Work Project, presented as part of the requirements for the Award of a Master's degree in Management from the Nova School of Business and Economics.

TITLE OF WORK PROJECT

MANAGING RISKS IN SUPPLY CHAIN: CHALLENGES, IMPACTS, AND MITIGATION STRATEGIES WHEN INTEGRATING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

ROSARIA BISCEGLIA 60480

Work project carried out under the supervision of:

Paulo Faroleiro

06/01/2025

ABSTRACT

This research explores the development of artificial intelligence (AI) and machine learning (ML) in supply chain management (SCM), taking into consideration their transformational potential and inherent risks. By analyzing data from surveys and interviews conducted with managers of various sectors, the research identifies three critical risks: data quality, cyber security and transparency. The findings provide the need for strong data governance, proactive cybersecurity measures and the adoption of AI frameworks that can be explained to improve confidence and efficiency. Recommendations include sector-specific risk management strategies, inter-departmental collaboration and ethical guidelines. This research provides insights to optimize AI and ML adoption in SCM, mitigating associated risks.

Keywords: AI risks; Supply chain management; Machine learning transparency; Data governance; Cybersecurity in SCM.

Acknowledgement

A deep thanks to my supervisor, Paulo Faroleiro, for his constant support and valuable advice that has guided every step of this work. Your support has been an invaluable source of inspiration and motivation.

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

1. Introduction **3**
2. Literature Review **4**
2.1 Explaination of Supply Chain 4
2.2 Major Risks in Supply Chain 6
2.3 Risks related to AI and ML in the SCM 7
3. Problem Statement **9**
3.1 Identification of Risks in AI and ML adoption 9
3.2 Research Gaps 9
4. Research Questions **10**
5. Research Methodology **11**
5.1 Research design 11
5.2 Data Collection Methods 11
5.2.1 Survey Methodology 11
5.2.2 Interview Process 12
5.3 Data Analysis Techniques 12
6. Surveys results **12**
6.1 Analysis of Survey Data 13
6.2 Key findings from quantitative analysis and survey limitations 15
7. Proposal **16**
7.1 AI and ML risk mitigation strategies 16
8. Interview results **17**
8.1 Qualitative Analysis of Interview Data 17
8.2 Mitigation Strategies and Synthesis of Interview Analysis 18
9. Comparison of Results: Survey and Interviews **19**
9.1 Summary of Findings 19
9.2 Implications for Theory and Practice 20
9.3 Preliminary Conclusions on Findings 22
10. Discussion **22**
10.1 Limitations and considerations 23
10.2 Directions for future research 23
10.3 Conclusions 24
11. References **26**
12. Appendices **29**

1. Introduction

The accelereted development of machine learning (ML) and artificial intelligence (AI) in latest years has profoundly transformed supply chain management (SCM) (M. 2011). These innovations are changing the way businesses oversee global supply networks and are becoming essential components of the larger digital transformation movement. AI and ML provide advanced strategies for solving historical problems in supply chain management, such as forecasting consumer demand, optimized inventory management, and timely response to disruptions along the supply chain. Supply chains are traditionally complex networks that require accurate coordination of information, resources and processes to move goods from suppliers to consumers (Ghadge, A. & Dani, S. 2012). These systems are based on efficient logistics, cooperation among multiple actors, inventory control and accurate demand forecasting. AI and ML represent disruptive technologies with unique potential to revolutionize these processes, addressing the growing need to improve efficiency, reduce costs and manage increasingly complex global networks (N.Faisal 2009). Supply chain management (SCM) is currently one of the most widely adopted fields of AI and ML, due to their ability to improve every aspect of operations. These technologies allow for more accurate demand forecasting, real-time monitoring of supply chain conditions and faster reaction to market changes. In a highly competitive and constantly changing scenario, AI and ML provide organizations with greater agility and data-driven decision making. In addition, faced with variables such as geopolitical conflicts, climate threats and the continuing digitalisation of businesses, global supply chains are becoming increasingly interconnected and unpredictable, making flexibility a key requirement (W. Blackburn 2007). Machine learning algorithms are developed on the use of large amounts of data and enable companies to accurately estimate demand, monitor the status of operations and respond quickly to market changes. However, despite its many advantages, integrating AI and ML into supply chain management involves several problems

and risks that companies must carefully address (P. Ahi 2014). Challenges include the spread of confidential information, increasing cyber security threats and poor data quality and failures due to bad algorithms. For smaller or less technologically advanced enterprises, the implementation of advanced technologies in existing systems and the high implementation costs may in some cases outweigh the expected benefits (Shukla, Rajendra Kumar, Dixit Garg 2011). In addition, the opaque nature of machine learning models, frequently cited as "black-box" systems, raises concerns about accountability, control and transparency in decision making. It becomes important to know and mitigate these risks to ensure that the capacity advantages of AI and ML integration are completely realized, without compromising the operational stability of companies. This document objectives to offer a consolidated overview of primary threats related to using AI and ML in supply chain management (Burstein, G., & Zuckerman, I. 2023) key issues such as cyber security and privacy threats, the contrast with human decision making and the costs and complexity of technology implementation will be analysed. Finally, practical strategies to mitigate these risks will be presented, with a critical analysis of available academic research and case studies to support companies in successfully addressing the challenges of supply chain digitization (P. Ahi, C. Searcy 2014).

2. Literature Review

2.1 Explaination of Supply Chain

The name “Supply Chain Management” refers to back to the manage of control and float of data, capital and assets for the production and distribution of the final product to the consumer (Shukla, R. K., Garg, D., & Agarwal, A. 2011). First defined by Oliver and Webber in 1982, SCM represents a strategic approach to coordinating complex actions: from raw materials procurement to delivery to the end customer, it begins to cover the entire logistics path of production, ensuring cost and time reductions (Colicchia C., Fernand Strozzi 2012). The main

goal of SCM is to offer maximum value to the customer under the conditions of maximum resource savings and reduced production costs. Due to globalization and technological advances, SCM has become a strategic function. Some examples of end-to-end activities found in today's supply chain governance are planning and pre-creation of raw materials, production, management, and repackaging of products with higher taste (Heckmann, Iris, Tina Comes 2014). Contemporary supply chains have many more linkages that include manufacturers, distributors, sellers, buyers, and many others. The interdependence among these actors means that problems in a given link in the scheme can cause significant disruptions, higher costs and customer dissatisfaction (Tiwari, S., H. M., & Daryanto, Y. 2020). In addition, digital progress has required efficient administration of information and financial flows to make the choices themselves fast and informed (Cucchiella Federica, Massimo Gastaldi 2006). Some examples of excellence in SCM are Walmart and Dell. Walmart has spent a lot of money on perfecting the transportation and technology aspect to improve the equilibrium between supply and demand by accelerating the decrease of inventory management costs (Gurtu, Amulya and Jestin Johny 2021). Dell, with its consumer distribution plan, has completely changed the supply chain concept through “offering customization and containing operating costs.” However, global expansion has presented new problems: supply chains cross continents and climb mountains and face logistical, cultural, regulatory and linguistic solutions. In addition, risky geopolitical conditions and unforeseen events such as epidemics or natural emergencies can cripple business (J. 2021). In this contensto, risk management is an investigative tool to identify, analyze and control possible barriers to support optimization of supply chain operations and business continuity (Vincent, A., Tang, L., & Zailani, S. 2021). In essence, well-developed SCMs not only earn the corporate world a better position in the market, but also make consumption more useful, precisely by freeing it from excess and inefficiency and bringing it closer to the consumer (W. R. Blackburn 2007).

2.2 Major Risks in Supply Chain

The strategic function of supply chain management can be threatened by risks that, if not well managed, can damage the organization's performance, future prospects, and reputation with customers. These risks are compounded by the growing interconnectedness of supply chains involving many suppliers, distributors, and logistics companies. In supply chain management (SCM), global risks may be categorized into inner and external (Lim M. K., Qu Y. Ni. & Xiao Z. 2023). Risks in SCM pose challenges to all stages involved in the process. Internal risks include problems such as poor productivity, equipment breakdown, or mistakes made by people within the institution. These can cause time delays, incorrect inventory and control flows, and financial cost escalation, especially within highly integrated systems such as the just-in-time manufacturing system (Ghadge A., Dani S., & Kalawsky R. 2012). On the other hand, external risks occur outside the reach of the organization and can include economic fluctuations, technological changes that affect the smooth functioning of the supply chain (Bailey, Tucker, Edward Barriball, Arnav Dey 2019). An additional classification is possible with reference to operational, supply, demand, network and environmental risks, each of which differs in some ways. Operational risks include disruptions in business processes such as inefficient quality control or dependence on outdated systems, which can amplify SCM vulnerabilities (H. Hoffman, C. Busse, C. Bode, M. Henke 2014). Supply risks are a consequence of dependencies arising from features such as product design, materials, and sourcing strategies. They include supplier failures, limited supply base, or any event that affects the availability of raw materials. An example is semiconductors, which have disrupted the automotive and electronics industries (A. Borghesi, B. Guedenzi 2011). There are also demand risks, generated by the unpredictability of consumer behavior. These risks have become even more evident in volatile environments introduced by e-commerce, as consumer behaviors change faster, increasing the demand volatilities to be addressed in inventory and demand

