Sistem Pendukung Keputusan dengan Aplikasi
Vol. 5, No. 1, (2026), pp. 58-68
ISSN: 2829-2189, DOI: https://doi.org/10.55537/spk.v5i1.1601

Data Poisoning, Data Drift, and Data Integrity in Supply Chain Systems: Emerging Threats to AI Governance

(Data Poisoning, Data Drift, dan Data Integrity dalam Sistem Supply Chain: Ancaman yang Muncul terhadap Tata Kelola AI)

Umamaheswari Shanmugam [a,*], Mohan Kumar Rajendran [b], Natarajan Jawahar [a], Narayana R. Karri V. V. S [a]

[a] JSS Academy of Higher Education & Research, Ooty, 643001, India
[b] Magnaait Ltd., London, WC1X 9BW, United Kingdom

* Corresponding author.
E-mail: uma.maye@gmail.com

Received 3 March 2026; Revised 26 March 2026; Accepted 31 March 2026;
Available online 1 April 2026.

ABSTRACT

Artificial intelligence (AI) plays a critical role in supply chain systems by enabling predictive analytics and data-driven decision-making. However, increasing reliance on AI exposes systems to significant data-related vulnerabilities that may compromise reliability and trust. This study investigates three major threats to AI governance: data poisoning, data drift, and data integrity. Using a qualitative literature-based analysis supported by synthesized empirical evidence, this study evaluates the impact of these threats on model performance and operational outcomes. The results show that data poisoning can significantly reduce model accuracy (from approximately 95% to below 75%) and introduce bias, while data drift leads to gradual performance degradation over time due to changing data distributions. In addition, data integrity issues—such as incomplete, corrupted, or unauthorized data—undermine decision reliability and amplify the effects of poisoning and drift. To address these challenges, the study proposes a multi-layered AI governance framework integrating technical safeguards (e.g., adversarial detection and continuous monitoring), organizational controls, and policy-level compliance mechanisms. The findings provide practical insights for improving AI robustness, operational resilience, and trust in supply chain environments, contributing to the development of effective and responsible AI governance.

Keywords: *AI Governance; Data Poisoning; Data Drift; Data Integrity; Supply Chain Systems; Ethical AI*

ABSTRAK

Kecerdasan buatan (Artificial Intelligence/AI) memainkan peran penting dalam sistem rantai pasok (supply chain systems) dengan memungkinkan analitik prediktif dan pengambilan keputusan berbasis data. Namun, meningkatnya ketergantungan pada AI membuat sistem rentan terhadap berbagai kerentanan terkait data yang dapat mengganggu keandalan dan tingkat kepercayaan. Studi ini meneliti tiga ancaman utama terhadap tata kelola AI, yaitu data poisoning, data drift, dan data integrity. Dengan menggunakan analisis kualitatif berbasis literatur yang didukung oleh sintesis bukti empiris, studi ini mengevaluasi dampak dari ancaman tersebut terhadap kinerja model dan hasil operasional. Hasil penelitian menunjukkan bahwa data poisoning dapat secara signifikan menurunkan akurasi model (dari sekitar 95% menjadi di bawah 75%) serta memperkenalkan bias, sementara data drift menyebabkan penurunan kinerja secara bertahap seiring waktu akibat perubahan distribusi data. Selain itu, masalah data integrity—seperti data yang tidak lengkap, rusak, atau tidak sah—melemahkan keandalan pengambilan keputusan dan memperkuat dampak dari poisoning dan drift. Untuk mengatasi tantangan ini, studi ini mengusulkan kerangka kerja tata kelola AI berlapis yang mengintegrasikan perlindungan teknis (misalnya deteksi adversarial dan pemantauan berkelanjutan), kontrol organisasi, serta mekanisme kepatuhan di tingkat kebijakan. Temuan ini memberikan wawasan praktis untuk meningkatkan ketahanan model AI, resiliensi operasional, dan kepercayaan dalam lingkungan rantai pasok, serta berkontribusi pada pengembangan tata kelola AI yang efektif dan bertanggung jawab.

Kata kunci: *AI Governance; Data Poisoning; Data Drift; Data Integrity; Supply Chain Systems; Ethical AI*

1. INTRODUCTION

1.1 Context of AI Governance

Artificial intelligence (AI) is a key technology in contemporary organizations that has transformed decision-making, operations, and strategy across various industries, including healthcare, finance, and supply chain management [1], [2]. As dependence on AI-driven systems increases, the need for well-developed AI governance frameworks has become more critical to ensure that AI applications remain ethical, reliable, and compliant with regulatory standards [3], [4].

AI governance includes policies, standards, and accountability mechanisms that guide the development, deployment, and oversight of AI systems. These frameworks emphasize transparency, fairness, and responsibility to ensure that AI technologies operate without causing unintended consequences or misuse [5], [6].

1.2 Relevance to Supply Chain and Information Systems

AI models are widely used in supply chain management for predictive analytics, demand forecasting, inventory optimization, and logistics planning. Despite these advantages, AI systems face emerging risks related to data poisoning, data drift, and compromised data integrity [7]–[9].

