innovation and collaboration between AI developers and manufacturers will reduce warranty fraud and simplify warranty management.

REFERENCES

1. M. A. Ilgin and S. M. Gupta, “Environmentally conscious manufacturing and product recovery (ECMPRO): A review of the state of the art,” Journal of Environmental Management. 2010. doi: 10.1016/j.jenvman.2009.09.037.

2. M. D. Hanna, W. Rocky Newman, and P. Johnson, "Linking operational and environmental improvement through employee involvement," Int. J. Oper. Prod. Manag., 2000, doi: 10.1108/01443570010304233.
3. P. Khare and S. Srivastava, "The Impact of AI on Product Management : A Systematic Review and Future Trends," vol. 9, no. 4, 2022.
4. S. K. R. Anumandla, V. K. Yarlagadda, S. C. R. Vennapusa, and K. R. V. Kothapalli, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation," Technol. \& Manag. Rev., vol. 5, no. 1, pp. 45–65, 2020.
5. P. Pathak, A. Shrivastava, and S. Gupta, "A survey on various security issues in delay tolerant networks," J Adv Shell Program., vol. 2, no. 2, pp. 12–18, 2015.
6. V. K. Yarlagadda and R. Pydipalli, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity," Eng. Int., vol. 6, no. 2, pp. 211–222, 2018.
7. V. K. Yarlagadda, S. S. Maddula, D. K. Sachani, K. Mullangi, S. K. R. Anumandla, and B. Patel, "Unlocking Business Insights with XBRL: Leveraging Digital Tools for Financial Transparency and Efficiency," Asian Account. Audit. Adv., vol. 11, no. 1, pp. 101–116, 2020.
8. A. Pandit and S. Gupta, "Warranty Fraud in a Remanufacturing Environment," in Responsible Manufacturing, 2019, pp. 241–262. doi: 10.1201/9781351239141-11.
9. J. Thomas, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," J. Emerg. Technol. Innov. Res., vol. 8, no. 9, 2021.
10. S. K. R. A. Sai Charan Reddy Vennapusa, Takudzwa Fadziso, Dipakkumar Kanubhai Sachani, Vamsi Krishna Yarlagadda, "Cryptocurrency-Based Loyalty Programs for Enhanced Customer Engagement," Technol. Manag. Rev., vol. 3, no. 1, pp. 46–62, 2018.
11. N. P. Murthy and N. Jack, "Game theoretic modelling of service agent warranty fraud," J. Oper. Res. Soc., 2017, doi: 10.1057/s41274-016-0125-z.
12. S. M. Samimi Amir, "Investigation of Risk Management in Food Industry," Int. J. Adv. Stud. Humanit. Soc. Sci., 2020.
13. T. Finne, "Information systems risk management: Key concepts and business processes," Comput. Secur., 2000, doi: 10.1016/S0167-4048(00)88612-5.
14. A. P. A. Singh, "STRATEGIC APPROACHES TO MATERIALS DATA COLLECTION AND INVENTORY MANAGEMENT," Int. J. Bus. Quant. Econ. Appl. Manag. Res., vol. 7, no. 5, 2022.
15. J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," in Procedia Computer Science, 2018. doi: 10.1016/j.procs.2018.08.167.
16. T. Aven, "Risk assessment and risk management: Review of recent advances on their foundation," European Journal of Operational Research. 2016. doi: 10.1016/j.ejor.2015.12.023.
17. S. Stackpole, "A User's Manual to the PMBOK Guide," 5th ed., 2013. [Online]. Available: https://download.e-bookshelf.de/download/0000/7530/96/L-G-0000753096-0003979205.pdf
18. Stoneburner, a. Goguen, and a. Feringa, "Risk Management Guide for Information Technology Systems," Natl. Inst. Stand. Technol. Spec. Publ. 800 -30, 2002.

19. K. V. V. and S. G. Jubin Thomas , Piyush Patidar, "An analysis of predictive maintenance strategies in supply chain management," Int. J. Sci. Res. Arch., vol. 06, no. 01, pp. 308–317, 2022, doi: DOI: https://doi.org/10.30574/ijsra.2022.6.1.0144.
20. S. A. Sherer and S. Alter, "Information Systems Risks and Risk Factors: Are They Mostly About Information Systems?," Commun. Assoc. Inf. Syst., 2004, doi: 10.17705/1cais.01402.
21. M. Maggipinto, A. Beghi, and G. A. Susto, "A Deep Convolutional Autoencoder-Based Approach for Anomaly Detection with Industrial, Non-Images, 2-Dimensional Data: A Semiconductor Manufacturing Case Study," IEEE Trans. Autom. Sci. Eng., 2022, doi: 10.1109/TASE.2022.3141186.
22. C. Cantarelli, B. Flybjerg, E. J. E. Molin, and B. van Wee, "Cost Overruns in Large-Scale Transport Infrastructure Projects," Autom. Constr., 2018.
23. A. Pandit and S. Gupta, "Tackling Substitution Fraud in Remanufactured Product Warranty Service," Int. J. Latest Eng. Res. Appl., vol. 6, no. 2, pp. 9–18, 2021.
24. R. Srinivasan, S. Manivannan, N. Ethiraj, s Devi, and S. Kiran, "Modelling an Optimized Warranty Analysis methodology for fleet industry using data mining clustering methodologies with Fraud detection mechanism using pattern recognition on hybrid analytic approach," Procedia Comput. Sci., vol. 87, pp. 322–327, Dec. 2016, doi: 10.1016/j.procs.2016.06.001.
25. S. Bhatia, "Pragmatic segmentation-based credit risk management using Machine Learning," in 2022 International Conference on Communication, Computing and Internet of Things, IC3IoT 2022 - Proceedings, 2022. doi: 10.1109/IC3IOT53935.2022.9768006.
26. A. M. S. R. H. Attanayake and R. M. C. Ratnayake, "On the Necessity of Using Supervised Machine Learning for Risk-based Screening of Distribution Transformers: An Industrial Case Study," in IEEE International Conference on Industrial Engineering and Engineering Management, 2022. doi: 10.1109/IEEM55944.2022.9989698.