forecasting (Tang 2006). Network risks arise from various disturbances that affect the entire supply chain environment such as labor disruptions or over-reliance on third-party logistics services. These risks are usually interconnected in such a way that failures in a particular aspect can cause strains throughout the supply chain (Mihalis G., Thanos P. 2015). Similarly, environmental threats such as epidemics, trade tensions and political instability, and external natural threats create supply chain disruptions on a global scale. The ultimate implications of unmitigated risks in the supply chain are costly. Specifically, it has been revealed that, with reference to large reported shocks, market value losses ranging from 5 to 10 percent can occur for companies in a matter of days (Christopher, Logistics & Supply Chain Management 2011). Managing these risks requires a preventive as well as an innovative strategy. A continuous flow of data analysis can be helpful for increased detection and faster recovery from disruptions, and effective cooperation among supply chain partners ensures better understanding of processes. In addition, funds must be available for contingency plans and risk modeling systems that companies must apply to anticipate possible disruptions. Risk management is about protecting processes within the supply chain and making them more competitive by promoting continuity, cost control and customer satisfaction. This has proved to be a complex process for managing these various risks, becoming an essential factor in supply chain management (Baryannis, G., Dani, S., & Antoniou, G. 2019).

2.3 Risks related to AI and ML in the SCM

In recent times, supply chain management has been transformed by AI and ML, improving critical processes such as logistics optimization, inventory control, and demand planning. These technologies are significant because they enable large volumes of structured and unstructured data to be analyzed, offering detailed real-time explanations to increase operational resilience, reduce costs, and increase productivity (Helo P., Hao Y. 2021). For

example, historical data analysis can be used by machine learning algorithms to predict future demand and external sources, such as weather patterns or world events, can also be analayzed to identify potential disruptions. Despite the advantages, the use of AI and ML is fraught with difficulties. Data availability and quality are crucial challenges, as many systems use incomplete or fragmented data from older systems and from various geographic areas, which reduces the reliability of analysis (V. 2023). In addition, another danger is transparency: AI models, often considered "black boxes," do not explain how decisions are made, undermining stakeholder trust and making it more difficult to adhere to rules and accountability requirements (Abbass K., Afaq M. 2020). Moral implications are equally important. Smaller providers or less developed regions could be penalized by algorithms designed to improve economic efficiency, thereby increasing inequality in the global economy. Data security is also a critical danger: when different supply chain participants share confidential information, the risk of cyber attacks and privacy breaches increases, which could damage the finances and reputations of participating organizations (Akhtar 2022). A further difficulty concerns the integration of AI technology into existing systems: many organizations continue to use old infrastructures that is often incompatible with state-of-the-art AI solutions, necessitating large investments in maintenance, employee training, and technology. In addition, inefficiencies and lower than expected return on investment can result from a lack of alignment between AI-driven analytics and business decision-making procedures (F. 2023). Ultimately, supply chain management can be improved in special ways by AI and ML, increasing its competitiveness and resilience. However, companies must manage the risks associated with data, ethics, transparency, security, and technology integration to fully reap the benefits. To ensure successful and responsible implementation, a well-balanced approach that integrates both automation and human control is needed.

3. Problem Statement

3.1 Identification of Risks in AI and ML adoption

The supply chain is dominated by the use of AI and ML, as they have the ability to improve speed and accuracy of processes. However, as they are adopted, risks emerge that, while initially having a moderate impact, can become significant and compromise the effectiveness of implementations. These are, for example, the obscurity of decisions made by AI damaging trust in organizations; or data quality issues that can increase inefficiencies and operational costs (Chen P. Y. & Wang F. K. 2020). In fact, we note that the more degraded the data, the worse the demand forecasts and subsequent inventory management, leading to poor decisions that negatively affect performance indicators such as inventory turnover and customer satisfaction. Other challenges include cybersecurity threats: as technology integration advances with the use of artificial intelligence, the likelihood of cyber attacks, data loss, and compromised operations increases (A. A. 2023). These risks can be managed more effectively by effective data governance, such as through regular data audits and the use of techniques that help reduce possible bias. The purpose of this research is to propose a coherent set of approaches to help integrate the identified risks into the strategies to be adopted. Thus, by connecting disconnected dots in current research and proposing tangible recommendations, it aims to guarantee that AI and ML are safely incorporated into the SCM and efficiently (Emrouznejad A., Abbassi M., & Sicakyüz S. 2023).

3.2 Research Gaps

The literature on in-depth risk mitigation techniques for AI and ML in supply chain management still has many gaps, despite a growing awareness of these issues. Although some studies recognize the danger, few provide specific frameworks or best practices to reduce the dangers (Zamani M., & Bhamra T. 2022). It becomes increasingly important to create efficient

risk management strategies as supply chain operations include AI and ML technologies. These tools seem to be still in the early stages of adoption, which means that many companies do not have the resources necessary to face and recognize the risks that could arise. So, the study focuses on bridging these gaps by analysing the point of view of some managers in the sector who use this new "method". It will present useful information that can help companies improve risk management procedures and make the most of AI and ML technologies without compromising safety, transparency or operational efficiency (Górski, M., Nowicki, T., & Ustun, T. S. 2020). It does so by focusing on information from surveys and interviews with supply chain professionals.

4. Research Questions

Through literature review, survey, and interviews, research questions are answered using the methodology analyzed in this section. This study is based on several well-defined research questions, aimed at deepening the functions of AI and ML in SCM. The topics were designed to highlight key issues related to the integration of these technologies, addressing temporary challenges and future trends.

RQ1: What are the key data quality, transparency and cybersecurity risks in integrating AI and ML in the supply chain management, and to what extent do those risks affect critical performance indicators?

RQ2: How far do supply chain managers and stakeholders trust the decision-making processes led by AI and ML considering transparency and ethical considerations, such as algorithmic bias and decision opacity?

RQ3: What risk management techniques can companies adopt to address the risks associated with integrating ML and AI in the supply chain?

Hypothesis

To support that questions, three hypotheses have been proposed: **H1:** Poor data quality, low levels of transparency and the main ethical issue of algorithmic bias generate poor inventory turnover, low delivery performance and customer dissatisfaction, compromising the benefits of AI and ML. **H2:** Decision-making based on AI and ML should be transparent, as opaque decision-making reduces stakeholder trust and cooperation. These practices are inefficient. **H3:** Sound data audit policies and procedures and bias reduction are likely to minimize risks. These practices improve demand signals, and strengthen confidence in the use of AI and ML models. This study should offer practical approaches to safely and effectively use ML and AI in supply chain by answering these research questions and supporting the hypotheses presented in it.

5. Research Methodology

5.1 Research design

To provide an accurate analysis of supply chain risks in ML and AI, this research is structured by comining quantitative and qualitative research approaches. Through the survey, we will collect general trends in risk perception from a large sample of field managers; in addition, interviews were conducted to analyse practical cases of this study. These two methods allor us to draw general conclusions. This will give us a more complete view of the challenges associated with AI adoption in the supply chain.

5.2 Data Collection Methods

5.2.1 Survey Methodology

Supply chain managers receive a structured online questionnaire. The survey aims to identify how organizations and their stakeholders perceive AI and ML risks in the supply chain. In addition, through the Likert scale, which evaluates elements from "strongly disagree" to

"strongly agree", one can observe a comprehensible evaluation of the attitudes and perceptions of risk of respondents. The survey is intended to be distributed through industry-specific platforms, sent via e-mail and professional networks. This technique allows for effective data collection from a large sample of supply chain experts geographically distributed.

5.2.2 Interview Process

For the qualitative component, a team of supply chain experts with direct knowledge of AI/ML implementation in their companies was selected. The interview method aims to complement the survey by providing more detailed insights into the unique risks, challenges and strategies that companies face in using AI/ML technologies in their operations. With the consent of participants, interviews are conducted via videoconference and recorded for transcription and further analysis.

5.3 Data Analysis Techniques

Descriptive statistics techniques will be used to examine survey data and to provide an overview of the most frequently identified risks and their relative importance. The methods used will include average scores and frequency distributions. This will help identify the elements that significantly affect risk perception and determine whether certain business models are more vulnerable to specific threats. As regards the analysis of interview data, an effective technique will be used to identify, examine and summarize relevant issues in the responses obtained. To understand how AI/ML risks are perceived and managed in real-world scenarios, the issues raised by this method will be compared to the survey results.

6. Surveys results

In this section, I will analyze the responses to surveys and research results, describing solutions to mitigate the main risks related to AI and ML.