Data poisoning involves the manipulation of training datasets that may significantly degrade model performance and lead to incorrect predictions and operational losses [10], [11]. Data drift occurs when the statistical properties of input data change over time, reducing model accuracy without proper monitoring and retraining [12], [13]. These issues threaten data integrity and undermine trust in AI-driven decision-making systems [14], [15].

1.3 Problem Statement

Although there has been increasing adoption of AI governance models, AI systems used in supply chain and information systems continue to face threats from adversarial attacks, data drift, and data corruption [8], [16], [17].

Existing governance mechanisms are often compliance-driven and operationally focused; however, they may lack comprehensive approaches for identifying and mitigating sophisticated attacks or maintaining long-term data integrity. Such limitations expose AI systems to risks of manipulation, which can negatively affect organizational efficiency, decision-making accuracy, and stakeholder trust.

Addressing these vulnerabilities is therefore essential to protect AI systems and ensure the ethical and sustainable deployment of AI technologies in complex organizational environments.

1.4 Research Objectives

This study seeks to address three primary research objectives. First, it analyzes how data poisoning affects the integrity and reliability of AI systems used in supply chain environments. Second, it examines the impact of data drift on AI-driven decision-making and identifies associated operational and strategic risks. Third, it evaluates governance models, technical mitigation strategies, and policy-level interventions that can reduce these risks and improve transparency, accountability, and trust in AI systems [18]–[20].

Through these objectives, the study aims to provide practical insights for practitioners, policymakers, and organizations implementing AI in high-stakes, data-intensive operational settings.

1.5 Contribution to the Field

The originality of this study lies in its integrated examination of data poisoning, data drift, and data integrity challenges within the broader context of AI governance, particularly in supply chain and information system environments.

By synthesizing current research and proposing governance and mitigation strategies, the study provides both theoretical and practical contributions to the field. The findings offer insights into improving AI system reliability, security, and ethical implementation. Furthermore, the study establishes a foundation for future research aimed at developing resilient AI governance frameworks capable of supporting reliable and trustworthy AI operations in increasingly complex data environments.

2. LITERATURE REVIEW

2.1 AI Governance and Supply Chain Systems

Artificial intelligence governance has become a major research focus due to the increasing adoption of AI systems in supply chain management and information systems. Governance frameworks aim to ensure that AI systems operate in an ethical, safe, and reliable manner while complying with organizational regulations and policies [1], [2].

AI technologies are widely used for predictive analytics, demand forecasting, logistics optimization, and inventory management in supply chains. However, these applications also introduce operational and ethical risks when AI models are compromised or poorly governed [4].

Several governance frameworks have been developed to incorporate ethical, technical, and regulatory controls into AI deployment [3], [5]. These frameworks emphasize transparency, accountability, and continuous monitoring to enhance trust in AI-assisted decision-making processes.

In addition, human-rights-centered governance approaches and corporate digital responsibility initiatives promote responsible AI practices and align AI governance with broader societal expectations [6], [21]. Governance paradigms

applied to cloud-based AI ecosystems further highlight the importance of maintaining regulatory integrity and secure data exchange to prevent supply chain disruptions [15].

2.2 Data Poisoning in AI

Data poisoning represents one of the most significant threats to AI systems because it involves the intentional manipulation of training data to compromise model performance or introduce systematic biases [7], [8].

In supply chain environments, such attacks can distort predictive analytics and lead to inaccurate demand forecasting, inefficient inventory management, and reduced operational efficiency [10], [11].

Empirical studies have identified several types of poisoning attacks, including label-flipping attacks, backdoor attacks, and targeted adversarial manipulation. These techniques can compromise both supervised and unsupervised machine learning models, highlighting the vulnerability of AI systems deployed in high-stakes environments [12], [14].

Mitigation strategies such as adversarial training, anomaly detection, and trustworthy AI mechanisms have been proposed to enhance resilience against such attacks [14]. Furthermore, securing interconnected AI infrastructures operating in cloud and edge computing environments is essential because compromised data can rapidly propagate across distributed systems [18].

2.3 Data Drift and Data Integrity Problems

Another major challenge affecting AI systems is data drift, which occurs when the statistical properties of input data change over time and negatively impact model performance [12], [13].

Concept drift is particularly significant in complex environments such as supply chains, where market conditions, consumer preferences, and operational dynamics continuously evolve.

If unmanaged, data drift can result in inaccurate forecasts, declining model performance, and operational inefficiencies [22], [23]. Maintaining data integrity is therefore critical for sustaining reliable AI-driven decision-making.

Data integrity issues such as corrupted datasets, incomplete information, and unauthorized modifications can significantly compromise both real-time operational decisions and long-term strategic planning. Mitigation measures such as continuous data auditing, automated validation systems, model retraining, and version control mechanisms help detect and address drift-related problems [19], [20].

2.4 Existing Mitigation Strategies

Various mitigation strategies have been proposed to address data poisoning, data drift, and data integrity challenges. Technical approaches include adversarial defenses, robust model training techniques, anomaly detection mechanisms, and privacy-enhancing technologies [14], [24].

