big data and cognitive computing

MDPI

Review

The Importance of AI Data Governance in Large Language Models

Saurabh Pahune [1], Zahid Akhtar [2,*], Venkatesh Mandapati [3] and Kamran Siddique [4]

[1] Cardinal Health, Dublin, OH 43017, USA; saurabh.pahune@cardinalhealth.com
[2] Department of Electrical and Computer Engineering, State University of New York Polytechnic Institute, Utica, NY 13502, USA
[3] FedEx Memphis, Collierville, TN 38017, USA; venkatesh.mandapati@fedex.com
[4] Department of Computer Science and Engineering, University of Alaska Anchorage, Anchorage, AK 99508, USA; ksiddique@alaska.edu
* Correspondence: akhtarz@sunypoly.edu; Tel.: +1-315-792-7238

Abstract: AI data governance is a crucial framework for ensuring that data are utilized in the lifecycle of large language model (LLM) activity, from the development process to the end-to-end testing process, model validation, secure deployment, and operations. This requires the data to be managed responsibly, confidentially, securely, and ethically. The main objective of data governance is to implement a robust and intelligent data governance framework for LLMs, which tends to impact data quality management, the fine-tuning of model performance, biases, data privacy laws, security protocols, ethical AI practices, and regulatory compliance processes in LLMs. Effective data governance steps are important for minimizing data breach activity, enhancing data security, ensuring compliance and regulations, mitigating bias, and establishing clear policies and guidelines. This paper covers the foundation of AI data governance, key components, types of data governance, best practices, case studies, challenges, and future directions of data governance in LLMs. Additionally, we conduct a comprehensive detailed analysis of data governance and how efficient the integration of AI data governance must be for LLMs to gain a trustable approach for the end user. Finally, we provide deeper insights into the comprehensive exploration of the relevance of the data governance framework to the current landscape of LLMs in the healthcare, pharmaceutical, finance, supply chain management, and cybersecurity sectors and address the essential roles to take advantage of the approach of data governance frameworks and their effectiveness and limitations.

Keywords: large language models (LLMs); data governance framework; data privacy laws; data quality management; fine-tuning; model validation; secure deployment; security protocols; ethical AI practices; healthcare; pharmaceutical; finance; supply chain management; cybersecurity

check for updates

Academic Editor: Domenico Ursino

Received: 31 March 2025
Revised: 19 May 2025
Accepted: 22 May 2025
Published: 28 May 2025

Citation: Pahune, S.; Akhtar, Z.; Mandapati, V.; Siddique, K. The Importance of AI Data Governance in Large Language Models. *Big Data Cogn. Comput.* **2025**, *9*, 147. https://doi.org/10.3390/bdcc9060147

1. Introduction

As a current trend, large language models such as GPT-3 and GPT-4 in software development cycles are widely used for different task activities, such as responding to complex queries and writing and interpreting code [1]. The impact of current LLM trends, nowadays in customer service chat, is gaining momentum across various industries such as e-commerce, finance, healthcare, and travel sectors [2,3]. LLM breakthroughs are rapidly advancing medical artificial intelligence, which are advancing trends in the medical domain [4] and enhance the examination of medical records by managing massive amounts of medical data [5,6] (e.g., unstructured clinical notes, diverse data types of medical images, hospital guides, telehealth, and electronic health records (EHRs)). The LLM integration approach (GPT-4 and BERT) in the medical system handles a large amount of healthcare data and improves patient care outcomes, diagnosis, treatment, and clinical support [7]. In this context, various types of clinical and biomedical specialized LLMs and multimodal LLMs [8] are present to improve the quality of healthcare, such as ClinicalBERT [9], BioBERT [10], PathologyBERT [11], and Med42-v2 [12].

Meanwhile, the evolution of LLMs across many industries is gaining importance, such as in the financial sector where there are various financial-based LLMs present to handle the complexities of financial tasks, such as BloombergGPT [13], FinBERT [14], and FinGPT [15], which need a large amount of data and benchmarks to train with a powerful infrastructure. There are studies that highlight LLM-based financial sentiment analysis (FSA) built on LLaMA2 [16], a synthesized LLM multiagent system [17], and the multi-document financial question and answer [18], which improves the completion of complex financial tasks. Studies have also demonstrated that LLMs focus on the travel mode choice task (TourLLM [19] and Tourism Recommender Systems (TRS) using an LLM-based RAG pipeline [20]), designed to improve travel choice modeling, enhance general public transport services, and forecast tasks related to human mobility and traffic [21–24]. However, while LLMs offer reasonable explanations and predictions, there are instances where they may hallucinate and violate logical consistency, particularly in personalized travel suggestions, which can impact the fairness of travel planning recommendations. To overcome challenges in various domains (finance [25–27], healthcare [28,29], and e-commerce [30,31]), the fairness of techniques, policy guidelines, and data security are the must-have priorities required as part of data governance technologies in LLMs.

1.1. How Are Data Crucial to Build LLM Performance?

Data are a fundamental and crucial component in training the millions or billions of parameters of LLMs to evaluate their performance. A recent study by Yin et al. [32] concluded that selecting the right data for training LLMs (redundancy, contradiction, and prioritizing data subsets with a low compression ratio) plays a vital role in improving model performance. The study by Kumar et al. emphasizes [33] the importance of high-quality data preparations (deduplications on crawl data) and that effective tokenization optimization strategies play an important role in Indic LLM performance. Keer et al. [34] introduce DataSculpt, a novel data management framework for long-context training data to enhance model performance (scalability and flexibility in training) and effective data management. Choe et al. [35] developed a popular gradient-based data valuation method to enhance the scalability of the data valuation process in LLMs. Jiao et al. [36] enhance the open-source PandaLLM with the use of an instruction-tuning approach based on training data factors (quantity, quality, and linguistic distribution) that affect model training. The article [37] proposed the importance of synthetic data generation that fills the gaps after LLM post-training, which tends to contribute to the better performance of LLMs. Wood et al. [38] introduce the Data Prep Kit (DPK) toolkit, built for data preparation for LLMs that enhances the performance of fine-tuning models using RAG.

In order to build and improve the performance of LLMs, data are an essential component throughout the lifecycle process. But problems like hallucinations, driven by factors like data misuse, data breaches, improper data for training (redundancy in data, biasness in data (e.g., cultural biases), and data security issues) are common challenges in modern LLMs. As a result of these difficulties, LLM performance and reliability are significantly impacted. Hence, a robust data governance system based on artificial intelligence (AI) is necessary to solve these problems. Listed below are the most important issues and consequences that could arise from not having a strong data governance structure in place for LLMs. In this paper, we leverage the framework and concepts of data governance that play a vital role in LLMs:

- The main issues in the absence of strong data governance in LLMs are "Hallucination" while performing the output response based on the input query.
- The other vital issue is "Data misuse", which creates a big issue due to ethical violations (unclear and unauthorized data usage policies).
- "Biasness in data" is a major concern that leads to creating biased approaches in LLMs.
- A lack of a data governance framework leads to "Data breach and lack of data security (security concern)" activity, which increases the risk of various adversarial attacks (backdoor attacks, data poisoning attacks, model inversion attacks, transfer-based black box attacks, etc.).
- Also, it impacts "Ethical implications and legal concerns" in LLMs due to the lack of data governance frameworks.
- The failure of LLMs, while deploying in a production pipeline, requires a strong LLMOps pipeline with the assistance of a solid data governance approach.

Avoiding data misuse, a biased nature, hallucinations, deployment issues, a lack of data security, ethical challenges, and misinformation tends to require strong regulatory compliance, guidelines, and robust data governance frameworks that we define in the following sections in detail for the use of solid data governance framework and its impacts on the performance and validation of LLMs.

1.2. Addressing Data Misuse, Biases, and Ethical Challenges in the Digital Era of LLMs

The emergence of LLMs in this digital era of the current world marks a transformative shift in automation in various domains (healthcare, financial, e-commerce, and others), and the generation of the output response based on text, image, video, and audio is fascinating and unimaginable. However, this digital era of LLMs has potential challenges in terms of data misuse, biases, and ethical challenges. Addressing critical issues and understanding the various factors and the implementation of robust data governance frameworks are crucial steps. Hence, given below are the impacted behaviors of LLMs that need to be enhanced and provide a more potential solution for the foundation of the data governance framework mentioned in Table 1.

Table 1. Impacted behavior and challenges of LLMs due to lack of data governance framework.

Application	References
(Cultural, algorithmic) biases in LLMs	[39–41]
Data privacy and security concerns	[42–44]
Hallucination in LLMs	[45–48]
Ethical implications and misinformation	[49–51]
Failure deployment of LLMs	[52–55]
Regulatory compliance and legal concerns	[56–58]
Unintended destructive outputs	[59–61]
Lack of data validation and data quality control	[62–65]
Data evolution and drift create a lack of performance	[66–69]

1.3. Problem Statement

Unregulated data practice flows and inadequate governance frameworks with newly discovered technologies across various sectors such as healthcare, finance, education, and others by leveraging LLMs create a risk factor. Hence, an effective data governance system plays a vital role.

The absence of data governance in healthcare creates a larger privacy and security issue (unauthorized access to patient information, non-compliance, and regulation). Due to the absence of data governance, this mismanagement can have an impact on financial loss, patient safety, and legal liabilities, and without structured policies, there is a large risk of data misuse [42,43]. This paper discussed hallucination detection in LLMs, a problem that often arises due to the absence of data governance, resulting in insufficient data quality control during LLM training and evaluation [45]. The lack of data governance frameworks in LLMs, which causes an issue with the unintended destructive output generation of LLMs called data dysphoria (due to poor data quality and validity) [59], and a lack of defining clear policies and defined roles can result in a mismanagement of data assets (such as data integrity, data quality, and data security) [62]. Regulatory compliance is a crucial step, as formal requirements for data storage, data sharing, and data collection with the absence of data governance frameworks can lead to legal and ethical sequences [70] and organization struggle to meet regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), which are requirements for data privacy in Information Technology (IT) audits [58]. The scalable and flexible governance model adapts regulations like the GDPR and CCPA. It is best practice to adapt the framework to protect safe data and resources in a cloud environment [71]. The author discussed data contamination occurring in LLMs that affects the overestimation of model performance and the importance of the data governance framework that encourages the detection of this problem using audit tools (to detect and address data contamination) [72]. The article [73] presented a detailed review of key challenges in LLMs such as misleading information, duplication of content, and personal information through the web-mined corpus. It requires a proper methodology (e.g., data cleaning and bias detection) to mitigate the issues in LLMs. The paper [74] focuses on the urgent need to provide a solid dynamic auditing system, which requires transparency in the implementation of the LLM as it's a crucial step for distinct ethical challenges (privacy and fairness, hallucination, verifiable accountability, and decoding censorship complexity in LLMs). The article [75] focuses on securing LLMs as the most vital step to avoid prompt attacks (e.g., jailbreak attacks and adversarial attacks as a prompt injection) and focuses on accuracy and bias issues. As they are growing impressively across various fields, a defense mechanism and safeguarding are needed.