6.1 Analysis of Survey Data

Demographic composition of respondents: The survey was completed by 83 professionals, 49.4% of which came from the supply chain, 15.7% from IT and 10.8% from data analysts. An increased number of respondents, 43.4%, have used AI/ML for 3-5 years, while 37.3% have used it for 1-2 years. One third (33.3%) of the respondents had experience levels of more than two years but less than five, while only 9.6% had experience levels of more than five years; 10.8% had less than one year, the participants had a wide range of experience. The distribution of roles among survey participants is illustrated in *Figure 5*. *Main risks identified:* When asked to assess the risks of integrating AI/ML into supply chains, as illustrated in *Figure 4* data quality was considered the highest risk, with 72.3% of participants perceiving it as such. It has been found that low-quality data collection contributes to higher levels of forecasting errors, inventory control problems and complications in demand analysis, as mentioned by Zamani and Bhamra (2022). Another critical area is cyber security, with 56.6% of respondents considering it highly important, while 34.9% attributed moderate importance to safeguarding AI/ML systems from breaches and cyber attacks. Another important element that emerged was *the lack of transparency*, which 79.5% of participants identified as a problem because IA's decision-making process is not transparent. When asked to what extent the lack of transparency affected collaboration, almost 47% said that the influence was moderate, while 44.6% said it had a considerable effect, as deteiled in *Figure 8*. In addition, only 59% of respondents noted improvements in working on ethical issues related to the adoption of AI/ML innovations. *The effect of risks on the functionality and success of supply chain:* The study also highlighted significant effects that identified risks have had on supply chain performance. For example, up

to 68.7% of participants observed increased costs using AI and ML solutions, particularly for cybersecurity issues or AI/ML integration efforts (Kshetri 2018). We see how 42.2% of respondents noted delays in decision-making processes, suggesting that slow or ambiguous AI-driven decisions could reduce supply chain flexibility. In addition, just under half, 42.2%, pointed to the problem of reduced efficiency due to poor data quality and lack of transparency. Although only 8.4% of participants reported a loss of trust from partners or customers, it remains one of the current problems and highlights the need to preserve stakeholder confidence. *Trust and transparency in AI/ML decisions:* The most common problem identified by companies was that AI/ML systems were not transparent, with 79.5% of respondents agreeing with this statement. In terms of impact level, the following was found: 40.5% of participants thought that transparency problems had a moderate effect on collaboration, while 47% said that transparency issues had a considerable influence on both internal dynamics and external engagements. The outcomes of this study demonstrate: it is essential to develop models of AI that can be explained in order to build trust with stakeholders and promote cooperation (Islam S., Amin S. H., Wardley L.J. 2021). Risk management strategies: To address these challenges, companies have adopted the following risk management strategies. 53.8% of companies have promoted clearer decision-making and communicated them to overcome the potential disadvantages of transparency by increasing confidence in the results produced by AI. The self-reported solution to data quality problems was data governance rules, and 39.8% of respondents mentioned them. It was also noted that 59% of organizations using AI/ML have established ethical guidelines to prevent inappropriate or unfavorable applications and results of the technology. However, regarding the role of AI/ML system upgrades, only 7.2% of respondents mentioned that their companies frequently audit these systems, suggesting the need to improve focus on proactive optimization of these innovations.

The main obstacles to integrating AI and ML into the supply chain, including data quality and transparency, are analysed and displayed in *Figure 1*.

6.2 Key findings from quantitative analysis and survey limitations

The results of the survey show how the previously discussed assumptions about the advantages and challenges inherent in AI and ML solutions can be confirmed. In support of Hypothesis H1, data quality has emerged as the most pressing concern; indeed, we see how this leads to inefficiencies in demand forecasting, inventory planning, customer relationships and chain distribution. These findings clearly indicate the importance of implementing robust data management systems to support quality and, more generally, AI/ML capability (Wu 2009). With reference to Hypothesis H3, 56.6% of respondents said that cyber security risks were extremely critical, reflecting the fact that data managed by AI systems is often sensitive. The problems related to cyber security vulnerabilities are supported by data in *Figure 6*, which illustrates the mitigation strategies companies have adopted to address these issues. However, less than one-third of participants, 34.9%, reported incorporating cybersecurity solutions, including constant system surveillance, demonstrating insufficient protection if vulnerabilities are identified. A total of 79.5% of respondents selected transparency as one of their main concerns, thus supporting Hypothesis H2, which indicates that lack of transparency leads to reduced confidence in artificial intelligence systems. However, the responses indicated that only 41% of respondents use explainability techniques to improve confidence in AI systems; however, 59% are trying to implement explainable AI models to increase confidence. The conclusions on the effect of IA on stakeholder confidence are shown in *Figure 7*, which highlights ongoing efforts to improve transparency of the model. These results therefore suggest the need to continue investing in AI-enabled systems to improve efficiency in the long term. Conclusions are also limited by sampling supply chain experts from sectors and areas of

the world, which limits the generalization of results to the global supply chain environment. These may be region-specific results, depending on state laws and the general economic climate (Thakur M., Patel P., Grupta L., Kumar M. 2023). In addition, the emphasis on sectors with a higher level of IA use has masked specific problems where IA use is lower. Therefore, future research could be useful if it included participants with a broader perception of the degree of integration of AI in the global supply chain. All this is synthesized in *Figure 3*, showing the dual impact on supply chain operations.

7. Proposal

This section provides solutions to address four main issues regarding the implementation of AI and ML in SCM, including cybersecurity, data quality, and transparency.

7.1 AI and ML risk mitigation strategies

The survey analysis identified three main risks: data quality, cyber security and transparency in AI systems. These risks can be mitigated through targeted interventions that improve organizational performance and also reduce negative impacts. First, data quality emerged as the most dominant risk among respondents, at 72.3%. This is critical for functions such as demand forecasting and inventory control (Ifesinachi, A. D., Sodiya, E. O., Jacks B. S. 2024). Effective solutions can be: installation of automated data control systems, frequent audits and training for employees to solve data problems appropriately. In addition, cyber security, which is named by 56.6% of participants, requires enhanced protective measures such as identity checks and regular vulnerability tests. Finally, 77.6% of respondents indicated that they are concerned about transparency in IA systems; human supervision can be used to improve this risk, ensuring accountability and compliance (Aljohani 2023). So, in conclusion, through a combination of technological and organizational approaches, these risks can be mitigated,

allowing companies to use the full potential of AI and ML. The mitigation strategies adopted by companies to address identified risks are illustrated in Figure 6.

8. Interview results

This part will be devoted to the analysis of information obtained through interviews with supply chain managers from the electronics, energy, medical and automotive sectors. The objective is to understand how these companies are dealing with the risks associated with the use of AI and ML, including examining practical solutions put in place to reduce them.

8.1 Qualitative Analysis of Interview Data

The survey involved four managers who have used AI and ML in supply chain management for three years or more. These are companies from the healthcare, energy, electronics and automotive sectors, responsible for running centres that involve the use of AI/ML to improve processes (Secchi R., Cannas V.G., Ciano M., Saltamalacchia M. 2022). The research conducted with supply chain managers offered meaningful highligh on the advantages, opportunities and difficulties like implementing ML and artificial intelligent, consistent with both the survey and examples of their use. Benefits of AI/ML: Managers have highlighted the improvement in demand forecasting capabilities, demonstrating that AI improves supply forecasting by reducing excess inventories. For example, one of them showed how AI can help a health manager to predict a shortage of vital medical supplies, another said it could help a manager in the automotive industry to be more responsive to changes in consumer preferences. *Table 1* provides a sector-wise overview of the significant consequences of AI and ML on efficiency and cost reduction, reinforcing these insights. In addition, improved operational agility was observed by reducing the time spent on technical interruptions and making faster decisions, as commented by participants, noting that all benefits depend on data quality. Risks and challenges: The three key risks identified during the survey - data quality, cyber security

and transparency - have been confirmed. Data disparity was cited as a significant problem that led to disruptions in operations, addressed through audits and training. *Table 2* illustrates how data quality is perceived as the highest risk among survey respondents, in line with challenges identified in the interviews. Security issues have been identified as critical; currently, managers have drawn attention to multi-factor authentication, risk assessment and contingency planning. These strategies are further supported by Figure 6, which highlights the adoption of advanced IT security measures among companies. Accountability in decision-making remains a crucial problem with the use of IA, as opaque responsibilities are less reliable (Modgil S., Gunasekaran A., Pournader M., & Seuring S. 2021). The SHAP and LIME tools have been described as essential to enhance safety and accountability in AI systems among stakeholders. *Figure 7* illustrates the role of AI in improving stakeholder confidence, a theme shared by interview participants. These findings support the strategies proposed in the thesis, underlining the need for effective data management, advanced cybersecurity and the implementation of Explainable AI models to address key hurdles and optimize the implementation of technologies of ML and AI in supply chain operations.