Continuous monitoring systems allow organizations to detect drift and unusual data patterns early, while periodic model retraining ensures sustained predictive accuracy [16].

These technical safeguards are complemented by organizational governance mechanisms such as internal audits, governance frameworks, and employee training programs. Regulatory compliance structures further strengthen governance by ensuring that AI systems operate ethically, securely, and responsibly [19], [25].

Empirical evidence suggests that a multi-layered governance framework integrating ethical, technical, and regulatory dimensions is the most effective strategy for addressing emerging AI risks in supply chain systems [18], [26].

2.5 Gap in Research

Although a substantial body of literature exists on AI governance and technical mitigation strategies related to data poisoning and data drift, a clear gap remains in aligning governance mechanisms with real-world supply chain practices. Many studies focus primarily on technical defenses or generic governance frameworks without considering the operational complexities of supply chain environments [7], [17].

This highlights the need for an integrated governance framework that combines ethical, technical, and policy-based mechanisms specifically tailored to address AI integrity risks in supply chain and information system contexts. The present study addresses this gap by synthesizing existing research and proposing governance strategies designed to enhance trust, sustainability, and ethical management of AI systems.

3. METHODOLOGY

3.1 Research Design

This study adopts a qualitative research design based on a conceptual and analytical approach to investigate emerging threats to AI governance in supply chain and information systems. Considering the complexity and dynamic nature of AI models operating in real-world environments, a qualitative approach is appropriate for examining issues related to data poisoning, data drift, and data integrity vulnerabilities [7], [8]. The study integrates findings from existing literature, documented case studies, and reported AI system failures to develop a comprehensive understanding of vulnerabilities and governance requirements. This approach enables the identification of trends, governance processes, and policy mechanisms that may not be fully captured through purely quantitative methods [9], [16].

3.2 Data Collection

Data for this study were collected from multiple secondary sources, including peer-reviewed journal articles, conference proceedings, industry reports, and preprint repositories related to AI governance and supply chain systems. These sources provided both theoretical and empirical insights into data poisoning attacks, concept drift, and AI data integrity challenges [12], [14].

The analysis also considered documented case studies involving AI-driven logistics systems, predictive analytics models, and decision-support platforms used in supply chains. The inclusion criteria focused on publications that provided relevant insights into governance mechanisms, technical mitigation strategies, and ethical control frameworks for AI systems [15], [18].

3.3 Threat Identification and Analysis

Threat identification involved the systematic analysis of vulnerabilities affecting AI systems, particularly data poisoning, data drift, and data integrity degradation. Previous studies have employed techniques such as anomaly detection, adversarial attack simulations, and continuous monitoring to analyze how these threats emerge and affect AI system performance [10], [11].

Data poisoning was examined through documented cases of manipulated training datasets and their impact on predictive accuracy and decision-making reliability [8], [17]. Concept drift was analyzed through studies describing the degradation of model performance over time in dynamic operational environments. Data integrity risks were evaluated through data quality management perspectives, including issues related to mislabeling, incomplete datasets, and unauthorized data modifications [13], [19].

In addition, existing defensive mechanisms such as anomaly detection systems, privacy-enhancing technologies, and monitoring frameworks were reviewed to evaluate their effectiveness in detecting and mitigating these threats [14], [24].

3.4 AI Governance Framework

To mitigate identified risks, the study evaluates a multi-layered AI governance framework integrating technical, organizational, and policy-level controls. The proposed framework includes continuous monitoring for data drift, implementation of defenses against data poisoning attacks, and mechanisms to ensure data integrity throughout the AI lifecycle [20], [25].

The framework also incorporates ethical governance and regulatory compliance structures that promote responsible AI deployment and accountability. By integrating governance controls across technical and organizational levels, the framework aims to enhance reliability and trust in AI systems operating in supply chain environments [15], [26].

3.5 Limitations

Despite providing a comprehensive qualitative analysis, this study has several limitations. First, the analysis relies primarily on secondary data sources, which may introduce biases due to selective reporting or limited access to detailed operational data. Second, the case studies and literature reviewed are derived from different industries and operational contexts, which may limit the generalizability of findings across all supply chain environments [7], [17].

Third, the study focuses on documented AI threats and governance practices, which means emerging or unreported vulnerabilities may not be fully captured. Finally, the governance framework proposed in this study is conceptual and requires empirical validation through real-world implementation and testing in supply chain or information system environments [18], [19].

4. RESULTS AND DISCUSSION

4.1 Findings on Data Poisoning

Data poisoning represents one of the most significant vulnerabilities affecting AI systems in supply chain management because it directly impacts predictive accuracy and model reliability. Two common forms of poisoning attacks—label-flipping and adversarial input manipulation—can significantly degrade forecasting accuracy, leading to operational inefficiencies such as inventory misallocation and inaccurate demand planning [7], [8].

Empirical evidence indicates that even small manipulations within training datasets can propagate through interconnected AI systems and amplify operational risks across supply chain networks [10], [11].