1.4. Objectives of the Survey

AI-driven data governance is a robust framework that involves various policies, regulatory and compliance monitoring, and standard practices to ensure responsibility for the development of AI (basically from the initial phase to the end phase) until the implementation of the cycle. Figure 1 describes the essential key pillars of AI data governance for LLMs. It encompasses the management of data for quality control and data privacy, regulatory compliance, the mitigation of biases, risk for the successful deployment of LLMs, ethical challenges, and security and privacy concerns. Hence, these five key main things are needed for effective AI data governance for large language models (LLMs) to work well. The mitigation of bias and fairness ensures that the data and results are equal for all groups of people (which builds trust in AI systems and helps with laws and rules against discrimination, which assists with a trustworthy AI framework). When an ethical model is deployed, clear rules are established to prevent misuse and stop mistreatment, ensuring the system comes with built-in rules and safety features that make sure it is used correctly and keep users safe from harm, bias, or unfair treatment (e.g., maintaining faith in the technology, keeping patients safe from inadequate output, and preventing biased or unfair diagnoses are essential steps in robust data governance). Security and privacy methods protect private data throughout the lifecycle of the model by allowing continuous monitoring and auditing, ensuring safe data storage, and stopping data leaks. Data validation and quality control ensure that they are correct and consistent, and legal compliance and data sourcing ensure that licensing and government standards are met. All of these five factors of the pillars work together to support responsible and trustworthy LLM growth.

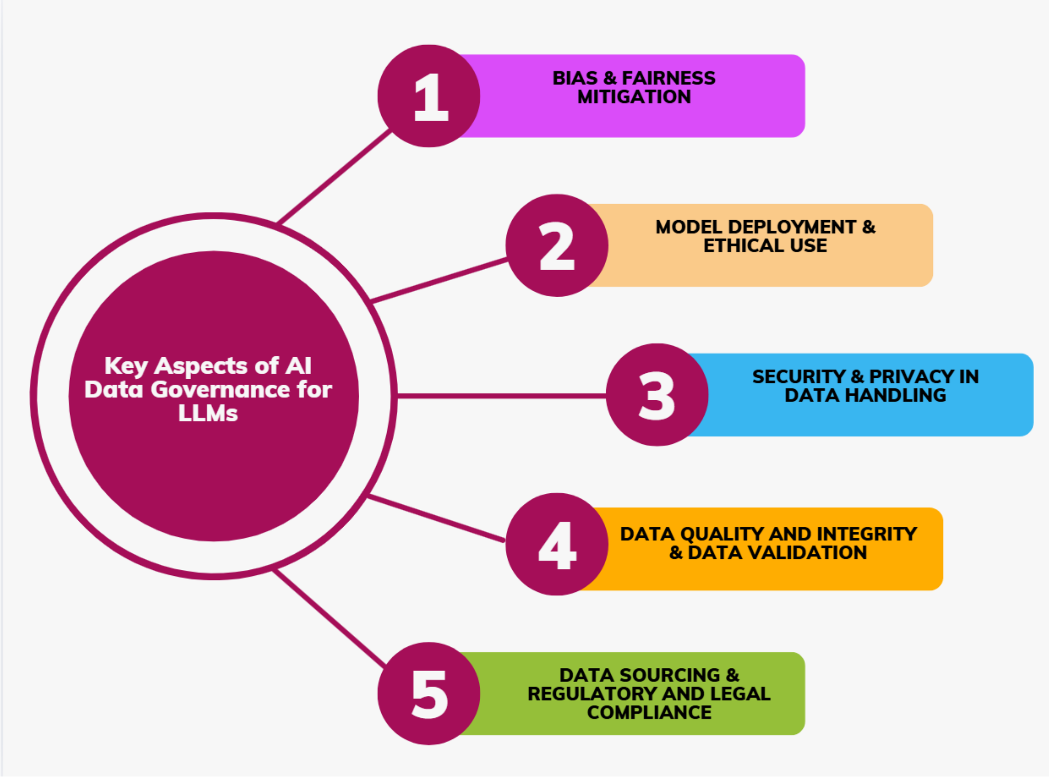
Key Aspects of AI Data Governance for LLMs
1
BIAS & FAIRNESS MITIGATION
2
MODEL DEPLOYMENT & ETHICAL USE
3
SECURITY & PRIVACY IN DATA HANDLING
4
DATA QUALITY AND INTEGRITY & DATA VALIDATION
5
DATA SOURCING & REGULATORY AND LEGAL COMPLIANCE

Figure 1. Essential key pillars of AI data governance for LLMs.

A list of various key aspects that leverage AI-driven data governance that involves LLMs is mentioned below. Uses in various sectors like healthcare, finance, e-commerce, and travel are given below, where it is essential to use this methodology:

- One paper proposed the use of an AI data governance framework in the context of LLMs to improve the detection of suspicious transactions (money laundering and anomaly detection in financial transactions) [76].
- The use of an AI-driven intelligent data framework that substantially improves operational efficiency, compliance accuracy, and data integrity for the future development of AI-based work [77].
- One author provides a critique of the use of centering the implementation of AI data governance in LLMs, which is more effective for model performance [78].
- One study recommends the use of a robust data governance framework in the AI-enabled healthcare system, which addresses ethical challenges and privacy concerns (builds trust among users of healthcare services) [79].
- The use of AI data governance frameworks automates the process of managing data quality in the banking sector to improve model performance [80].
- The use of data-centric governance throughout the model learning lifecycle, responsible for the deployment of an AI system which reduces the risk of deployment failure, reduces the deployment process, and increases the solution design approach [81].

- The integration of an AI-driven data governance framework with a banking system that enhances data accurately, reliably, and securely, which creates trust and accountability in the financial sector [82].
- As AI is evolving very rapidly in daily life, lots of manual tasks are being reduced due to automation capabilities. Therefore, trust in the AI system is needed, which needs to be addressed through co-governance implementation techniques such as regulation, standards, and principles. The use of data governance frameworks improves AI maturity [83].

As AI is rapidly evolving a wide range of applications, a trustable AI approach needs to be established to have a secure and efficient approach. Hence, the integration of an intelligent data governance framework approach is needed that leverages many aspects such as the security and privacy data handling process, bias and fairness mitigation, regulator and legal compliance, and safeguarding an ethical approach. The scope of AI data governance is examined through various main elements outlined in Table 2.

Table 2. Scope of AI data governance.

Aspect	Description
Data lifecycle management	Use of intelligent data governance across the AI model throughout the end-to-end lifecycle from development phase to end of deployment phase.
Regulatory compliance and legal frameworks	The scalable and flexible governance model adapts the global regulation like GDPR, CCAA, HIPAA, AI Act, and AIRMF.
Ethical and fair AI practices	The implementation of AI data governance ensures that AI models and systems operate with transparency and fairness without any discriminatory metrics (e.g., regardless of race, gender, religion, age, and others).
Data privacy and security	The implementation of an intelligence of data governance leverages the data privacy and encrypted mechanism to mitigate data breach activity. Also prevents various cyber threats and several attacks (e.g., adversarial, model inversion, inference, data poisoning, and others).
Data quality, integrity, and validation	Data quality, integrity, and validation are essential elements of data governance. These three factors directly impact the quality of trustworthiness in AI models.
Data lineage and traceability	Data lineage and traceability are the vital components of data governance methodology, which assist auditors in tracing data usage and assist with debugging the issue for root cause analysis.
More secure end-to-end model deployment	The use of this data governance approach assists with secure and confident deployment of AI model via various pipelines (DevOps, MLOps, and LLMOps) from initial phase, robust model training, testing and validation, deployment phase, and post-deployment phase.

As illustrated in Figure 2, this paper explores several core areas of AI data governance in LLMs, including data sourcing, privacy, fairness, accountability, and regulatory frameworks. The remainder of this article is structured as follows: Section 2 presents the foundations of AI data governance. In Section 3, the AI data governance methodology is discussed in various domains. Section 4 gives challenges in data governance for LLMs. Section 5 provides key components of data governance, and regulatory and ethical considerations are discussed. Section 6 outlines best practices for the AI data governance methodology. Section 7 describes case studies on the implementation of data governance in LLMs. Section 8 presents open issues and future directions, emerging technologies, and interdisciplinary research to address AI governance. The conclusions are described in Section 9.

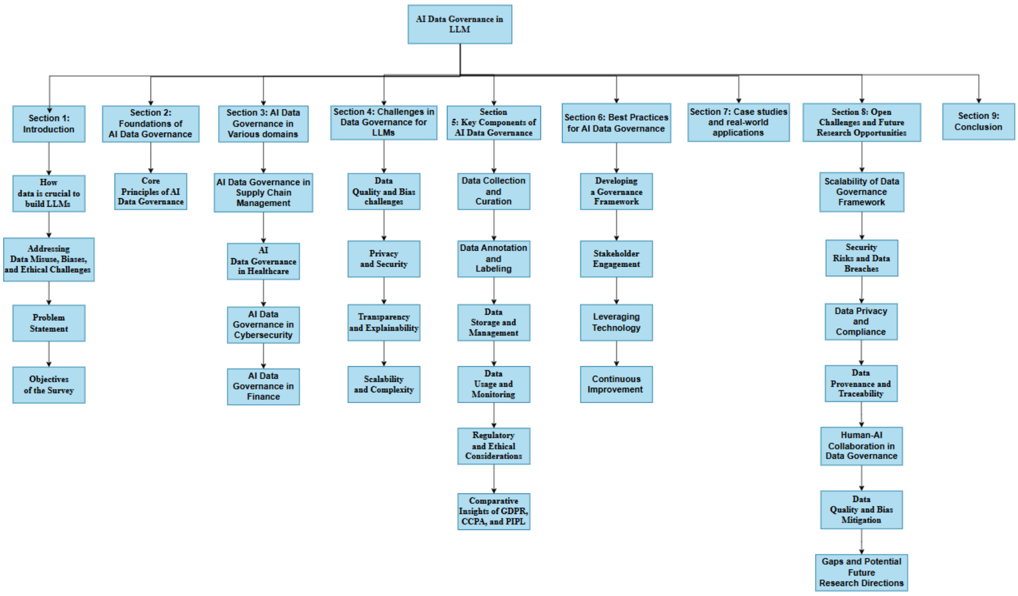
AI Data Governance in LLM
Section 1: Introduction
How data is crucial to build LLMs
Addressing Data Misuse, Biases, and Ethical Challenges
Problem Statement
Objectives of the Survey
Section 2: Foundations of AI Data Governance
Core Principles of AI Data Governance
Section 3: AI Data Governance in Various domains
AI Data Governance in Supply Chain Management
AI Data Governance in Healthcare
AI Data Governance in Cybersecurity
AI Data Governance in Finance
Section 4: Challenges in Data Governance for LLMs
Data Quality and Bias challenges
Privacy and Security
Transparency and Explainability
Scalability and Complexity
Section 5: Key Components of AI Data Governance
Data Collection and Curation
Data Annotation and Labeling
Data Storage and Management
Data Usage and Monitoring
Regulatory and Ethical Considerations
Comparative Insights of GDPR, CCPA, and PIPL
Section 6: Best Practices for AI Data Governance
Developing a Governance Framework
Stakeholder Engagement
Leveraging Technology
Continuous Improvement
Section 7: Case studies and real-world applications
Section 8: Open Challenges and Future Research Opportunities
Scalability of Data Governance Framework
Security Risks and Data Breaches
Data Privacy and Compliance
Data Provenance and Traceability
Human-AI Collaboration in Data Governance
Data Quality and Bias Mitigation
Gaps and Potential Future Research Directions
Section 9: Conclusion

Figure 2. A comprehensive overview of AI data governance in LLMs.