8.2 Mitigation Strategies and Synthesis of Interview Analysis

From the interviews we can highlight how the four managers highlighted concrete strategies to mitigate the famous risks connected to the implementation of AI and ML. These contributions highlighted specific approaches, highlighting both common challenges and sectoral peculiarities. As one manager from the electronics industry commented on data flow monitoring: "Data governance is certainly a topical issue among managers; for example, many have emphasized real-time archiving dashboards and audits to improve data credibility and organizational performance". As regards the energy sector, the manager stressed the concerns for cyber security, stating that they have taken measures such as encryption practices, the use

of multi-factor authentication and measures for better management of security incidents. In addition, an automotive manager uses these tools to rationalise supplier decisions, thus instilling trust among stakeholders. *Table 3* provides recommendations for future strategies across sectors, including advancements in data governance tools. Survey and interview results show that risks are interrelated and highlight differences in the sector. However, specific problems were observed in the sectors: the automotive industry faced difficulties with the implementation of legacy systems and did not perceive the benefits of the technology, The healthcare industry has been demanding accurate information for life-critical jobs (Z. 2023). These subtle differences demonstrate the effectiveness of the proposed strategies, with a focus on perpetual audits, improved cybersecurity and use of Explainable AI to integrate AI/ML. In conclusion, the results of the survey and interviews provide evidence that solutions need to be flexible, sector-oriented and based on sound governance principles (E. 2024). These results highlight the need for appropriate frameworks to incorporate in an optimistic way. These findings highlight the need for appropriate frameworks to optimistically incorporate AI and ML models into supply chain management, addressing common and specific problems.

9. Comparison of Results: Survey and Interviews

This section analyses the first conclusions emerging from the results of the survey

9.1 Summary of Findings

There are three significant risks in integrating AI and ML into supply chain management: data quality, cybersecurity, and transparency of AI-driven decision making. These risks highlight the neccesity for frameworks that address data inconsistencies, protect sensitive infrastructures and promote explainable AI for sustained confidence and efficiency, as supported by Yang et al. (2023). The predictive capacity of algorithms is compromised by inaccurate or insufficient

data, which causes operational inefficiencies, Difficulties in managing inventory and inaccurate demand forecasts-problems that most survey respondents rated as critical. With a significant percentage of respondents highlighting the dangers in AI-based infrastructures, cybersecurity emerged as one of the main concerns. Next to the danger of sensitive data, the possibility of data breaches or system disruptions caused by cyber attacks also increases the risk of operational upheaval (A. Ghadge, S. Dani, R. Kalawsky 2012). The opacity of AI's "black box" algorithms, on the other hand, has been widely criticised as undermining stakeholder confidence and making cooperation difficult, especially in complex supply chain ecosystems. These conclusions were supported by in-depth information from qualitative interviews with supply chain leaders in sectors such as healthcare, electronics and automotive. The operational disruptions caused by inconsistent data were often highlighted by participants, highlighting the need for strict control and real-time monitoring to preserve the integrity of the data. In addition, the increasing complexity of cyber threats was highlighted and multi-layered security solutions such as regular vulnerability tests and multifactor authentication were promoted. Finally, the importance of using explainable AI (XAI) technologies such as SHAP and LIME to increase stakeholder confidence and transparency in decision making was highlighted (R. 2023). Taken together, these findings provide a comprehensive picture: although AI and ML have the potential to revolutionize supply chain agility and efficiency, there are serious risks associated with these technologies. Strategic and sector-specific solutions that give high priority to proactive cybersecurity, strong data governance and the integration of transparent AI technologies are needed to address these issues. These findings not only support the tactics suggested, but also highlight how crucial it is to control risks in AI-driven supply chains in a systematic and flexible way.

9.2 Implications for Theory and Practice

The results of this paper highlights significant theoretical and practical contributions to aim at facilitating the integration of the two most tools (ML and AI) in the supply chain. The work fills significant theoretical gaps in knowledge about the dangers of adopting AI and ML, particularly regarding data quality, cyber security and transparency. The study enhances our understanding of the challenges of using AI to optimize supply chains by providing a multidimensional framework that combines organizational, ethical and technological perspectives (Christopher, Logistics & Supply Chain Management 2011). These results are deepened by qualitative interviews, which show how risks differ in different companies and underline the importance of adapting mitigation tactics to specific situations. In practice, the report offers supply chain professionals precise and useful advice. To ensure data integrity and the proper functioning of operations, strong data governance principles such as regular audits and mechanised tools for real-time monitoring of data must be adopted. Two examples of advanced security are multi-factor authentication and incident response procedures, which are critical to protecting sensitive data and technology infrastructure from increasingly complex attacks. Therefore, the use of explainable artificial intelligence technologies is proposed to solve transparency challenges and promote trust among stakeholder (Naz, A., Nazir, T., & Afzal, S. 2021). Using these technologies, companies can improve accountability and cooperation by providing clarity and justification for AI-based decisions. This study not only advances academic conversation, but also provides companies with useful tactics to address the challenges of AI adoption by combining these theoretical insights with practical tips. The findings highlight the need for a well-balanced strategy that exploits the innovative potential of IA while ensuring that risks are adequately controlled to maintain operational reliability and stakeholder confidence.

9.3 Preliminary Conclusions on Findings

There are some significant differences, as well as strong agreement on critical issues, between the survey data and interviews, according to the comparative analysis. Transparency, IT security and data quality have been consistently recognised as key risk areas in both quantitative and qualitative data. The interviews provided a more in-depth background, which enriched the survey results. For example, patient safety and data quality were closely linked in the health sector, while the integration of new AI technologies with outdated systems was a barrier in the automotive sector. There is a clear difference in the way in which cyber security problems have been tackled (Rana M., & Daultani Y. 2022). The survey results showed that people were generally aware of the problem, but interviews revealed that not all sectors were equally prepared. For example, the energy sector has stressed the need to protect against new cyber threats, while the electronics industry has shown a higher rate of taking sophisticated preventive measures. The interviews highlighted practical challenges in implementing Explainable AI models, an aspect not fully captured by the questionnaires. This comparison show how qualitative and quantitative approaches work together: surveys deliver general view of perceived risks, while interviews provide more in-depth context and practical insights. The results suggest that mitigation strategies should address the unique requirements of each sector and aligned with organisational objectives.

10. Discussion

This section summarizes the study's findings, limitations, contributions to future research, and practical implications.

10.1 Limitations and considerations

This research contributes significant insights into the implementation of ML and AI in supply chain management; however, it is not without limits. First, the geographical focus was mainly on sectors and regions with medium to high levels of AI adoption. Therefore, the outcomes might not adequately represent experiences of areas with limited resources for technology adoption or where AI infrastructure is still in a preliminary stage. This regional trend may limit the applicability of recommendations to developing markets or regions with less advanced technology (R. A. 2020). The study also focused on sectors such as automotive, electronics and health care, which are often the first to adopt AI. This focus has led to under-representation of sectors such as logistics, small scale retail and agriculture, which face distinct challenges including financial constraints, workforce preparation and technological preparation. As a result, the unique risks and obstacles faced by these under-represented industries remain insufficiently explored. Finally, while the survey results were statistically significant, the size and scope of the sample could be extended to include a wider and more diverse set of respondents. The research presents only a temporary view of the current state of AI integration, limiting the ability to monitor how risks and benefits evolve over time. Consequently, it is important to take these constraints when analyzing the study's findings and recommendations.

10.2 Directions for future research

In order to mitigate these challenges and expande our knowledge of these tools, future research should aim at broadening their industrial and geographical scope (T. Wu & J.Blackhurst 2009). It would also be useful to carry out comparative studies across different geographic areas and regulatory regimes to explore how local political and economic factors influence the adoption of IA and risk mitigation strategies. Such research could reveal best practices specific to a region and contribute to a global framework for integrating AI into supply chains. In addition,

longitudinal studies could provide valuable information on the dynamic nature of risks and benefits over time, Capturing how organizations are adapting to evolving challenges such as cyber security threats or changes in transparency concerns (P. 2022). The ethical implications of AI adoption, particularly in areas such as health where human impact is significant, deserve further investigation. Addressing issues related to the algorithmic bias, equity in decision making and potential job substitution would enrich academic discourse and inform practical governance frameworks. Finally, promoting collaboration between technology providers, policymakers and industry leaders could accelerate the establishment of uniform standards for AI implementation. To ensure the choice of IA implementation, sector-specific guidelines on ethics, data security and transparency may be developed, Always maintaining the trust of stakeholders and improving the global scalability of supply chain solutions.

10.3 Conclusions

The study's findings show how machine learning (ML) and artificial intelligence (AI) could revolutionize supply chain management. These technologies have demonstrated their ability to increase efficiency and resilience in an increasingly complex world, improving demand forecasting, inventory management and operational agility (Abbas K., Afaq M., Khan T. 2020). However, significant challenges such as data quality deficiencies, cyber security vulnerabilities and lack of clarity in AI-based decision making processes hamper this potential. Incorporating machine and artificial intelligence into the supply chain is essential for strategic development, demanding strong governance structures, cross-functional cooperation and proactive risk management. It is not just a technological issue (Sodiya E. O., Jacks B. S., Ugwuanyi E. D. 2024). Building stakeholder confidence and ensuring the long-term sustainability of AI-based supply chains depends on how these issues are addressed.