As shown in Table 1, model performance declines progressively as the percentage of poisoned data increases. At 0% poisoning, the model achieves 95% accuracy and 94% F1-score; however, performance drops to 73% accuracy and 72% F1-score at 20% poisoning. This demonstrates the high sensitivity of AI models to data manipulation.

Table 1. AI Model Performance Decline Under Data Poisoning Attacks

Poisoning Percentage (%)	Model Accuracy (%)	F1-Score (%)
0	95	94
5	91	90
10	86	85
15	80	79
20	73	72

As further illustrated in Figure 1, both accuracy and F1-score decrease consistently as the proportion of poisoned data increases, reinforcing the numerical findings presented in Table 1.

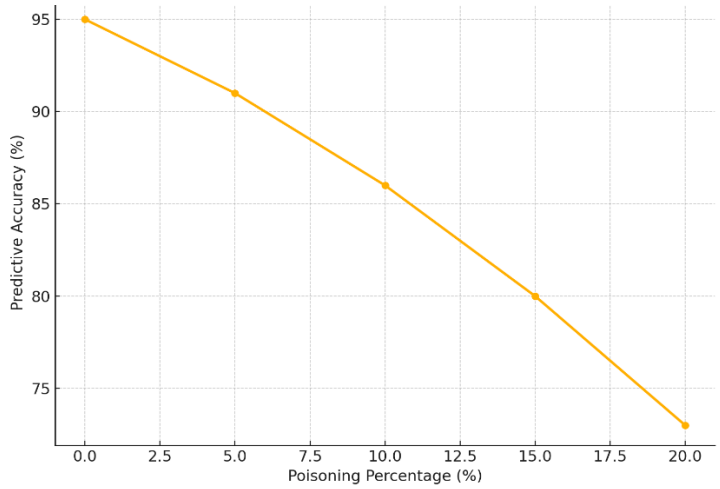

Figure 1. Impact of Data Poisoning on AI Model Performance.

The findings highlight the need for effective mitigation strategies, such as adversarial training, anomaly detection, and trustworthy AI frameworks, to ensure the reliability and sustainability of AI systems used in supply chain management [8], [14].

4.2 Impact of Data Drift

Data drift, which occurs when the statistical distribution of input data changes over time, can significantly affect long-term predictions and decision-making in AI systems [12], [13]. In dynamic supply chain environments, such drift reduces model adaptability and negatively impacts both demand forecasting and logistics scheduling accuracy.

Concept drift, in particular, arises when underlying patterns—such as consumer behavior, supplier relationships, and market dynamics—evolve, requiring predictive models to continuously adapt to changing conditions.

As presented in Table 2, model performance gradually declines over a 12-month period. Model accuracy decreases from 95% to 78%, while precision and recall follow similar trends, indicating reduced model effectiveness over time.

Table 2. Model Performance Degradation Due to Concept Drift

Time Period (Months)	Model Accuracy (%)	Precision (%)	Recall (%)
0	95	94	93
3	92	90	89
6	88	86	85
9	83	81	80
12	78	76	75

This trend is further illustrated in Figure 2, which shows the consistent degradation in model performance due to evolving data distributions.

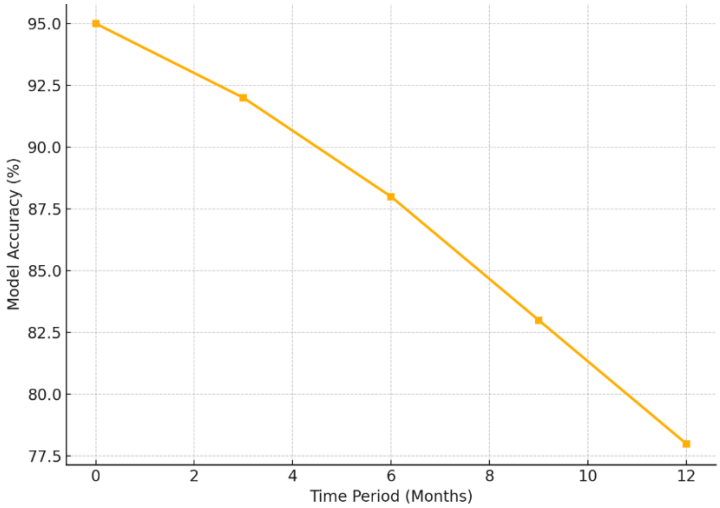

Figure 2. Model Performance Degradation Due to Concept Drift.

Regular model retraining, continuous monitoring, and automated validation pipelines are essential mechanisms for mitigating the effects of data drift and maintaining operational efficiency [19], [20].

4.3 Data Integrity Challenges

One of the most significant challenges in AI-driven supply chain systems is ensuring data integrity. Issues such as missing data, data corruption, unauthorized modifications, and incomplete records can significantly affect the reliability of decision-making processes and introduce operational inefficiencies [22], [23].
Compromised data not only exacerbates the effects of data poisoning and drift but also undermines stakeholder trust.