2. Foundations of AI Data Governance

The foundations of AI data governance frameworks are the most crucial steps in the digital era of AI during the building of a model. These steps are a core part of the process to ensure the responsible development and management of the AI model lifecycle. The focus of model building using the data-centric governance approach develops the dynamic capabilities to adapt technology advancement in a more secure and flexible way. In addition, it makes AI systems ethical and effective for legal compliance and regulatory processes. Nowadays, building an LLM-based application to gain trustworthiness, secure data, obtain ethical and fair answers, and prevent various attacks is needed.

There are various frameworks of AI data governance categorized as data-centric AI governance, policy-driven AI governance, model-centric AI governance, regulatory-compliance AI governance, risk-based AI governance, ethical AI governance, security focus, industry-specific, and federated AI governance. Each governance type implementation is applied according to the scope of the process, the development of the model, and the technical requirements of the design. As shown in Figure 3 mentioned in the following, the model is related to various types of AI data governance categorizations, whereas Table 3 outlines the detailed key aspects of various types of AI data governance.

Table 3. Types of AI data governance, focus, and key aspects for LLMs.

Types of AI Governance	Focus	Key Aspects	References
Policy-driven governance	Regulations and compliance: focus on various policies and data protection law	GDPR, HIPAA, AI Act, and CCPA	[84,85]
Data-centric governance	Data quality and integrity: ensure data fairness, accuracy, and bias mitigation approach	Master data management, data encryption, and third-party data sharing policies	[78,81,86]
Model-centric governance	Model explainability: focus on model's lifecycle from initial phase to secure deployment phase	Model lifecycle management (MLOps and LLMOps) and model performance and accuracy	[86–88]
Risk-based governance	AI risk management: identifies potential AI risk (e.g., algorithmic bias, data privacy breaches, and security vulnerabilities) and applies data governance controls	Financial and operational risk, security and cyber risk management, and algorithmic risk management	[89,90]

Table 3. *Cont.*

Types of AI governance	Focus	Key Aspects	References
Federated AI governance	Decentralized AI systems: AI model training with secure confidential data (e.g., train AI model without sharing confidential patient data)	Decentralized model governance and accountability, security and trust in federated systems, and decentralized model governance and accountability	[91,92]
Regulatory-compliance governance	Adherence to laws: ensure models do not break rights, privacy, and laws	Healthcare AI must comply with HIPAA regulations	[93,94]
Ethical AI governance	Fairness and bias prevention: identifies biased, unfair, and other discriminatory metrics	Transparency and explainability, ethical guidelines and frameworks (e.g., OECD AI principles), and safety and robustness	[95,96]
Security-focused governance	AI cybersecurity and attacks: to prevent models from experiencing various attacks (e.g., model inversion and prompt injection)	Model security and integrity, Cybersecurity Act (e.g., NIST and ENISA), and secure AI model development and post-deployment security	[97–100]
Industry-specific governance	Domain-based AI rules: ensure compliance is aligned with domain-specific regulation (e.g., pharma and healthcare domain)	AI-driven drug discovery follows FDA, healthcare AI must go with HIPAA, and finance with GDPR regulation	[101–103]

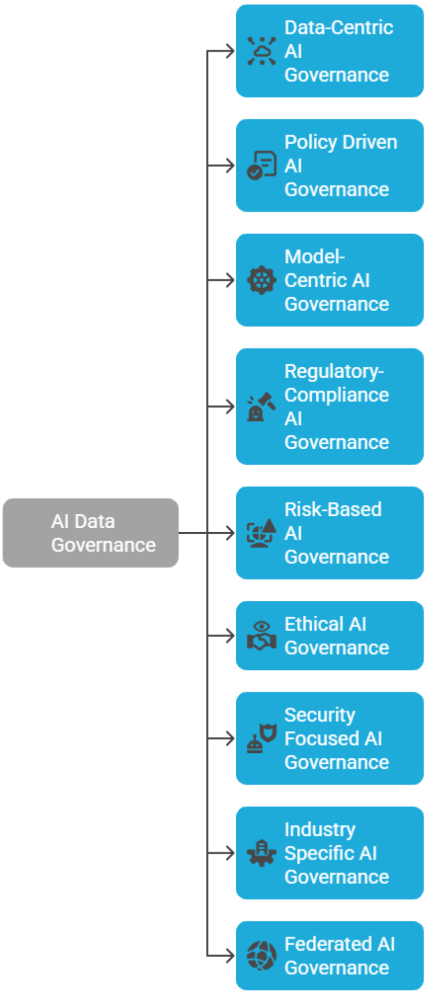
AI Data Governance
Data-Centric AI Governance
Policy Driven AI Governance
Model-Centric AI Governance
Regulatory-Compliance AI Governance
Risk-Based AI Governance
Ethical AI Governance
Security Focused AI Governance
Industry Specific AI Governance
Federated AI Governance

Figure 3. Types of AI data governance frameworks.

2.1. Core Principles of AI Data Governance Relevance to LLMs

As LLMs are widely used in various domains (e.g., healthcare and pharmaceutical [104–106], by analyzing and training a large number of clinical datasets, a genomic analysis of biological data, reshaping molecular biology, and drug development are possible. ShennongGPT [107] is trained in a distilled drug database and makes human-like decisions to personalize drug advice and prevent adverse drug reactions in patients. Overall, LLMs in the healthcare sector must avoid biases and inaccuracies in generated output, enhance data security, and cover privacy concerns (e.g., patient data privacy), so the robustness of AI data governance is needed to understand the capabilities and limitations of the models in healthcare applications.

In finance [108–110], by contrast, LLMs are reshaping financial market analysis, risk assessments, and investment decision making based on vast amounts of financial data (e.g., FinLLM [111], KemenkeuGPT [112], BloombergGPT [13], and FinGPT [15]). In addition to cybersecurity [113–116], they are providing cyber threat intelligence (CTI) analysis, the ability to automate threat detection, the ability to mitigate approaches to random threats, and vulnerability assessments. However, future research is needed to safeguard data, ensure social ethics, ensure robust encryption, and enhance authentication methods and legal norms to defend LLMs against adversarial attacks and perform token manipulation [117,118]. Currently, the benefits of the integration of the AI data governance approach are of great importance for security and reliability against malicious activities in LLMs.

The use of LLMs in supply chain management and the integration of data governance significantly impact business operations (e.g., inventory management, supply chain optimization, avoiding supply chain risk, early detection of vulnerabilities in software supply chains, automating contract renewal, etc.) [119–121]. In personalizing recommendations and enhancing the ability to work on a large-scale, multidimensional dataset (e.g., e-commerce chatbots [122–124] for personalized recommendations based on users' historical data and a conversational recommender system (CRS) [125]), education is transforming the new digital era via an intelligent tutoring system by us for LLMs [126–128] as well as several areas that effectively shape industry operations. Hence, the role of AI data governance is the crucial step in creating an AI model that is used to train LLMs with billions/millions of parameters, which is responsible for creating various content generation outputs such as text-to-multimedia content generation [129,130] that encompasses various outputs (image-to-video, video-to-image, audio-to-image, or cross model content generation). To obtain refined LLM outputs, it needs fairness, reliability, transparency, compliance, trustworthiness, unbias, safety, the prevention of adversarial threats, and alignment with ethical AI standards.

Therefore, effective integrations of AI data governance frameworks are needed to mitigate risks. The main core principles of AI data governance are listed below, which are key parts of the process to ensure that LLMs gain the ability to build the trust of the end user with the AI-driven decision-making process.

2.2. Core Principles of AI Data Governance

Figure 4 provides an overview of various core principles of AI data governance that set standards throughout the data lifecycle to ethically build and deploy large language models. Accurate, complete, and consistent training data and impartial outcomes require data quality and integrity, whereas data management follows fairness and ethical AI principles to minimize discrimination and promote transparent, equitable model behavior. The GDPR and HIPAA require encryption, confidentiality, and access limits to protect sensitive data. Data governance prevents the misuse and degradation of LLMs through performance tracking, auditing, and human-in-the-loop techniques. Regulatory and compliance concepts integrate legal, industry, and ethical norms to reduce risk and promote accountability. Finally, data lineage and traceability demonstrate how data flow and impact outputs, providing explainability, debugging, and confidence. These six core principles enable safe, fair, and reliable LLM systems. The details of various components are mentioned below.

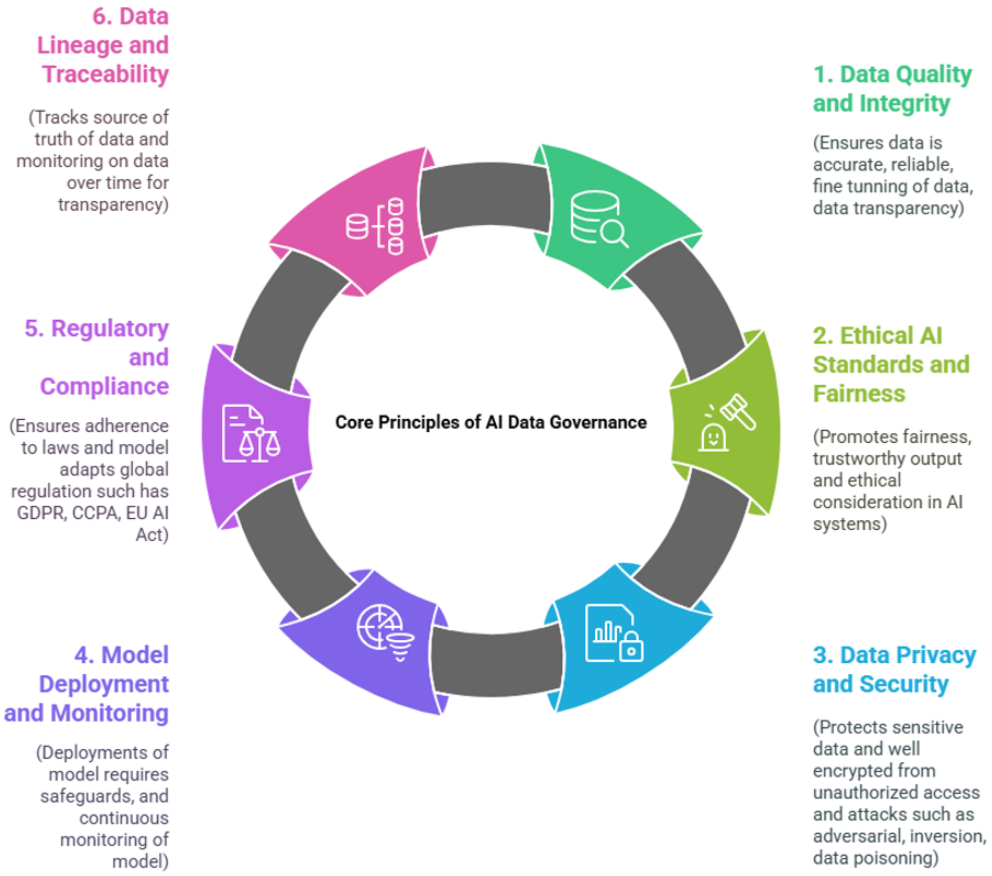
6. Data Lineage and Traceability
(Tracks source of truth of data and monitoring on data over time for transparency)
1. Data Quality and Integrity
(Ensures data is accurate, reliable, fine tunning of data, data transparency)
5. Regulatory and Compliance
(Ensures adherence to laws and model adapts global regulation such has GDPR, CCPA, EU AI Act)
Core Principles of AI Data Governance
2. Ethical AI Standards and Fairness
(Promotes fairness, trustworthy output and ethical consideration in AI systems)
4. Model Deployment and Monitoring
(Deployments of model requires safeguards, and continuous monitoring of model)
3. Data Privacy and Security
(Protects sensitive data and well encrypted from unauthorized access and attacks such as adversarial, inversion, data poisoning)

Figure 4. The foundation of trustworthy LLMs: six core AI data governance principles.