Call to Action for Stakeholders

The following actions should be taken by supply chain managers, legislators and business executives to fully capitalize on the advantages of machine learning and artificial intelligence while minimizing potential risks: 1. Invest in Data Governance: To ensure accurate and high quality data, implement automated methods for data validation and conduct regular audits. 2. Strengthen Cyber Security Measures: To protect sensitive data, adopt multi-factor authentication, advanced encryption technologies and incident response strategies. 3. Promote Transparency: Prioritize Explainable AI (XAI) frameworks to make AI judgments verifiable and interpretable. 4. Cross-departmental cooperation: For a well-rounded AI strategy for integration, encourage collaboration between different teams to ensure that AI projects support and align with the company's overall goals. 5. Interact with Legislators: Promote the creation of industry-wide guidelines that support data security and ethical use of AI.

By addressing these issues, companies can leverage AI and ML to develop more efficient, secure, transparent and flexible supply chains to adapt to changing needs.

11. References

Christopher, M. 2011. *Logistics and supply chain management.* Pearson Education.

Ghadge, A. & Dani, S. 2012. *Supply chain risk management: present and future scope.* The International Journal of Logistics Management.

N.Faisal, M. 2009. *Prioritization of Risks in Supply Chains.* Managing Supply Chain Risk and Vulnerability.

Blackburn, W.R. 2007. *The sustainability handbook: The complete management guide to achieving social, economic and environmental responsability.* London: Earthscan.

Shukla, Rajendra Kumar, Dixit Garg. 2011. *Understanding of supply chain: a literature review.* International Journal of Engineering Science and Technology.

Shukla, R. K., Garg, D., & Agarwal, A. 2011. *Understanding of supply chain: a literature review.* International Journal of Engineering Science and Technology.

Colicchia C., Fernand Strozzi. 2012. *Supply chain risk management: A new methodology for a systematic literature review.* Supply chain management: an international journal.

Heckmann, Iris, Tina Comes. 2014. *A critical review on supply chain risk- Definition, messure and modeling.* Omega.

Tiwari, S., H. M., & Daryanto, Y. 2020. *Big data analytics in supply chain management between 2010 and 2016: Insights to industries.* Computers & Industrial.

Cucchiella Federica, Massimo Gastaldi. 2006. *Risk management in supply chain: a real option approach.* Journal of Manufacturing Technology Management .

Gurtu, Amulya and Jestin Johny. 2021. *Supply Chain Risk Management: Literature Reviews.* Risks.

J., Johny. 2021. *Supply Chain Risk Management: literature review and future research.* Journal of business research.

Vincent, A., Tang, L., & Zailani, S. 2021. *Cybersecurity strategies for mitigating AI risks in supply chain management.* Information Security Journal.

Blackburn, W. R. 2007. *The Sustainability Handbook: the complete management guide to achieving social, economic and environmental responsability.* London: Earthscan.

Lim M. K., Qu Y. Ni. & Xiao Z. 2023. *Supply chain risk management with machine learning tecnology: a literature review and future research directions.* Computers & industrial Engineering.

Ghadge A., Dani S., & Kalawsky R. 2012. *Supply chain risk management: present and future scope.* The International Journal of Logistics Management.

Bailey, Tucker, Edward Barriball, Arnav Dey. 2019. *A practical approach to supply chain risk management.* McKinsey & Company.

H. Hoffman, C. Busse, C. Bode, M. Henke. 2014. *Sustainability- Related Supply Chain Risks: Conceptualization and Management in Business Strategy and the Environment.* John Wiley & Son.

A. Borghesi, B. Guedenzi. 2011. *Il Risk Management nella Supply Chain.* Sinergie rivista per studi e ricerche.

Tang, C. S. 2006. *Perspectives in supply chain risk management.* UCLA Anderson School.

Mihalis G., Thanos P. 2015. *Supply chain sustainability: a risk management approach.* International Journal of Production Economics.

Christopher, M. 2011. *Logistics & Supply Chain Management* . Pearson Education Limited.

Helo P., Hao Y. 2021. *Artificial intelligence in operations management and supply chain managment: an exploratory case study.*

V., Magri. 2023. "L'intelligenza artificiale e le applicazioni nei servizi finanziari."

F., Zuccari. 2023. "LLM: Applicazioni Pratiche e Prospettive Future."

Chen P. Y. & Wang F. K. 2020. *Artificial intelligence for supply chain management: a comprehensive literature review and research agenda. Expert Systems with Application.*

Emrouznejad A., Abbassi M., & Sicakyüz S. 2023. *Supply chain risk management: a content analysis-based review of existing and emerging topics.*

Zamani M., & Bhamra T. 2022. *Addressing data quality challenges in AI and ML applications for sustainable supply chains.* Sustainability and SCM.

Wu, T., & Blackhurst, J. 2009. *Supply chain risk management in China: Using the analytic hierarchy process for multi-criteria decision making.* International Journal of Logistics Research and Applications.

Thakur M., Patel P., Grupta L., Kumar M. 2023. *Applications of Artificial Intelligence and Machine Learning in Supply Chain Management: A Comprehensive Review.* European Chemical Bulletin.

Secchi R., Cannas V.G., Ciano M., Saltamalacchia M. 2022. *Supply chain management e intelligenza artificiale: migliorare i processi e la competitività aziendale.*

Z., Raziee. 2023. *AI and ML as an Antifragile Driver in the Supply Chain.* International Journal of Industrial Engineering and Operational Research.

A. Ghadge, S. Dani, R. Kalawsky. 2012. *Supply chain risk management: present and future scope.* The international journal of logistics management.

P., Akhtar. 2022. *detecting fake news and disinformation using artificial intelligence and machine learning to avoid supply chain disruptions.*

Abbas K., Afaq M., Khan T. 2020. *A blockchain and machine learning-based drug supply chain management and recommendation system for the smart pharmaceutical industry.*

Sodiya E. O., Jacks B. S., Ugwuanyi E. D. 2024. *Reviewing the role of AI and machine learning in supply chain analytics.* GSC Advanced Research and Reviews.

T. Wu & J.Blackhurst. 2009. *Managing Supply Chain Risk and Vulnerability: Tools and Methods for Supply Chain Decision Makers.*

A., Rai. 2020. *Explainable AI: From black box to glass box.* Journal of the Academy of Marketing Science.

Rana M., & Daultani Y. 2022. *Strategic AI applications in supply chains: Enhancing data quality and accuracy.* Supply Chain Dynamics.

Naz, A., Nazir, T., & Afzal, S. 2021. *Artificial intelligence and machine learning as future-proof strategies for supply chain risk mitigation.* Supply Chain Journal.

Christopher, M. 2011. *Logistics & Supply Chain Management.* Pearson Education Limited.

R., Manulli. 2023. *L'AI nel futuro del lavoro: competenze necessarie e sviluppo professionale.* Articolo Accademico.

E., Masia. 2024. *Supply Chain nel 2024: una partita a scacchi che si vince con l'AI* . Articolo Accademico.

Modgil S., Gunasekaran A., Pournader M., & Seuring S. 2021. *Resilience and agility in global supply chain networks: A study of AI-driven risk management.* International Journal of Production Research.

Ifesinachi, A. D., Sodiya, E. O., Jacks B. S. 2024. *Reviewing the role of AI and machine learning in supply chain analytis.*

Islam S., Amin S. H., Wardley L.J. 2021. *Machine Learning and optimization models for supplier selection and order allocation planning.* International Journal of production economics.

Kshetri, N. 2018. *Blockchain's roles in strengthening cybersecurity and protecting privacy.* Telecommunications Policy.

Górski, M., Nowicki, T., & Ustun, T. S. 2020. *Legal and ethical challenges in the AI-driven supply chain.* Technology and Ethics.

A., Aljohani. 2023. *Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility.* Sustainability.

Baryannis, G., Dani, S., & Antoniou, G. 2019. *Predicting supply chain risks using machine learning.* Future Generation Computer Systems.

Burstein, G., & Zuckerman, I. 2023. *Predicting supply chain risks using machine learning: The importance of explainability and transparency.* Journal of Supply Chain Management Science.

P. Ahi, C. Searcy. 2014. *Assessing sustainability in the supply chain: a triple bottom line approach in Applied Mathematical Modelling.* Toronto: Ryerson University.

12. Appendices

Risk	Mitigation Strategy	Practical Implications
Data Quality	- Implementation of regular data audits. - Use of automated tools for real-time data quality monitoring.	- Improved accuracy of AI/ML models. - Prevention of erroneous decisions caused by incomplete or incorrect data.
Cybersecurity	- Introduction of multi-factor authentication (MFA) systems. - Regular vulnerability assessments of systems.	- Reduced risk of cyberattacks. - Better protection of sensitive information exchanged between partners.
Transparency of AI Decisions	- Adoption of Explainable AI (XAI) models such as SHAP or LIME. - Human supervision in critical decisions.	- Increased trust and collaboration among supply chain partners. - Better compliance with regulatory requirements.
Technological Integration	- Investments in modern infrastructures compatible with AI/ML. - Training personnel on new technologies.	- Reduced implementation times. - Enhanced effectiveness of new technologies in daily operations.
AI Ethics	- Creation of ethical guidelines for AI usage. - Continuous monitoring to identify and reduce algorithmic bias.	- Prevention of discrimination or unfair decisions. - Increased accountability and compliance with corporate values.