As summarized in Table 3, different types of data integrity issues have direct implications for AI decision-making. For example, incomplete data reduces predictive accuracy, while unauthorized modifications compromise model reliability and trustworthiness.

Table 3. Data Integrity Issues in Supply Chain AI Systems

Data Integrity Issue	Description	Impact on AI Decision-Making
Incomplete Data	Missing entries in datasets	Reduced predictive accuracy and flawed forecasts
Corrupted Data	Erroneous or inconsistent entries	Misleading predictions and operational inefficiencies
Unauthorized Modifications	Data altered without proper control	Compromised model trustworthiness
Data Duplication	Repeated or redundant entries	Skewed model learning and bias
Inconsistent Formatting	Variations in data structure or labeling	Errors in data processing

The propagation of these issues throughout the AI pipeline is illustrated in Figure 3, showing how errors introduced at early stages affect downstream outputs.

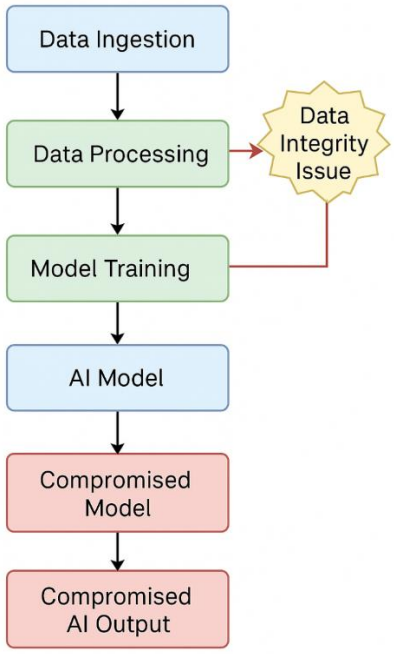

Figure 3. Propagation of Data Integrity Failures in AI Pipelines.

Ensuring the reliability of AI models requires robust governance mechanisms, including regular data audits, validation procedures, and ethical oversight frameworks [15], [18].

4.4 Governance and Mitigation Strategies

A multi-layered governance approach can effectively mitigate AI-related risks in supply chain systems by integrating technical, organizational, and policy-level interventions.

Technical solutions include adversarial defenses, anomaly detection mechanisms, privacy-enhancing technologies, and continuous monitoring of model performance [14], [24]. Organizational strategies involve establishing accountability structures, conducting internal audits, and providing personnel training to identify and respond to AI-related risks [25], [26]. Policy-level governance ensures responsible AI implementation through regulatory compliance and alignment with industry standards.

As presented in Table 4, different AI threats require specific governance strategies and corresponding mitigation measures.

Table 4. Governance Strategies for AI Risk Mitigation

AI Threat	Governance Strategy	Type of Measure	Expected Outcome
Data Poisoning	Adversarial training, anomaly detection	Technical	Detect and neutralize malicious inputs
Data Drift	Continuous monitoring, periodic retraining	Technical	Maintain predictive accuracy
Integrity Breaches	Data auditing, validation protocols	Technical/Organizational	Ensure reliable data
Unauthorized Access	Access control, encryption	Technical/Policy	Prevent unauthorized changes
Regulatory Non-Compliance	Policy alignment, compliance frameworks	Policy/Organizational	Ensure legal and ethical compliance
Ethical Misalignment	Training and accountability mechanisms	Organizational	Promote responsible AI use

The integrated governance structure is further illustrated in Figure 4, highlighting how different layers of control work together to mitigate AI-related risks.

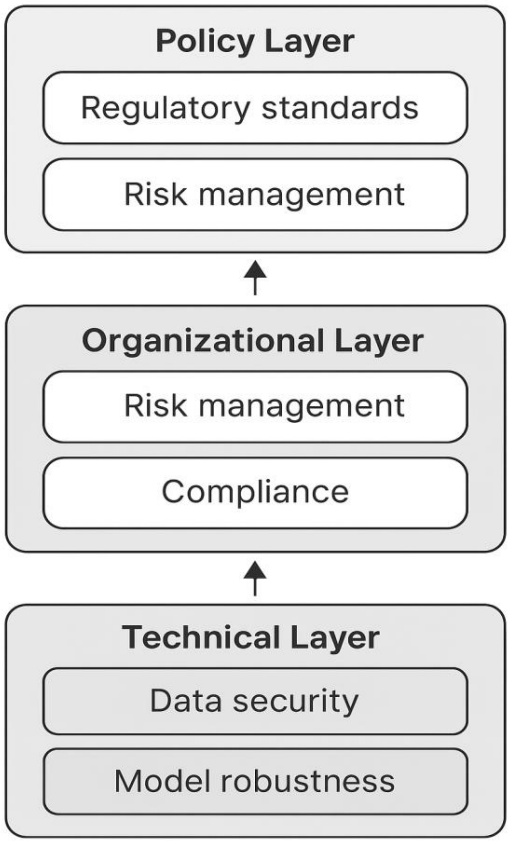

Figure 4. Multi-layered AI Governance Framework for Supply Chain Systems.