2.2.1. Data Quality and Integrity

Data quality is critical for a reliable LLM performance. For training corpora, Yao et al. [131] proposed methods that can mitigate the undesired data properties during the generation, cleaning, and training of the data to improve the data quality for LLMs. One of the key aspects of a large language model is pre-training on vast data and subsequent fine-tuning tailored to the specific domains and industries by using specialized training datasets that can improve the data quality, which can mitigate problems like hallucinations and data inconsistency, which can ultimately increase trust in the LLM outputs. The paper by Nazi and Peng [132] mentioned pre-training the model on diverse datasets, which will enable the model to acquire knowledge from a broad spectrum of linguistic instances. Within healthcare settings, data quality is imperative to develop evaluation frameworks. Some models are not publicly available, and this can possibly give rise to data transparency issues, which is a crucial factor in the healthcare domain and which can hinder the process of thoroughly examining the data quality and integrity while examining the results of the model.

2.2.2. Ethical AI Standards and Fairness

LLM development is going through a rapid transformation and is showing great signs of great potential for various applications in all industries. However, it also comes with substantial associated risks, including ethical standards and intellectual property [133].

LLMs can be biased based on their training data, which raises ethical concerns. Carefully documented datasets can increase ethical AI standards and fairness rather than simply ingesting everything on the Internet into the model. It is likely that there is already misinformation on the Internet, and this can be reinforced if we do not set ethical standards. Using alignment techniques, Liu et al. [134] mentioned that LLMs can be more reliable, safe, fair, and attuned to human values that will foster greater trust among their users. Notable general guidelines, namely the "HHH" principle, advocate alignment that is helpful, honest, and harmless.

2.2.3. Data Privacy and Security

If the LLMs are trained with user personal information and proprietary data (name, emails, phone numbers, etc.), there is a risk of exposing or leaking those data. Without safeguards, LLMs can inadvertently violate data confidentiality. To protect sensitive data, the model can be trained on decentralized data sources (user devices, private servers, etc.) where the raw data do not leave their source. Carlini et al. [135] shared how LLMs are vulnerable to numerous privacy attacks if they are not trained in privacy-preserving algorithms. Training data extraction attacks have been limited to small LLMs under artificial training setups or in cases where the adversary has prior knowledge of the data they want to extract. Pan et al. [136] observed that general-purpose language models tend to capture sensitive information in sentence embeddings, which can lead to a data breach by the adversary. If the adversary can access it, they can reverse engineer it to disclose sensitive information.

2.2.4. Model Deployment and Monitoring

Especially in the framework of machine learning (ML) systems, model deployment and monitoring are essential elements of data governance. Once LLM training is concluded, deploying the model in real life requires several safeguards. LLMs are discovered to be vulnerable to prompt injection assaults, and there is a need for continuous evaluation throughout the LLM lifecycle using the integration of LLMOps and MLOps with a data governance approach [52,137]. One study suggests using an MLOps pipeline to automatically set up machine learning models and keep an eye on certain measures to make sure that predictions are very accurate. It focuses on constant improvement by using automatic model management and changing based on new data. Adding AutoML makes tracking the speed even easier and helps with ongoing system optimization [138]. Multidimensional evaluation techniques must be used to measure technical performance, data privacy, input stability, calibration, and output alignment, and to find out about possible restrictions and how to meet legal requirements and compliance [139].

One paper discusses MLOps as a way to set up and keep an eye on machine learning models automatically. It talks about how important it is to keep an eye on things throughout the development process and to connect the development and production environments [140]. Another study focuses on a complete model monitoring framework that uses Grafana (analyzes data from various sources across various domains [141]) and Dynatrace (a real-time software intelligence platform that detects model drifts, data quality issues [142]) to ensure that ML models work well, keep an eye on KPIs, find problems, and control model drift. This improves data governance and reliability in machine learning applications that are currently in use, thus improving the trustworthiness of the model [143].

2.2.5. Regulatory and Compliance

The GDPR, CCPA, LGPD (Brazil's general data protection law), and HIPAA are very strict laws on data safety (ensuring data safety, data integrity, and privacy and security regarding data access [144,145]). Data governance is a key part of making sure that regulatory and compliance rules are followed. Companies need strong governance systems to protect private data and handle compliance risks as they rely more on data-driven strategies.

There are strict rules about data privacy for LLMs because they might have access to personal information. Hence, worldwide practice regulations are being used; examples are the GDPR (General Data Protection Regulation) and California Consumer Privacy Act (CCPA) regulations imposed to meet the requirements for ML models. Users must agree to the use of their personal data, have the right to have them deleted, and be aware of how LLMs use their data to follow the rules (MemoAnalyzer in LLMs enables the user to delete and modify sensitive information, leading to increased user awareness [146]). Data privacy rules are being pushed to their limits by the speed with which LLMs are being built. Information about people who can be identified (PII) is used to train the LLM (the adaptive PII framework can be used for LLMs to mitigate the risk of personal identifiable information to meet with compliance [147]). If the right security measures are not in place, these data could be memorized and private information could be shared (hence, control over memory management in LLMs is essential to modify and delete sensitive information as an essential part to be added in data governance work).

2.2.6. Data Lineage and Traceability

Data lineage and traceability are critical components of data governance to be able to track and trace the flow of data movement and closely monitor the source of the truth of data from various sources throughout the data management lifecycle process. Hence, leveraging the data lineage traceability approach inside the data governance framework assists the organization in meeting regulatory requirements.

A lack of data lineage, a lack of knowledge of exactly the sources of the training data, and various other scenarios could make it difficult to address any problem. One method is to apply IDs or hashes to the data samples for dataset training for data traceability (HashGraph [148]). The adoption of a new data version and control systems would be helpful in tracking the state of the dataset and documenting changes [149]. Mirchandani et al. [150] assessed LLMs as pattern machines that are categorized into three areas: sequence transformation, sequence completion, and sequence improvement. If an LLM produces an inappropriate output, the lineage tools can trace it back to the training data, and the lineage also supports attribution, which can give credit to its contributors. Chen et al. [151] mentioned that keeping track of the data is essential for data flow vision; hence, the use of data lineage graphs (DLGs) makes it easy to see all the data assets and how they are connected. DLGs can learn new skills that help them better handle data and come up with new business ideas. Hence, DLGs are an essential part to integrate into the data governance framework to track and trace data flow.

3. Use of AI Data Governance in Various Domains

Figure 5 illustrates that the use of an implementation of AI data governance is crucial across multiple sectors, including supply chain management, cybersecurity, healthcare, and finance, to maintain data integrity, security, and compliance. The governance framework ensures that AI systems operate in compliance with regulatory standards, maintain data privacy, and safeguard sensitive information while improving decision-making capabilities. Implementing data governance principles enables firms to achieve dependable and transparent AI outcomes, fostering responsibility and reducing risks, and below are the detailed subsections for various domains.

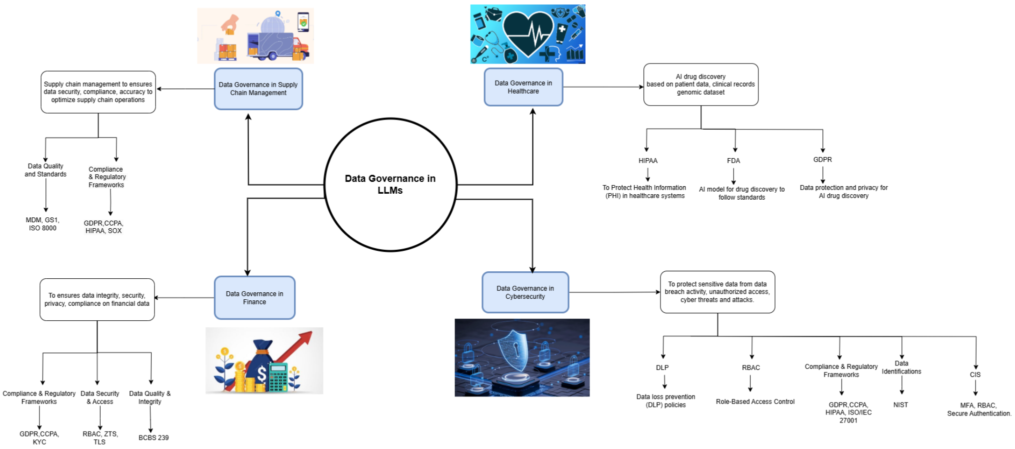
Data Governance in LLMs
Data Governance in Supply Chain Management
Supply chain management to ensures data security, compliance, accuracy to optimize supply chain operations
Data Quality and Standards
Compliance & Regulatory Frameworks
MDM, GS1, ISO 8000
GDPR,CCPA, HIPAA, SOX
Data Governance in Finance
To ensures data integrity, security, privacy, compliance on financial data
Compliance & Regulatory Frameworks
Data Security & Access
Data Quality & Integrity
GDPR,CCPA, KYC
RBAC, ZTS, TLS
BCBS 239
Data Governance in Healthcare
AI drug discovery based on patient data, clinical records genomic dataset
HIPAA
FDA
GDPR
To Protect Health Information (PHI) in healthcare systems
AI model for drug discovery to follow standards
Data protection and privacy for AI drug discovery
Data Governance in Cybersecurity
To protect sensitive data from data breach activity, unauthorized access, cyber threats and attacks.
DLP
RBAC
Compliance & Regulatory Frameworks
Data Identifications
CIS
Data loss prevention (DLP) policies
Role-Based Access Control
GDPR,CCPA, HIPAA, ISO/IEC 27001
NIST
MFA, RBAC, Secure Authentication.

Figure 5. Data governance in various domains.

3.1. *AI Data Governance in Supply Chain Management*

Organizations are progressively adopting AI technologies, making AI data governance in supply chain management essential for ensuring compliance, accountability, and efficiency. This paper proposes the implementation of AI data governance in supply chain management to mitigate compliance risks. It requires a comprehensive strategy that assesses risks throughout the AI implementation process of the robust framework, thus guaranteeing adherence to data privacy laws and the preservation of quality and safety standards [152]. One study proposes a regulatory framework for AI data governance in the supply chain that is intended to mitigate vulnerabilities in the AI data supply chain. In order to improve transparency, accountability, and safety, this framework prioritizes mechanisms such as mandatory reporting, KYC regulations, and dataset verification [153]. Another article introduces a "Data Bill of Materials" (DataBOM) to enhance AI data governance in supply chains by ensuring traceability, verifiability, and reproducibility through blockchain technology. This method addresses the challenges of accountability among a variety of stakeholders in the field of data management [154]. Robust data governance is essential for the successful incorporation of AI and machine learning in supply chain management. It ensures data quality, addresses ethical concerns such as privacy and bias, and enables scalable solutions, therefore improving efficiency and sustainability in supply chain operations [155].