Summary- Mitigation Strategies for Risks in AI/ML-Based Supply Chain

12.1 Analysis of survey

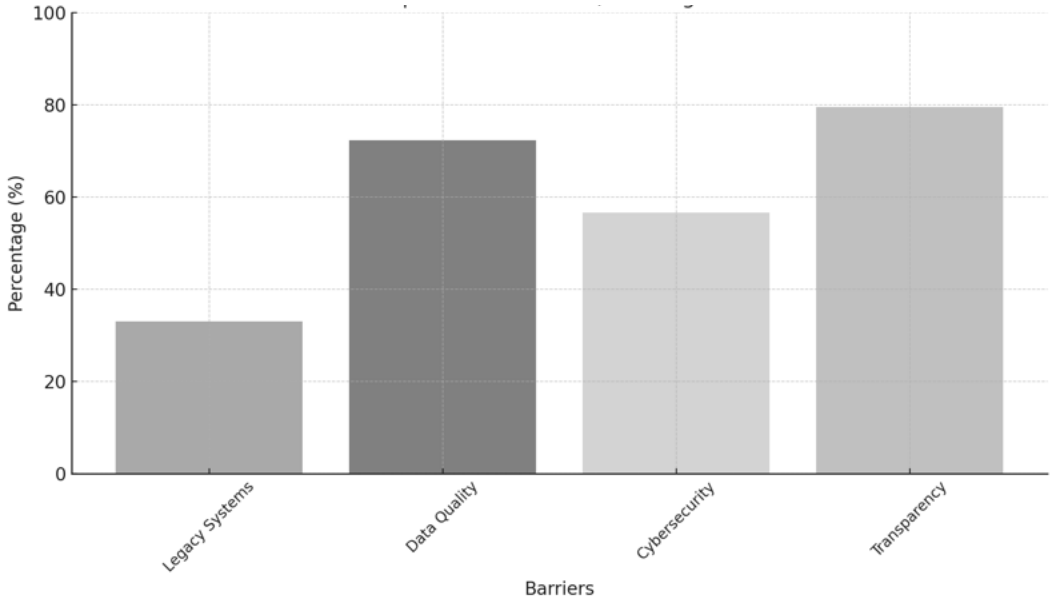

Figure 1- Adoption Barriers to AI/ML Integration

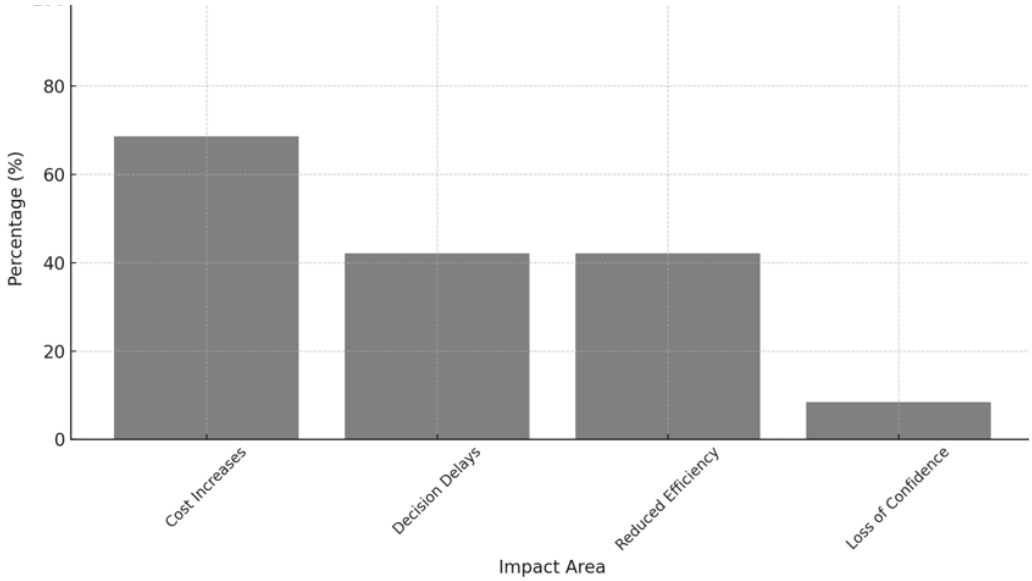

Figure 2- Impact of AI/ML Risks on Supply Chain Performance

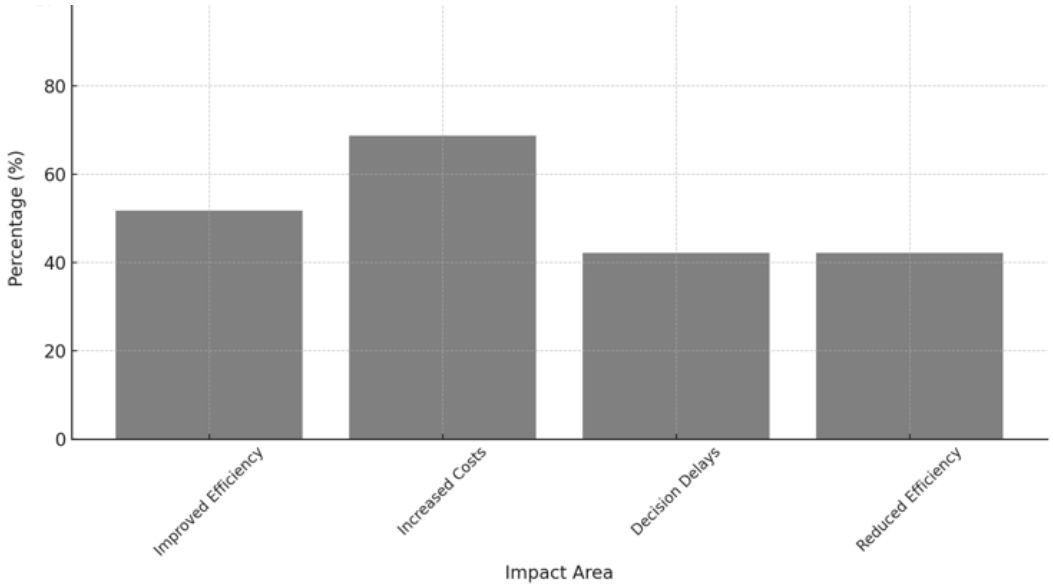

Figure 3- Performance Impact of AI/ML on Supply Chains

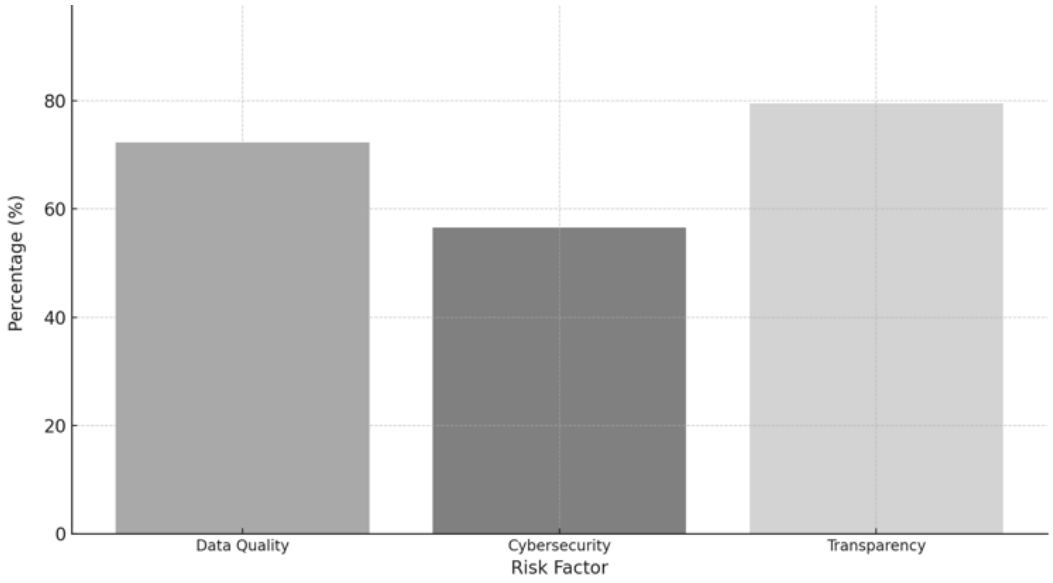

Figure 4- Perceived Risks in Supply Chain AI/ML Integration

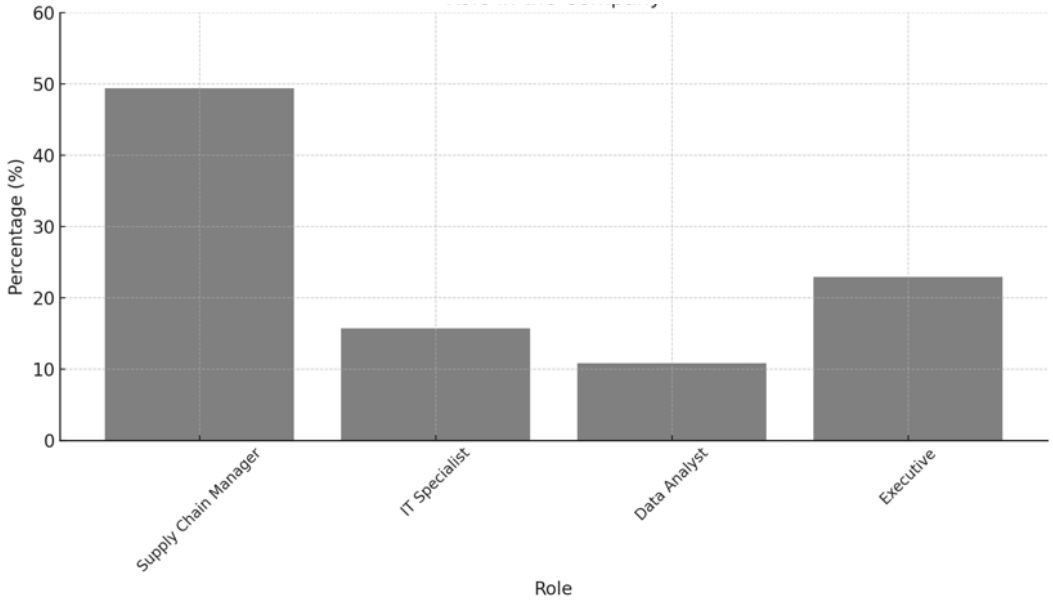

Figure 5- Role in the company

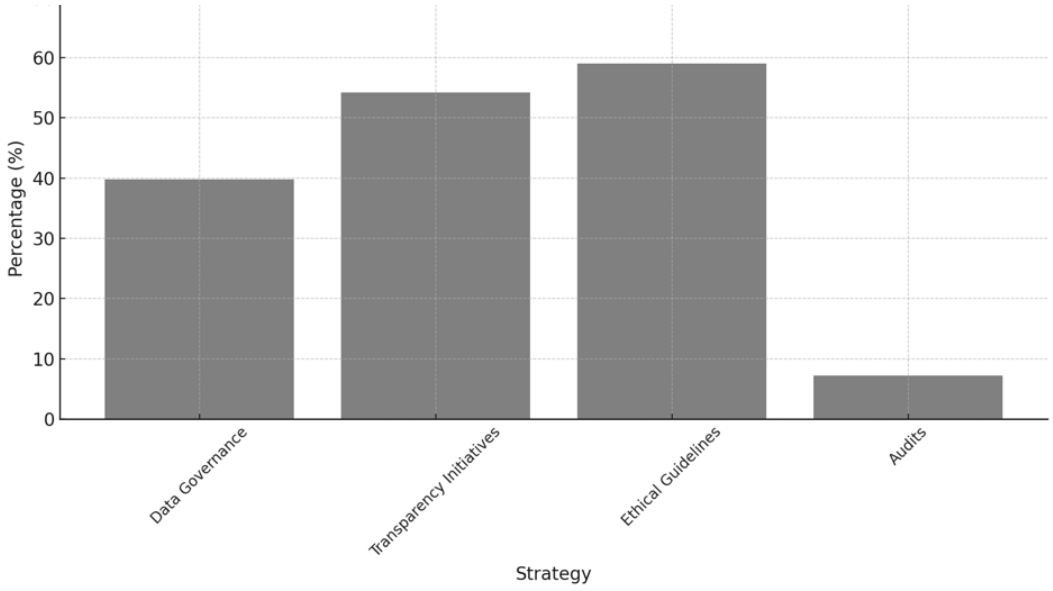

Figure 6- Adopted Strategies for Risk Mitigation

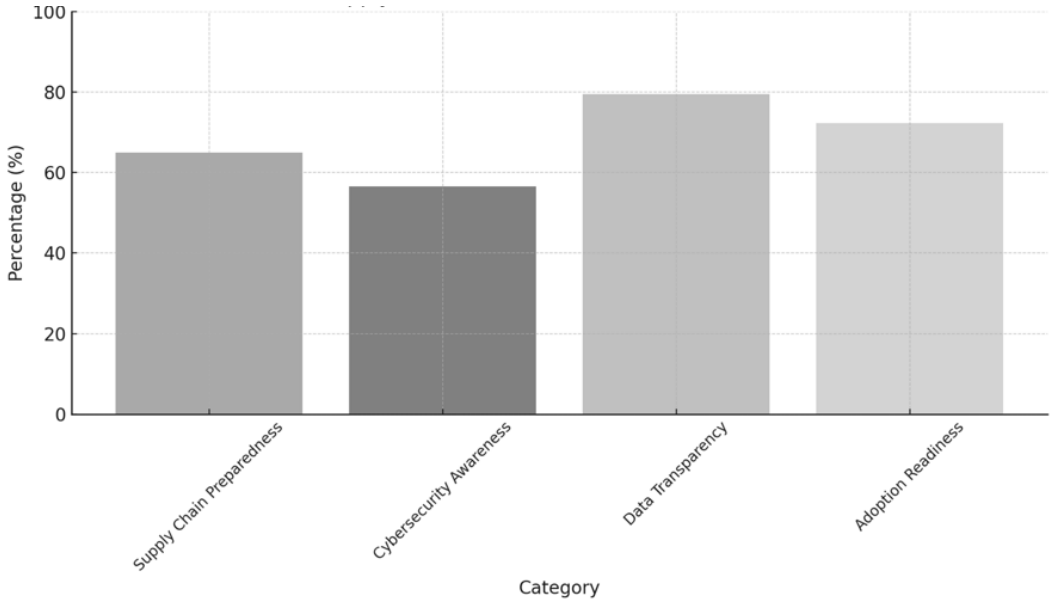

Figure 7- Supply Chain AI/ML Readiness and Awareness

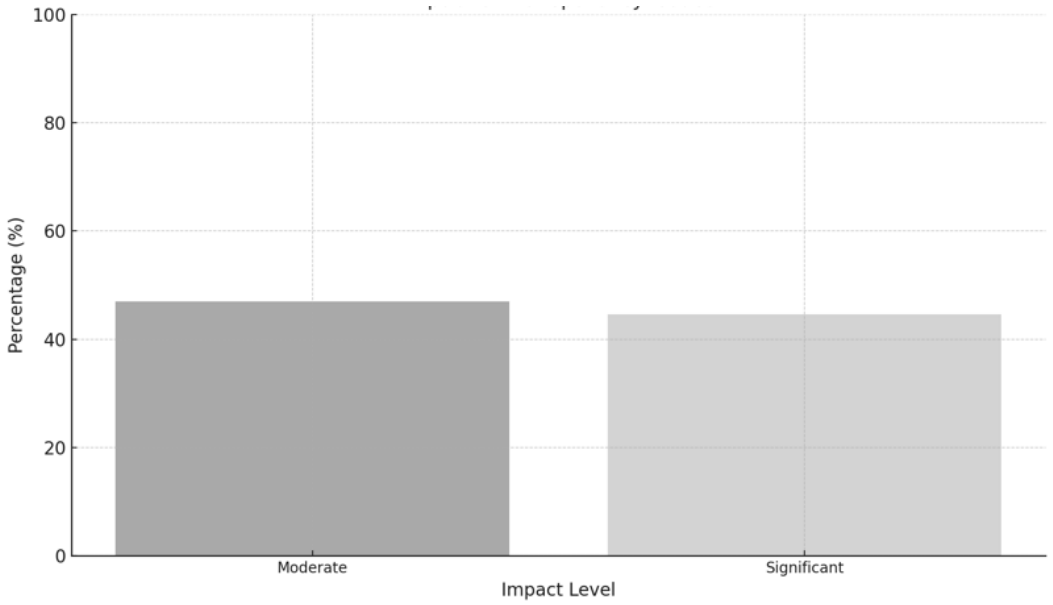

Figure 8- Impact of Transparency Issues

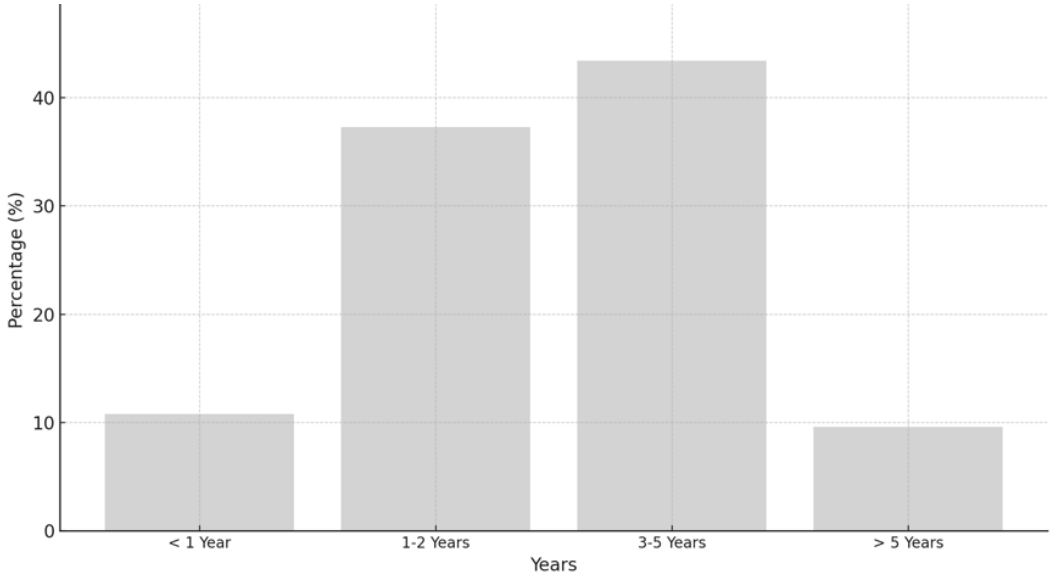

Figure 9- Years of AI/ML Usage in Supply Chain Operations

12.2 Analysis of interviews

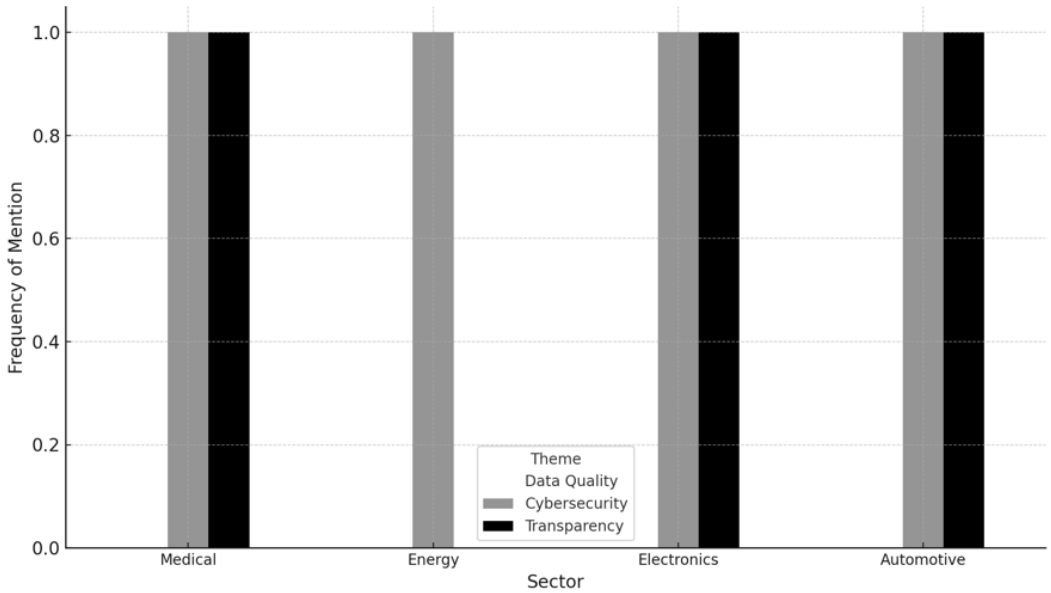

Figure 10- Key Risk Themes Across Sectors