Using this framework, organizations can enhance AI reliability, reduce operational risks, and improve trust in AI-driven supply chain systems [19], [20].

4.5 Practical Implications

The findings have important implications for businesses, AI practitioners, and supply chain managers. Operational resilience and predictive accuracy can be improved through continuous monitoring of AI systems, periodic model retraining, and robust data auditing protocols [8], [25].

In addition, ethical oversight and regulatory compliance mechanisms enhance stakeholder trust, particularly when AI systems process sensitive operational or customer-related data.

As summarized in Table 5, several best practices can support effective AI governance implementation.

Table 5. Best Practices for AI Governance Implementation

Practice Area	Recommended Action	Purpose / Benefit
Data Governance	Continuous auditing and validation	Ensure data integrity
AI Model Management	Regular retraining and drift monitoring	Maintain accuracy
Threat Mitigation	Adversarial training and anomaly detection	Prevent attacks
Ethical Oversight	Accountability structures and training	Ensure ethical AI use
Regulatory Compliance	Align with legal and industry standards	Maintain compliance
Technical Safeguards	Access control and encryption	Prevent data breaches
Organizational Readiness	Cross-functional collaboration	Improve responsiveness

The relationship between AI threats, governance strategies, and operational outcomes is illustrated in Figure 5, showing how proper governance improves system reliability and efficiency.

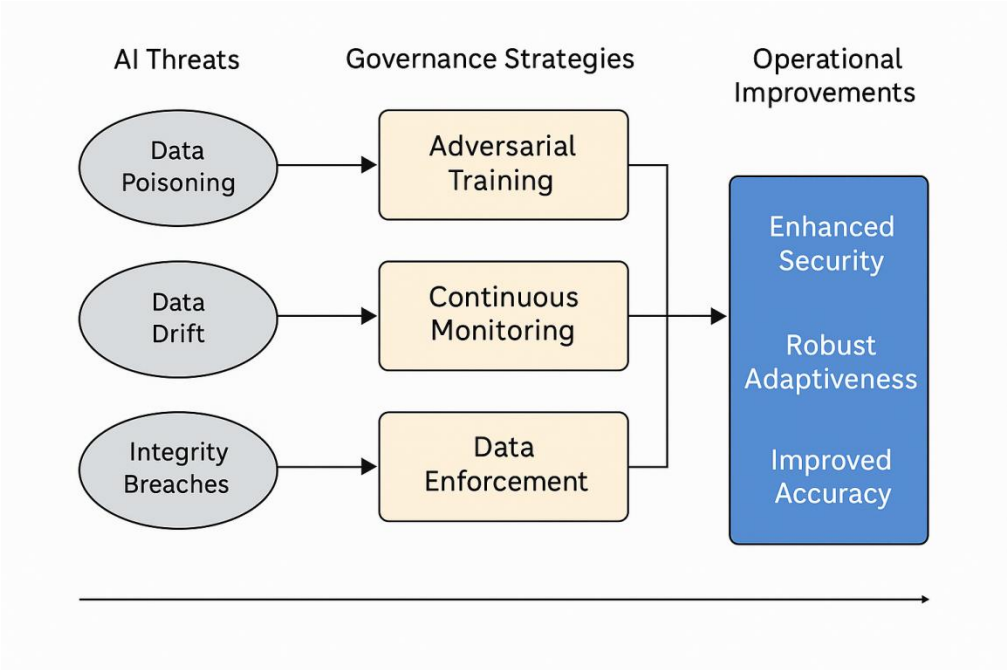

Figure 5. Relationship Between AI Threats, Governance Strategies, and Outcomes.

The implementation of these governance strategies enables organizations to protect AI-driven decision-making, reduce financial and operational risks, and enhance the reliability of supply chain information systems.

5. CONCLUSION

5.1 Summary of Key Findings

This study examined emerging threats to AI governance in supply chain and information system environments, focusing on data poisoning, concept drift, and data integrity challenges. The findings indicate that even minor manipulation of training datasets can significantly reduce predictive accuracy and operational reliability, highlighting the vulnerability of AI systems to adversarial attacks.

Similarly, concept drift was found to reduce the adaptability of predictive models over time, leading to measurable declines in forecasting accuracy and strategic decision-making capability. In addition, maintaining data integrity remains a persistent challenge, as corrupted or incomplete datasets can amplify the negative effects of data poisoning and drift, ultimately reducing operational efficiency and stakeholder trust.

The study further demonstrates that multi-layered governance frameworks—combining technical safeguards, organizational policies, and regulatory compliance mechanisms—are effective in mitigating these risks. The integration of technical interventions, such as adversarial training, anomaly detection, and privacy-enhancing technologies, with ethical governance and accountability structures can significantly improve the resilience and reliability of AI systems operating in supply chain environments.

5.2 Implications for AI Governance

The implications of this study for AI governance are substantial, emphasizing the need for comprehensive governance frameworks that integrate ethical, technical, and policy dimensions. Robust governance structures are essential to ensure that AI systems remain reliable and trustworthy in dynamic and data-intensive supply chain environments.