3.2. *AI Data Governance in Healthcare*

As AI technologies progress rapidly, the need for robust governance structures is crucial to ensure patient safety, data privacy, and accountability. A wide variety of frameworks and approaches have been proposed to address these challenges, highlighting the need for tailored tactics for various healthcare settings. One article outlines seven critical areas of AI governance in healthcare, including organizational structure and external product assessment, and presents the AI governance readiness assessment of healthcare (HAIRA) to help organizations assess and improve their AI governance capabilities based on available resources [156]. The governance of AI data in healthcare is crucial for addressing ethical and regulatory issues. It ensures the proper, ethical, and secure use of AI tools, promoting equity, fairness, inclusion, and accountability while safeguarding human dignity and fundamental rights in healthcare services [157]. One study analyzed the imperative for an AI governance framework in healthcare to address the challenges in the installation and acceptance of AI systems, ensuring the secure integration of AI technology into practical applications that improve operational efficiency and improve patient outcomes [158]. Another study stresses the importance of comprehensive data governance frameworks in AI-driven healthcare, emphasizing obstacles such as privacy issues and regulatory limitations. It promotes more transparency, public knowledge, and adaptable regulatory frameworks to cultivate trust and ethical AI implementation [79]. The governance of AI data in healthcare involves creating frameworks for the ethical application of AI, ensuring rigorous clinical validation, and adhering to WHO standards. Countries are in varying stages, with specific recommendations emerging particularly in regions such as Singapore and Rwanda [159]. One article outlines a six-stage governance framework for AI healthcare research, focusing on ethical principles such as transparency, accountability, and inclusion, while addressing data acquisition, privacy, and ongoing quality control to ensure equitable and effective AI healthcare systems in South Korea [160]. The report analyzes the structure of the EU Artificial Intelligence Act on the governance of AI data in healthcare, focusing on ethical oversight, risk classification, and compliance with existing medical standards, in order to improve the safety, legality, and protection of fundamental rights in the use of health data [161].

3.3. AI Data Governance in Cybersecurity

The governance of AI data in cybersecurity is essential to improve security protocols and maintain compliance with regulatory standards. The integration of AI data governance technology into cybersecurity protocols enhances threat detection and response while simultaneously dealing with governance, risk, and compliance (GRC) concerns. The governance of AI data in cybersecurity is crucial due to recognized threats and legal inadequacies. One study highlights the importance of robust compliance frameworks, governance flexibility, and integration of AI automation with human oversight to enhance security effectiveness in high-risk environments [162]. The work highlights the importance of resilient governance frameworks in AI-enhanced cybersecurity, guaranteeing adherence to data protection regulations such as the GDPR and CCPA. It emphasizes the necessity for algorithmic transparency and ethical data use to cultivate consumer trust and mitigate hazards [163]. Artificial intelligence improves data governance in cybersecurity by helping organizations develop robust security policies, track compliance metrics, and refine incident response. The design automates the monitoring and auditing procedures, ensuring a continuous assessment of systems to effectively meet regulatory compliance requirements [164]. Another document emphasizes governance and risk management within its AI-enhanced Cyber-Resilient IT Project Management Framework, focusing on proactive risk assessment, real-time threat detection, and automated incident responses to improve data security and cybersecurity strategies across various sectors [165]. AI-enhanced security enhances cybersecurity by increasing the speed and precision of threat detection, automating responses, and reducing human error. However, ethical governance, data privacy, and transparency issues require strong regulatory frameworks for the proper implementation of AI in public sector security systems [166]. One article emphasizes the imperative of aligning data governance regulations with AI standards to respect rights, such as the AU Convention on Cybersecurity, to ensure the reliable implementation of AI in Africa, highlighting the importance of protecting personal data and promoting accountability [167]. The data governance of AI in cybersecurity involves the implementation of security protocols and efficient data management to protect against digital attacks. It emphasizes the importance of secure data access management to mitigate issues associated with data mining, analytics, and blockchain technology [168].

3.4. AI Data Governance in Finance

Data governance in finance is essential for providing compliance, security, and the appropriate management of data as a strategic asset. Financial institutions face different issues related to regulatory mandates and the complicated process of integrating data from multiple sources. An effective data governance structure mitigates risks while improving operational efficiency and decision-making capabilities. Data governance in finance involves establishing frameworks to ensure regulatory compliance, data integrity, and consistency in various contexts. One article highlights AI-driven solutions for real-time monitoring, automated metadata management, and intelligent classification, crucial to managing complex financial data in hybrid cloud settings [169]. Another article addressed data governance in finance, which involves establishing frameworks to ensure compliance, security, and data integrity in projects that integrate data from several sources. It mitigates risks such as data breaches and regulatory non-compliance, fostering a culture of compliance and employing innovative technology for improved capabilities [170]. Building data governance in finance emphasizes the imperative of rigorous policies, procedures, and stakeholder participation to ensure optimal data quality, privacy, and security. It addresses regulatory compliance challenges and uses technology to effectively manage risks and enhance data assets within the sector [171].

3.5. Domain-Specific Strategies and Challenges in LLM Data Governance

Table 4 presents a comparison of domain-specific data governance strategies in the deployment of LLMs. It shows how different sectors (e.g., supply chain, healthcare, cybersecurity, and finance) implement tailored governance practices to address their unique data needs and regulatory environments. The table shows the specific governance strategies adopted, the positive outcomes achieved (e.g., improved accuracy, safety, or compliance), and the sector-specific challenges encountered, including issues such as data privacy, evolving threats, and regulatory complexity.

Table 4. Domain-specific governance strategies, outcomes, and challenges in LLM deployment.

Domain	Governance Strategy	Outcomes	Challenges	References
Supply chain	Enforcement of data quality such as inventory levels, ensuring logistics data are accurate, transparency (e.g., routing optimizations), and model monitoring (e.g., drift and hallucination)	Better processes and fewer mistakes	Managing different data sources and keeping track of data history	[172–174]
Healthcare	Ethical data management/ stewardship (e.g., EHRs, medical images, and clinical notes), privacy controls (e.g., personally identifiable information), and continuous monitoring of medical chatbots	Enhanced patient safety and reduced errors in diagnoses	Keeping data private and reducing bias in medical data	[175,176]
Cybersecurity	Security protocols, continued risk assessment, and transparency mechanism (e.g., maintaining audit trails)	Early detection of threats and better reaction to disasters	Evolving threats, balancing security and privacy	[177,178]
Finance	Regulatory accountability, audit trails, and working together with stakeholders	Better fraud identification and compliance with regulations	Taking care of complicated legislation and stopping unfair credit scoring	[179,180]

4. Challenges in Data Governance for LLMs

Figure 6 defines the various challenges in data governance for LLMs such as data quality and bias, scalability and complexity, privacy and security, and transparency and explainability, which are mentioned in detail below. As LLMs train on millions/billions of parameters, they need a high computational load with the powerful infrastructure requirements of GPUs/TPUs (high-performance computing clusters are needed for the data parallelism process). The main issue with integrating data governance with LLMs is the high operational costs associated with running this integration pattern implementation approach.

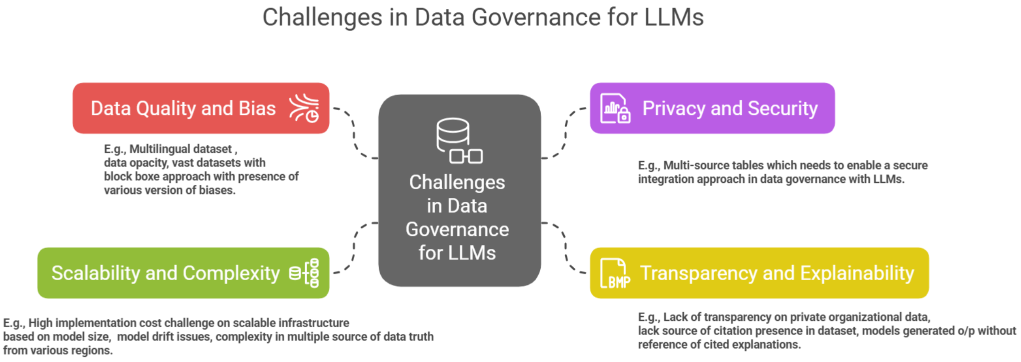
Challenges in Data Governance for LLMs
Data Quality and Bias
E.g., Multilingual dataset , data opacity, vast datasets with block boxe approach with presence of various version of biases.
Privacy and Security
E.g., Multi-source tables which needs to enable a secure integration approach in data governance with LLMs.
Challenges in Data Governance for LLMs
Scalability and Complexity
E.g., High implementation cost challenge on scalable infrastructure based on model size, model drift issues, complexity in multiple source of data truth from various regions.
Transparency and Explainability
E.g., Lack of transparency on private organizational data, lack source of citation presence in dataset, models generated o/p without reference of cited explanations.

Figure 6. Challenges in Data Governance for LLMs.

Zhou et al. [181] proposed a design in LLMDB (a general framework for developing and utilizing LLM-used data management programs) to enhance the data management platform to address the limitations of existing LLMs, consisting of hallucinations, high operational costs, and a low performance in complex tasks. As LLMs train on vast amounts of datasets from multiple public, open-source data (the web, articles, etc.) and private domains (e.g., billions of tokens from various sources), it is difficult to track the data sourcing and ownership issues. Hence, it has an impact on legal actions on copyright data and challenges related to ethical concerns over data ownership issues to suit data governance frameworks. In general, the leverage of data governance to provide a desired solution and a balance act for ethical consideration, bias and fairness, data quality, ownership issues, and transparency to act sensibly are the biggest challenges due to vagueness. The following are several challenges in data governance with the use of LLMs.

4.1. Data Quality and Bias

Data quality, which has a diversity of data sources and bias present in the dataset, is a significant challenge in data governance for LLMs. The quality of the data used to train LLMs has inherent biases from the dataset that can lead to misinformation about the results and ethical concerns. The study [182] reveals that LLMs trained in diverse datasets inherit and amplify societal biases from training data, causing an impact on data quality and extreme versions of biases (e.g., stereotypes and content moderation) within the data governance framework. Using a data governance approach to analyze and optimize LLM training dataset curation leads to biased and low-quality content output from models that impacts performance [183]. The context of non-English datasets that have less information about the source (e.g., a Chinese or Korean context) creates hurdles for data governance to ensure data scarcity, accuracy, unclear ideas about the fairness of the data, and trusted source issues, which impact model performance as well [184]. LLMs trained on multilingual datasets are considered “black boxes”, which means difficult-to-understand datasets and expected outputs of the models [185].

4.2. Privacy and Security

LLMs train on vast amounts of data (e.g., millions and billions of parameters) in various domains, and data are a crucial part of tuning the model behavior. As this large model trains on huge data, privacy and security play a key role. To prevent this extensive information, maintaining compliance with global data protection laws plays a crucial role as a part of the data governance framework. However, there are challenges in data governance related to privacy and security, which are mentioned below.

LLMs have the ability to train on large datasets and can mistakenly memorize the data and regenerate information from personal sensory data such as patient details, medical records, financial information, and others (e.g., data poisoning attacks) [186]. It also targeted inference attacks, where malicious attacks can impact the vector database and can pull private data using queries, which is a massive security concern with various malicious attacks (e.g., privacy breaches in model training and prediction phases, membership inference attacks, and model inference attacks) [187]. The strict guidelines and regulations of RBAC prevent access roles for these models based on user profiles; if an untrained person obtains access to write and retrieve data, this will create an issue of data exposure risk [188,189]. Due to a rapid increase in data volumes, implementation is a big challenge for LLMs in a data governance framework, as data come from multisource tables which need to enable a secure integration approach [190].