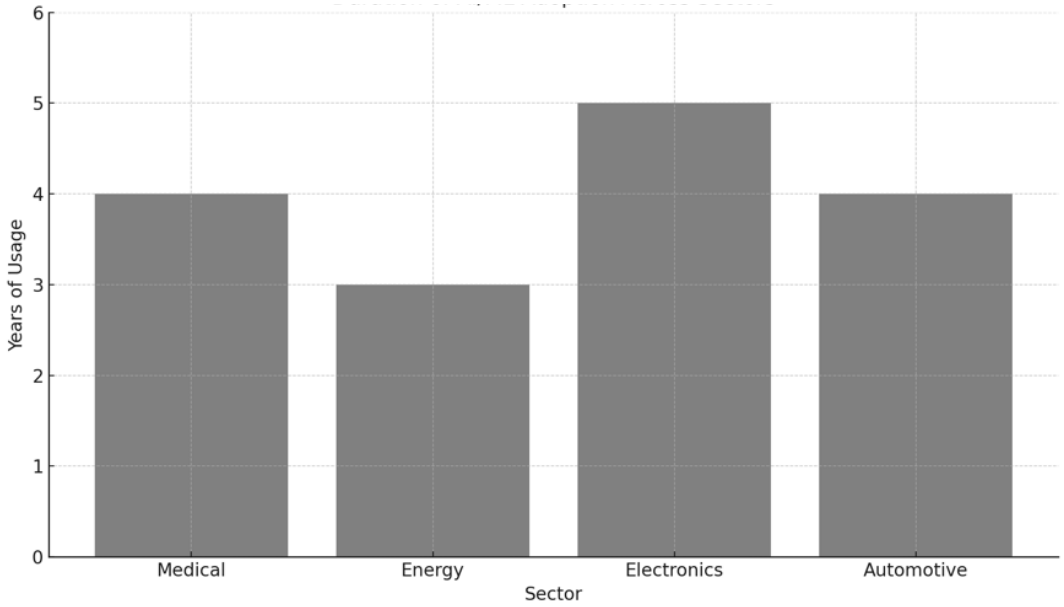

Figure 11- Duration of AI/ML Adoption Across Sectors

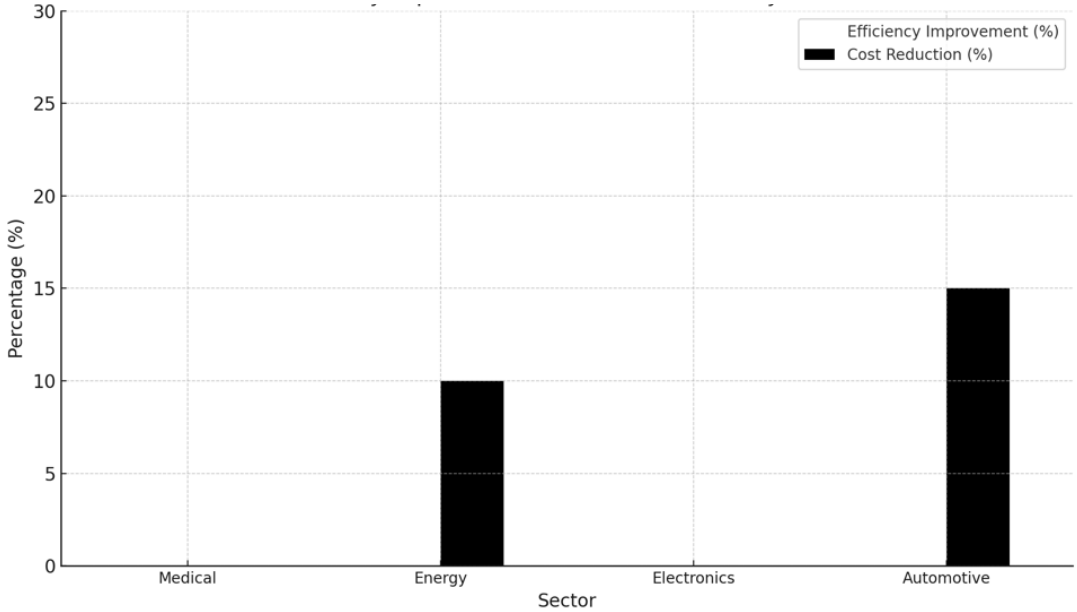

Figure 12- Efficiency Improvement and Cost Reduction by Sector

Sector	Significant Impact
Medical	Reduced downtime (-15%), rapid demand response
Energy	Reduced material losses (-20%), improved resource efficiency
Electronics	Improved demand forecasting (+25%), reduced inefficiencies (-30%)
Automotive	Improved logistics precision (+25%), reduced delivery delays

Table 1- Significant Impact of AI/ML Across Sectors

Sector	Mitigation Strategies	Adaptations
Medical	Real-time dashboards, updated privacy protocols	Updated privacy protocols, blockchain exploration
Energy	Constant algorithm evaluation, weather adjustments	IoT for resource monitoring
Electronics	Continuous model monitoring, encryption upgrades	Chatbots for supplier queries
Automotive	KPI tracking, supplier-specific adaptations	Blockchain for component traceability

Table 2- Mitigation Strategies and Adaptations Across Sectors

Sector	Recommendations
Medical	Start small, evaluate data quality
Energy	Invest in workforce training
Electronics	Begin with pilot projects, test data reliability
Automotive	Gradual AI integration, test in small steps

Table 3- Recommendations for the Future Across Sectors

Sector	Role	Years of AI/ML Usage
Medical	Supply Chain Director, focusing on logistics	4 Years
Energy	Logistics and Supply Chain Manager	3 Years
Electronics	Supply Chain Director for predictive processes	5 Years
Automotive	Operations Manager for components management	4 Years

Table 4- Roles and AI/ML Usage Across Sectors

Sector	Future Vision	New Solutions
Medical	Real-time monitoring for medical devices	Exploring blockchain for traceability
Energy	AI for demand prediction, automated deliveries	IoT for real-time resource monitoring
Electronics	AI for market trend forecasting	Chatbots for supplier management
Automotive	Just-in-time production optimization	Blockchain for component traceability

Table 5- Future and New Solutions Across Sectors