The findings highlight that AI governance should not be viewed solely as a compliance requirement but rather as a proactive strategy to address emerging risks such as data poisoning and concept drift while maintaining model integrity and trustworthiness.

Furthermore, organizations should implement continuous monitoring mechanisms, rigorous data auditing processes, and strong ethical oversight structures to maintain accountability and trust throughout AI-driven decision-making processes.

5.3 Recommendations for Practitioners and Future Research

Practitioners should adopt integrated governance models that combine technical, organizational, and policy-level interventions to effectively manage AI-related risks. Advanced mitigation techniques—such as real-time anomaly detection, continuous model retraining, and strict data integrity validation—should be implemented to maintain operational accuracy and system reliability.

In addition, organizations should prioritize staff training, regular audits, and adherence to emerging regulatory frameworks to ensure responsible and trustworthy AI implementation.

Future research should focus on the development of adaptive governance frameworks capable of responding to adversarial attacks and concept drift in real-time environments. Further investigation into AI-specific regulatory standards and automated compliance monitoring tools may also strengthen governance practices. Moreover, empirical studies evaluating the effectiveness of such frameworks across diverse supply chain contexts would provide valuable insights.

Overall, this study contributes to the growing field of AI governance by providing both theoretical and practical insights into the development of resilient, ethical, and trustworthy AI systems capable of maintaining operational integrity in complex and dynamic supply chain ecosystems.

FUNDING STATEMENT

This research received no external funding.

ETHICS STATEMENT

This study is based on literature review and conceptual analysis. No human or animal participants were involved; therefore ethical approval was not required.

DATA AVAILABILITY STATEMENT

All data used in this study are derived from published literature sources cited within the manuscript.

REFERENCE

[1] C. Cath, "Governing artificial intelligence: Ethical, legal and technical opportunities and challenges," *Philosophical Transactions of the Royal Society A*, vol. 376, no. 2133, p. 20180080, 2018.

[2] U. Gasser and V. A. Almeida, "A layered model for AI governance," *IEEE Internet Computing*, vol. 21, no. 6, pp. 58–62, 2017, doi: 10.1109/MIC.2017.4180835.

[3] J. Fjeld, N. Achten, H. Hilligoss, A. Nagy, and M. Srikumar, "Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3518482.

[4] J. Morley, L. Murphy, A. Mishra, I. Joshi, and K. Karpathakis, "Governing data and artificial intelligence for health care: Developing an international understanding," *JMIR Formative Research*, vol. 6, no. 1, p. e31623, 2022, doi: 10.2196/31623.

[5] C. Lahusen, M. Maggetti, and M. Slavkovik, "Trust, trustworthiness and AI governance," *Scientific Reports*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-71761-0.

[6] K. Yeung, A. Howes, and G. Pogrebna, "AI governance by human rights-centred design, deliberation and oversight: An end to ethics washing," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3435011.

[7] M. Aljanabi *et al.*, "Data poisoning: Issues, challenges, and needs," in *IET Conference Proceedings*, 2024, doi: 10.1049/ICP.2024.0951.

[8] K. I. Iyer, "Poisoning AI models: New frontiers in data manipulation attacks," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 11, no. 11, 2023.

[9] N. Lekota, "Governance considerations of adversarial attacks on AI systems," in *Proc. International Conference on AI Research*, vol. 4, no. 1, pp. 227–233, 2024, doi: 10.34190/ICAIR.4.1.3194.

[10] H. Zhang *et al.*, "Practical data poisoning attack against next-item recommendation," in *Proc. The Web Conference*, 2020, pp. 2458–2464, doi: 10.1145/3366423.3379992.

[11] A. E. Cinà *et al.*, "Wild patterns reloaded: A survey of machine learning security against training data poisoning," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–39, 2023.

[12] J. Hausenloy, D. McClements, and M. Thakur, "Towards data governance of frontier AI models," *arXiv preprint*, 2024.

[13] P. Mahendra *et al.*, "A comprehensive review of AI and ML in data governance and data quality," in *Proc. ICICI*, 2025, pp. 1–6.