4.3. Transparency and Explainability

LLM integration with a data governance framework consists of significant challenges related to transparency and explainability; as it is difficult to trust models, the justification of answers from models, mitigation of bias, and regulatory compliance are the main concerns since, as it is trained on large data sources, it is difficult to trace the source of the truth of the data, which comes from several tables (e.g., dark data, data opacity, data gaps, and algorithmic bias).

Most LLMs are trained on private organizational enterprise data; hence, most of these data are dark data, not accessible to the public. This is vague when it comes to gaining trust in the source of the data and model output, which creates challenges in transparency, regulation, and trust [191]. Financial chatbots trained on a historical financial market data analysis (e.g., stock prices, forex, etc.) and various corporate reports (e.g., balance sheets, income statements, etc.) with a lack of a source of citations raises large concerns about data transparency [192–194]. Healthcare chatbots for patient recommendations are trained on public healthcare datasets, research papers, the medical literature (PubMed and WHO guidelines), and EHRs. However, this chatbot model cannot provide insight into the output result reference that makes a model decision opaque [195]. LLMs like GPT-4, BERT, and others remain the black box of the system (e.g., trained on billions or millions of parameters and the model generates an output without citing source details), which tends to create a very big challenge when implementing the data governance framework approach as, for example, the EU AI Act and US AI bill of rights need transparency and explainability behind each decision [196–198].

4.4. Scalability and Complexity

Regarding LLM integration with a data governance framework approach, it is a big concern to keep track of the enterprise data ecosystem. As this large model replies based on vast, diverse domains and unstructured data (e.g., image, video, and audio), this makes it difficult to manage and govern these diverse, scalable, and complex data patterns.

LLMs need high infrastructure components for a safer deployment of AI models. This leads to a higher implementation cost based on the scalability of the architecture pattern and the size of the model, which makes it harder to implement a data governance approach at the enterprise level [199]. The LLMs are continuously learning and logging memory data and evolving efficiently with a learn-and-evolve approach. Models are consistently growing as a model drift, which creates a challenge for implementing a data governance framework [200,201]. The model generates the output based on training with large training datasets that come from multiple sources of data from various regions (e.g., the US region, Europe region, and others). However, each region has its own specific AI regulation laws, such as cross-border data compliance, creating a pertinent challenge to implementing a data governance methodology [202,203].

5. Key Components of AI Data Governance for LLMs

AI data governance is a vital step in implementing the robust framework approach to ensure that LLMs are developed, trained, and tested securely. This ensures several key components, such as privacy, security, and the ethical use of data, to gain the trust of the user. Figure 7 presents key components of AI data governance, which gives high data quality, data annotation, data storage and management, data usage, regulatory and ethical considerations and frameworks, and accountability and auditing in AI applications. Below are the key components of AI data governance for LLMs.

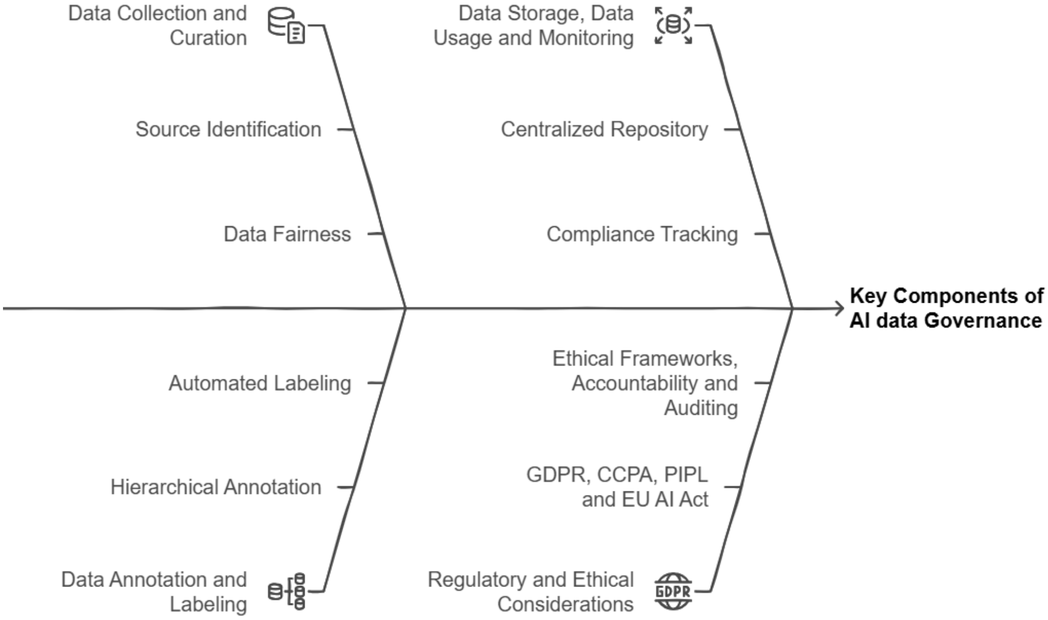
Data Collection and Curation
Source Identification
Data Fairness
Data Storage, Data Usage and Monitoring
Centralized Repository
Compliance Tracking
Key Components of AI data Governance
Automated Labeling
Hierarchical Annotation
Data Annotation and Labeling
Ethical Frameworks, Accountability and Auditing
GDPR, CCPA, PIPL and EU AI Act
Regulatory and Ethical Considerations
GDPR

Figure 7. Key components of AI data governance.

5.1. Data Collection and Curation

Source identification: Effective governance to ensure that the data used for training and the data source that is used for fine-tuning come with high quality [172]; ensuring diversity to select data samples that enhance model training [204]; requiring data to have ethical sources that comply with data protection laws (e.g., the GDPR, HIPAA, CCPA, and others) [205]; using human-curated data, which indicates high quality [206,207]; and ensuring data fairness are important steps as part of the core components of data governance for LLMs. The role of data cataloging ensures data lineage tracking and the use of a metadata management approach [208].

5.2. Data Annotation and Labeling

LLMs using enterprise data can benefit from using hierarchical annotations of structured data, where instead of using a single label, they are classified at multiple levels based on label granularity. Instead of using a single label, a tree structure benefits LLMs to improve scalability and a better performance output [191]. Hence, leveraging hierarchical annotations allows for the identification of complex relationships and patterns within the dataset. Regarding AI data governance for LLMs, automated labeling is a crucial component, as it deals with dynamic label schema integration techniques to improve the ability to understand and classify data with high precision [209]. Dynamic label schemas allow labels to evolve based on data input and requirements, allowing the system to adjust automatically and labels to remain accurate without manual efforts [210].

5.3. Data Storage and Management

Data storage is a crucial step in determining the impact of AI data governance in terms of maintaining data quality, data integrity, and data storage and management, which plays a significant role in securing data storage with a centralized data repository to manage a vast dataset [211] to minimize the risk of data leakage, and this helps to maintain data security using the central data approach. One study emphasizes the impact of the data governance framework on a secure data leak mitigation approach via the centralization of the data repository for vast datasets, transforming enterprise data management through the unified data governance methodology [212]. Another paper proposed a qualified compliance to align ISO/IEC 5259 [213] standards with the EU AI Act, Article 10. This process is a key component of data governance to improve data management and compliance tracking and facilitate organizations in demonstrating compliance with both legal and technical standards [214]. The current research discusses how AI data governance can help with data management by keeping an eye on compliance, making data more effective, and handling risk with a mitigation approach [215]. Using advanced machine learning technologies can enhance data governance capabilities with multisource data integration patterns by using reference tools for data quality checks, data profiling, data cleaning, and continuous monitoring [216].

5.4. Data Usage and Monitoring

Data usage and monitoring are critical components to implement AI data governance frameworks to mitigate the risk of data misuse and allow data compliance with the regulations and guidelines that apply. Effective data governance impacts the data filtering and data monitoring approach during training and testing to secure the AI deployment pipeline of large models [153]. Recommendations for the data governance mechanism based on the detection of unauthorized data requires the protection of patient data in healthcare by closely monitoring the process through transparency and accountability to prevent harm; therefore, data encryption, masking, and hashing can protect patient health information within the use of a conceptual data governance framework [217]. The OECD recommendation on the governance of health data underlines the need to establish national governance frameworks that protect personal health data while facilitating their use for public policy purposes. It encompasses measures to identify unwanted data access to protect patient data security and privacy [218]. Data protection regulation policies such as the GDPR and CCPA reshape data usage in a way that enhances customer trust. Due to the importance of regulation-aware datasets (e.g., C3A), they are managed effectively to comply with relevant regulations, policy standards, and ethical guidelines [219].

5.5. Regulatory and Ethical Considerations

Global Regulatory Landscape

The global regulatory landscape for data protection laws is spread out across various regions throughout the globe (e.g., Europe, the United States, China, etc.) to utilize the regulatory frameworks to enhance data privacy and security standards. The following is a list of widely used regulatory frameworks.

The General Data Protection Regulation (GDPR): The GDPR sets a high standard for data protection laws by the European Union to mitigate data privacy and security vulnerability. This regulation sets strict requirements for organizations related to data handling, data processing, data breach notifications, and data storage to ensure transparency and accountability.

The key components of the GDPR are data protection rights, breach notifications, lawful processing, extraterritorial reach, and data subject rights (e.g., the Right to Access and Right to Rectifications) [220,221]. Integrating the GDPR and EU AI Act within the global regulatory landscape enhances compliance strategies and strengthens data protection and trustworthy AI systems [222].

The California Consumer Privacy Act (CCPA): The CCPA represents privacy laws that govern data collection, data sharing, and letting customers control their data. It gives people in California certain rights over their personal information, such as the right to know what information is being collected, the right to see and delete that information, and the right not to have their information sold [223,224]. The CCPA protects specific groups of people, with a focus on customer rights when it comes to data sales. It has made a lot of advances in protecting privacy, showing different ways of handling privacy problems in the digital world today [225]. This law was subsequently revised and expanded by the California Privacy Rights Act (CPRA), which introduced enhanced consumer protections and enforcement mechanisms [226].

China's Personal Information Protection Law (PIPL): The PIPL is a comprehensive framework and a significant step in China for data protection, data classification, and user rights within digital platforms [227]. The main components of the PIPL are informed consent, data classification, and user rights. This framework in China is used for the protection of personal data, which emphasizes informed consent, the classification of data, and remedies for data violations, and is based on the principle of proportionality to improve data security and privacy rights [228]. It is designed to regulate the use of personal data by digital platforms, with a focus on the state's authority over user data control and privacy practices [229].

5.6. Comparative Insights of GDPR, CCPA, and PIPL in Practice for LLM Governance

Table 5 presents a comparison of the three main data protection regulations laws for LLM governance: the GDPR (EU), CCPA (CA, USA), and PIPL (Beijing, China) based on various key aspects. It outlines key regulatory aspects like consent requirements, impact on LLM operations, cross-border data transfer rules, data localization mandates, jurisdictional scope, and the treatment of automated decision making. The table highlights how each regulation differs in its approach to data protection and oversight, which shapes how LLMs are developed, deployed, and governed across jurisdictions.

Table 5. Comparative insights of GDPR, CCPA, and PIPL for LLM governance.

Aspect	GDPR (EU)	CCPA (CA, USA)	PIPL (Beijing, China)
Consent requirements	Requires clear, educated consent	An opt-out approach for selling data and permission for sensitive data	Needs clear, informed, and willing permission, especially for private information
Impact on LLM governance	A lot of focus on rights and reduction in data along with being able to explain	Pay attention to customer rights, limits on data sales, and limited explanations	Focuses on data localization, clear permission, and state oversight
Cross-border data transfers	Restricted: needs to be adequate or have safety measures like SCCs (Standard Contractual Clauses)	No strict rules about crossing borders	Large-scale transfers need to be approved by the government and subject to security checks
Data localization	Not required: open to assessment of competency	Not required	Strong rules for localizing important or private data
Jurisdiction scope	Apply to all organizations that handle data about EU people	For companies that deal with personal information of California residents	This rule applies to all handling of personal data about people in China
Automated decision making	Must give a good reason, allow people to help, and defend rights	There are no clear rights when it comes to automated choices	Needs to be clear, have an explanation, and give people the right to refuse fully automated choices

5.6.1. Ethical Frameworks

An ethical framework and AI data protection and regulations are vital steps to ensure ethical data practices by various stakeholders (e.g., government regulations, researchers, developers, organizations, and businesses) with the principle of responsible AI development (e.g., transparency, fairness, a human-centric approach, etc.).

Stakeholder engagement in ensuring ethical data practices: The roles of stakeholders are critical in ethical data practices to mitigate data risk assessments using government and regulatory involvement to foster trust by implementing various regulatory frameworks (e.g., the CCPA, GDPR, EU AI Act, and others) and to implement sustainable development [230]. The use of stakeholder participation is critical by participating in brainstorming sessions, consultations to clarify ethical responsibilities, and addressing ethical conflicts [231]. Ethical considerations in data analysis are the best practices for the researcher and developer to implement an ethical AI model with fairness, fostering trust throughout the lifecycle of model development [232]. The use of the enhanced enterprise data ethics framework fosters strategic decision making and legitimate engagement in higher education data management by emphasizing transparency, fairness, accountability, and a centric approach between stakeholders [233].

The fundamental principles of responsible AI development: These principles must guide the end-to-end machine learning lifecycle of AI development that builds securely with ethical safeguards of model deployment, prevents bias in the model, and ensures a non-discriminatory and ethical approach throughout the life of the model iteration. A comprehensive framework and data protection laws are important for responsible AI development that includes fairness, transparency, privacy, security, accountability, and system robustness [234]. This report highlights the importance of stakeholder participation, comprehensive monitoring systems, and structured ethical frameworks as fundamental principles for responsible AI development. These components guarantee that technological advances are consistent with ethical principles and human values, ultimately resolving issues such as accountability and algorithmic bias with the requirements of responsible AI governance [235]. The main idea of this paper is to show a complete approach to creating a trustworthy ethical framework of AI that builds morals, ethics, and requirements in the AI systems and rules that are responsible. A strong set of laws, morals, and ethical standards is used throughout the lifecycle of the AI system to ensure responsibility and the general well-being of society [236].

5.6.2. Accountability and Auditing

To gain trust in various sectors with the use of emerging AI technologies like LLMs, it is crucial to have a mechanism for auditing data practices. The integration of robust auditing mechanisms and accountability is important to improve efficiency and precision in AI applications with real-time AI monitoring [237]. It is crucial to uphold public confidence in data practices through the implementation of both internal and external audits. Research underscores the importance of comprehensive auditing, which, together with stakeholder participation and digital transformation, improves transparency and accountability in public sector accounting [238]. One study indicates that internal audits conduct periodic self-assessments to ensure adherence to data protection regulations in the implementation of the GDPR to ensure compliance with data protection measures [239,240]. In order to improve the quality of national statistics and data curation, another paper stresses the necessity of establishing robust data governance frameworks that are based on widely accepted standards. These cybersecurity frameworks may include internationally recognized standards such as ISO 27001 [241] (an international standard for information security management systems), SOC 2, and NIST to ensure accountability and a rigorous auditing process [242].

6. Best Practices for AI Data Governance in LLMs

AI data governance plays an important role in LLMs, providing strong guidelines and regulatory authority for data management via end-to-end lifecycle management in LLMs to ensure compliance, regulations, security, an auditing methodology, and an ethical approach. The best practices of effective data governance involve implementing robust data governance frameworks, leveraging valuable technology for data monitoring and security, engaging stakeholders for transparency and accountability, and consistently enhancing governance policies to accommodate advancements in AI and evolving regulations based on requirements. Hence, implementing the best practices of data governance assists organizations in minimizing risk, providing trustworthiness in AI applications from the user's side, maintaining data integrity, securing data against adversarial attacks, and continuously monitoring data pipelines for anomalies. As shown in Figure 8, an overview of best practices for AI data governance at a high level and the key components are outlined below.

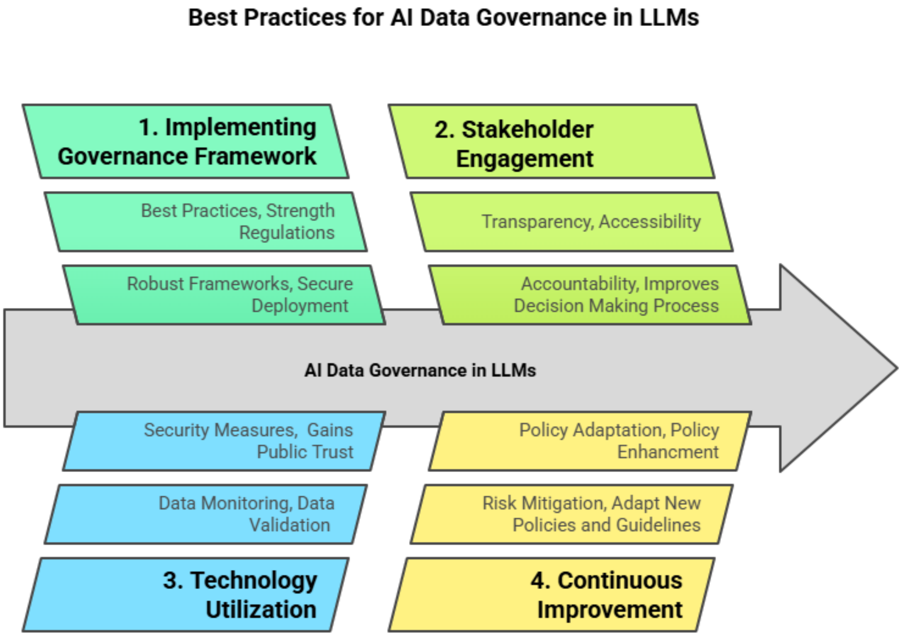
Best Practices for AI Data Governance in LLMs
1. Implementing Governance Framework
Best Practices, Strength Regulations
Robust Frameworks, Secure Deployment
2. Stakeholder Engagement
Transparency, Accessibility
Accountability, Improves Decision Making Process
AI Data Governance in LLMs
Security Measures, Gains Public Trust
Data Monitoring, Data Validation
3. Technology Utilization
Policy Adaptation, Policy Enhancment
Risk Mitigation, Adapt New Policies and Guidelines
4. Continuous Improvement

Figure 8. Best practices for AI data governance in LLMs.

6.1. Developing a Governance Framework

A well-structured governance framework played a crucial role in protecting sensitive information in a data quality management-based approach [243] that enhances decision making and facilitates the compliance approach. It implemented the integration of the data governance framework that strengthens the compliance and regulations that build trust between the user and AI applications [244]. The research cited in one study states that strong information governance guidelines are important (i.e., strong governance standards are needed). Trust in AI systems can be built by making sure that they are open and teaching users how to use them [245]. In every step of LLM lifecycle management, data ownership, transparency, accountability, and secure deployment are keys to the success of LLMs, defined as a clear role using data governance [246]. Another study offers a data governance framework suited for blockchain, IoT, and AI technologies and uses three main core pillars such as data integrity, security and privacy, and ethical considerations to adapt to evolving technologies [247].

6.2. Stakeholder Engagement

Stakeholder involvement, which includes early input from all participants (e.g., AI engineers, compliance officers, data scientists, and a regularity audience), gives an important knowledge exchange between the research team and the data owners, which helps identify potential risks and ethical concerns prior to the development phase and ensures a diversity of perspectives in AI development [248,249]. One paper demonstrates the importance of ongoing stakeholder engagement, particularly in the design of generative AI tools, with an especially strong focus on older adults. This participatory approach guarantees that AI applications, such as LLMs, are effective and useful to their intended users by addressing usability and accessibility. In addition, they assist in brainstorming various concerns to be addressed and improve the decision-making process [250,251].

6.3. Leveraging Technology

As LLMs on a large scale utilize and perform complex operations, in this case, the use of technology within the data governance methodology plays a critical role. The use of advanced technologies such as AI-driven tools can lend itself to an automation approach to audit and monitor the regulation approach with respect to maintaining data integrity. An AI-driven data analysis enhances the identification of trends and patterns and assists in policy-making criteria, policy evaluation, improved transparency, and public trust in governance [252]. However, using an automated data validation approach, a data validation document (DVD)-based approach reduces the risk of human error, allows for the close tracking of data, and facilitates compliance and regulatory standards. Overall use of AI-driven technology improves operation processes and supports large-scale data-driven governance.

6.4. Continuous Improvement

LLMs use fine-tuning mechanisms (which allow LLMs to take advantage of both labeled and unlabeled data [253]) to adapt to a specific task and evolve performance and applicability. AI data governance uses an iterative approach to assist with the iteration and feedback-based mechanism and requires a continuous monitoring and refinement approach to LLMs as it continues to evolve. As LLMs are trained on large datasets and integrated with various applications, data governance practices adapt the process accordingly. Regular updates to policies and regulations help mitigate the risk associated with data bias, model inaccuracies, and security breaches [254]. Hence, a continuous improvement approach in a data governance framework plays a critical role in aligning with current processes and future process updates.

6.5. Tools and Metrics for Auditing Governance Quality in LLM Pipelines with Lifecycle Phases

As can be seen in Figure 9, there are two phases. Phase 1 consists of the data collection approach using the data source, the data quality assessment with a filtering mechanism, PII detection tools, bias and fairness audits, StereoSet, Fairlearn tools, and data lineage and tracking (e.g., Apache Atlas and MLflow). However, phase 2 has model evaluation and benchmarks and concentrates on verifying LLM outcomes for equity and security through benchmarks, bias/toxicity evaluations, and human assessments. Governance technologies such as Truera and MLflow provide audit tracking and enhancements informed by feedback.