[14] E. Bluemke, T. Collins, B. Garfinkel, and A. Trask, "Exploring the relevance of data privacy-enhancing technologies for AI governance use cases," *arXiv preprint*, 2023.
[15] S. V. Bayani, S. Prakash, and L. Shanmugam, "Data guardianship: Safeguarding compliance in AI/ML cloud ecosystems," *Journal of Knowledge Learning and Science Technology*, vol. 2, no. 3, pp. 436–456, 2023, doi: 10.60087/jklst.vol2.n3.p456.
[16] M. M. Rahman *et al.*, "Security risk and attacks in AI: A survey of security and privacy," in *Proc. IEEE COMPSAC*, 2023, pp. 1834–1839, doi: 10.1109/COMPSAC57700.2023.00284.
[17] M. T. Hossain *et al.*, "A review on attacks against artificial intelligence and their defence," *Control Systems and Optimization Letters*, vol. 2, no. 1, pp. 52–59, 2024, doi: 10.59247/csol.v2i1.73.
[18] M. K. Pasupuleti, "Securing AI-driven infrastructure: Advanced cybersecurity frameworks for cloud and edge computing environments," 2025, doi: 10.62311/nesx/rrv225.
[19] A. K. Sharma and R. Sharma, "Data governance in the age of artificial intelligence: Challenges, best practices and regulatory compliance," *Applied Marketing Analytics*, vol. 10, no. 4, p. 390, 2025, doi: 10.69554/xwhm1191.
[20] I. M. Leghemo *et al.*, "Data governance for emerging technologies: A conceptual framework for managing blockchain, IoT, and AI," *Journal of Engineering Research and Reports*, vol. 27, no. 1, pp. 247–267, 2025, doi: 10.9734/jerr/2025/v27i11385.
[21] K. Elliott *et al.*, "Towards an equitable digital society: AI and corporate digital responsibility," *Society*, vol. 58, no. 3, pp. 179–188, 2021, doi: 10.1007/s12115-021-00594-8.
[22] N. N. Gupta, "How inadequate data governance frameworks lead to unethical outcomes in artificial intelligence systems," *International Journal of Scientific Research Archive*, vol. 7, no. 1, pp. 580–590, 2022, doi: 10.30574/ijsra.2022.7.1.0274.
[23] J. Woodhams, "Maintaining research integrity when using AI in research," 2025.
[24] R. Nacheva and O. Azeroual, "Security of AI-powered systems: Threat intelligence on the edge," in *Proc. ISMSIT*, 2024, doi: 10.1109/ISMSIT63511.2024.10757185.
[25] R. S. T. Palanichamy, "AI and data governance: Enhancing security, privacy, and accountability," *International Journal of Science and Advanced Technology*, vol. 14, no. 1, 2023, doi: 10.71097/ijsat.v14.i1.2807.
[26] D. Chhillar and R. V. Aguilera, "An eye for artificial intelligence: Insights into the governance of AI and vision for future research," *Business & Society*, vol. 61, no. 5, pp. 1197–1241, 2022, doi: 10.1177/00076503221080959.

AUTHOR BIOGRAPHY

Umamaheswari Shanmugam is an Assistant Professor and researcher affiliated with the Department of Pharmaceutics, JSS College of Pharmacy, JSS Academy of Higher Education & Research, Ooty, The Nilgiris, Tamil Nadu, India. Her area of expertise includes pharmaceutics, clinical research, artificial intelligence in medical devices, and healthcare regulatory science. She is actively engaged in academic research and scientific publications, particularly in the areas of AI as a Medical Device (AIaMD), clinical trial design, and regulatory frameworks for medical technologies. She has contributed significantly to research methodology, data curation, and manuscript preparation. e-mail: uma.maye@gmail.com

Mohan Kumar Rajendran is a researcher and industry professional affiliated with Magnaait Ltd., London, United Kingdom. His area of expertise includes artificial intelligence in healthcare, AI as a medical device (AIaMD), clinical trial design, regulatory science, and post-market surveillance of medical AI systems. He is actively engaged in research and scientific publications focusing on global regulatory frameworks, adaptive AI validation, and the clinical implementation of AI-driven medical technologies. He has contributed as a co-author, reviewer, and validation lead in peer-reviewed medical and regulatory science publications. e-mail: mohan.rajendran@magnaait.co.uk

Jawahar Natarajan is a faculty member and researcher at the Department of Pharmaceutics, JSS College of Pharmacy, JSS Academy of Higher Education & Research, Ooty, The Nilgiris, Tamil Nadu, India. His expertise lies in pharmaceutical sciences, clinical research methodology, medical device regulations, and healthcare innovation. He is actively involved in academic supervision, research guidance, and scientific publications, particularly in the field of AI-based healthcare technologies and regulatory compliance. He has contributed extensively to manuscript review, editing, and research supervision. e-mail: jawahar.n@jssuni.edu.in

Veera Venkata Satyanarayana Reddy Karri is a researcher and academic professional affiliated with the Department of Pharmaceutics, JSS College of Pharmacy, JSS Academy of Higher Education & Research, Ooty, The Nilgiris, Tamil Nadu, India. His area of expertise includes pharmaceutical sciences, medical technology research, artificial intelligence applications in healthcare, and clinical validation studies. He is actively engaged in research and scientific publications related to medical devices, AI-driven clinical systems, and healthcare innovation. He has contributed to scientific review,

editing, and research collaboration in multidisciplinary healthcare studies. e-mail: narayana.reddy@jssuni.edu.in

How to cite:
U. Shanmugam, M.K. Rajendran, J. Natarajan and N.R.K.V.V Satyanarayana, "Data Poisoning, Data Drift, and Data Integrity in Supply Chain Systems: Emerging Threats to AI Governance", *Sistem Pendukung Keputusan dengan Aplikasi*, vol. 5, no. 1, pp. 58-68, March. 2026.