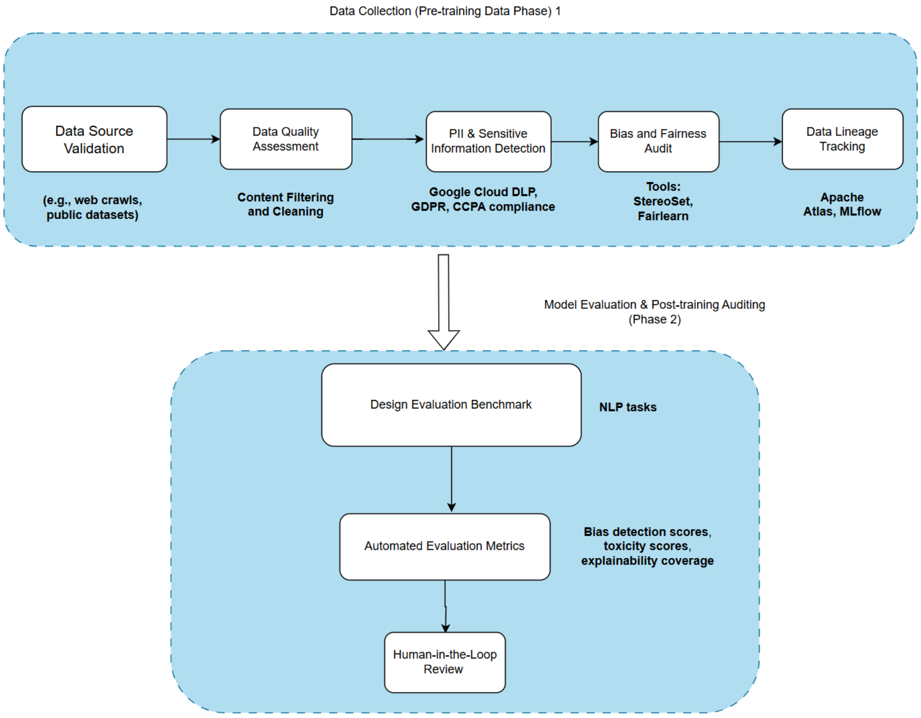
Data Collection (Pre-training Data Phase) 1
Data Source Validation
(e.g., web crawls, public datasets)
Data Quality Assessment
Content Filtering and Cleaning
PII & Sensitive Information Detection
Google Cloud DLP, GDPR, CCPA compliance
Bias and Fairness Audit
Tools: StereoSet, Fairlearn
Data Lineage Tracking
Apache Atlas, MLflow
Model Evaluation & Post-training Auditing (Phase 2)
Design Evaluation Benchmark
NLP tasks
Automated Evaluation Metrics
Bias detection scores, toxicity scores, explainability coverage
Human-in-the-Loop Review

Figure 9. LLM lifecycle phases using data governance approach in LLMs.

Table 6 gives the various tools and metrics that are often used to check and rate governance quality in large language model pipelines (LLMs).

Table 6. Overview of tools and metrics used to audit governance in LLM pipelines.

Category	Tools/Framework	Key Aspects and Metrics	References
Bias and fairness auditing	StereoSet, Fairlearn, and Aequitas	Bias detection score, stereotype preference ratio (based on region, gender, race, and profession), demographic parity, disparate impact, false discovery rate, and false omission rate	[255–258]
Model monitoring and drift	Truera and WhyLabs	Date drift detection score, fairness metrics, and stability score	[259,260]
Audit logging and traceability	MLflow and Apache Atlas	Performance metrics (F1-score, BLEU (for NLP), and custom metrics logging)	[261,262]
Data quality and lineage	DataHub, Alation, and Datafold	Accuracy and traceability score	[263–266]
Privacy and compliance	Google Cloud DLP	PII detection score, risk re-identification index, and compliance ratings	[267,268]

7. Case Studies and Real-World Applications on Implementing Data Governance in LLMs

Many companies at the enterprise level are using data governance frameworks in data security to manage master data management (MDM), such as customer data management, product master data management, and vendor master data management [269]. Google was the first in the industry to leverage data governance in generative AI to protect AI/ML privacy commitments, providing higher security over customer data stored in the cloud [270]. Microsoft Azure implements new opportunities for modern AI data governance to integrate LLMs with transparency, accountability, security, and a focus on fairness in AI's decision-making abilities [271,272].

The proposed framework in the financial industry (e.g., IBM watsonx.governance [273]) with the implementation of AI governance in LLMs is the main impact behind the use of the human-controlled AI-regulated task together with the automation pipeline to process models using MLOps and LLMOps. This along with high-level design and methodologies to manage organization in the blueprinting phase and end-to-end model development guidelines with the use of guidance and regulation throughout the LLM lifecycle from the design to the development, testing and validation, deployment, monitoring, and enhancement of models are crucial in the advancement of ethical and responsible AI. One author proposed Nickerson's framework [274] development process that captured the scope of building a model (the data, model, system, people targets and scope, and organizational scope and targets), outline, governance mechanism (structural, procedural, and relational), model targets (e.g., RAG), antecedents, consequences (risk management and performance effects), and mitigation risk while integrating GenAI. The author of this research recommended differential governance, supervision, controls, and procedures incorporating generative AI. The first step was differential privacy, enabling financial institutions to detect fraud while protecting customer privacy rights and regulatory obligations [76]. The author of intelligent data governance has proposed a modern framework [77] built on a modular microservice architecture deployed on a scalable cloud infrastructure. This method, with the use of this architecture and design pattern (e.g., modular microservices and scalable cloud infrastructure), provides organizations with the ability to rapidly adapt to evolving data governance requirements, providing unparalleled scalability, integration, and flexibility. One researcher proposed [275] blueprinting for auditing LLMs using a three-layered approach such as governance audit, model audit, and application audit, and the adoption of this AI governance model in LLMs collectively addresses ethical, legal, and technical challenges, as shown in Figure 10.

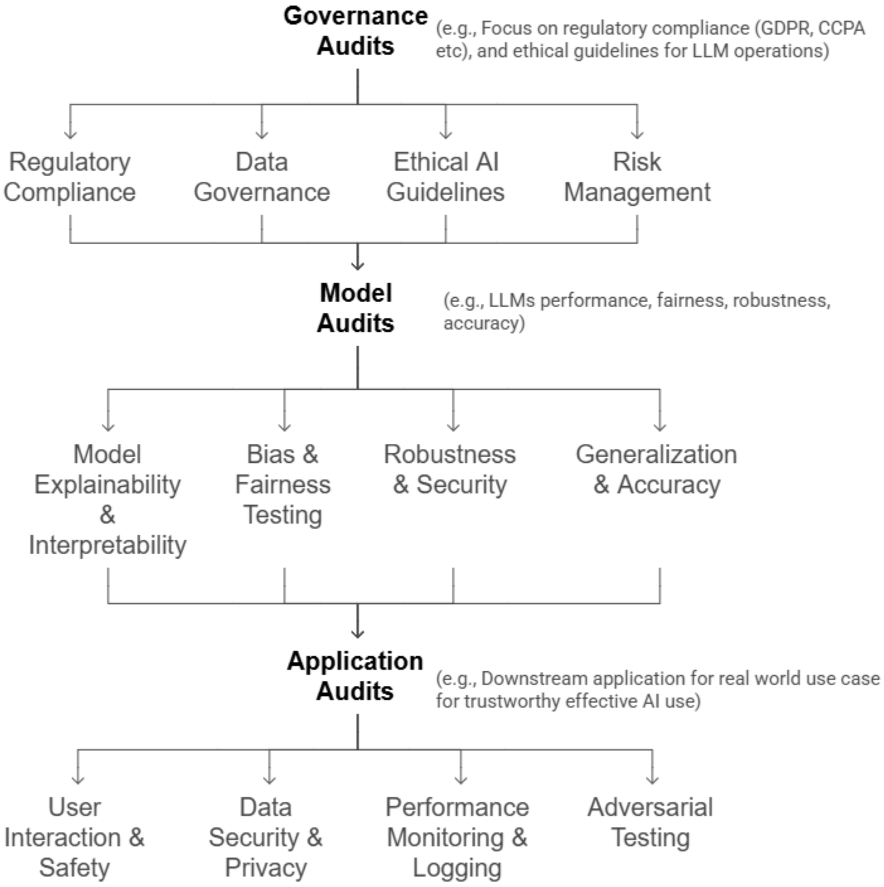
Governance Audits
(e.g., Focus on regulatory compliance (GDPR, CCPA etc), and ethical guidelines for LLM operations)
Regulatory Compliance
Data Governance
Ethical AI Guidelines
Risk Management
Model Audits
(e.g., LLMs performance, fairness, robustness, accuracy)
Model Explainability & Interpretability
Bias & Fairness Testing
Robustness & Security
Generalization & Accuracy
Application Audits
(e.g., Downstream application for real world use case for trustworthy effective AI use)
User Interaction & Safety
Data Security & Privacy
Performance Monitoring & Logging
Adversarial Testing

Figure 10. Auditing data governance framework for LLMs: a three-layered approach [275].

Another paper addresses Telecom Knowledge Governance (TKG) for LLMs and describes how a high-quality telecom corpus and an automated Q&A dataset were generated to improve model performance in telecom industry apps such as customer service and data search [276]. The paper talks about real-life case studies that show how AI can be used successfully in data governance. It emphasizes automating compliance evaluation, improving data quality, and managing risk [215]. The paper presents case studies highlighting the significant challenges in LLMs related to privacy and security concerns, and hence it needs to implement the GDPR and CCPA data protection laws. In this work, the author proposed a framework referred to as the OneShield Privacy Guard. This framework is intended to mitigate the privacy risks associated with user inputs and outputs produced by LLMs in open-source and enterprise environments [277]. The system that leverages AI regulation successfully assists in tackling legal queries with variable precision by utilizing GPT-3.5 and GPT-4 to interact with EU legislation (a system of laws and legal frameworks enacted by the European Union). The potential of LLMs in governance applications was demonstrated by integrating the use of augmented retrieval generation (RAG), which improved the functionality of this system [278].

8. Open Challenges and Future Research Opportunities

Data governance frameworks are vital to the process of their integration with LLMs. Although there is an emerging trend of adapting the digital landscape of the data governance base, there are still open items that need to be addressed, which are mentioned below.

8.1. Scalability of Data Governance Framework

As LLMs scale up, they are trained on millions or billions of parameters based on the complexity and enhancement of the model. A solid, scalable, and robust approach is required in the data governance integration pattern for a large dataset training process. Furthermore, with the given scale of LLMs, the new data governance framework must be adaptable, continuously monitored with the ability to provide real-time updates, and ensure clear and refined data governance compliance and regulation.

There are not any scalable governance models that can handle the huge amounts and different types of data used in LLM training and rollout right now. Researchers should work on making flexible real-time governance models that can always verify compliance in very large datasets that are constantly changing.

8.2. Security Risks and Data Breaches

As large language models are deployed in production instances, which require secure LLMOps pipelines to deploy AI models, they need an encrypted, robust mechanism within the data governance framework to avoid data breach activity while delivering the AI model in a production instance. However, it needs a multilayer approach in data governance frameworks, which will assist in handling the AI model deployment logging activity from the initial phase to the deployment phase and the maintenance phase of the model by embedding security and compliance protocols.

As of now, there are not many strong, comprehensive security tools that are made exclusive for LLMOps processes. There should be complete encryption, log-in, and compliance processes built in from the start of training through model maintenance. These will keep data safe and stop breaches.

8.3. Data Privacy and Compliance

Cross-border data transfer has a language barrier in various regions, as different countries have different data protection regulation laws in their native language, e.g., LGPD (Brazil), the CCPA (California), and the EU AI Act (Europe), which creates a vague understanding and implementation of data governance rules. As a result, the establishment of a unified compliance strategy will be an extremely difficult task. Hence, companies must develop multilingual compliance frameworks and automated translation tools as prospective actions to overcome this challenge in data governance frameworks.

8.4. Data Provenance and Traceability

It is challenging to determine the source of the truth of the data, which is derived from multiple tables (e.g., dark data, data opacity, data gaps, and algorithmic bias), as LLMs are trained on large data sources and the data are constantly cleaned and refreshed. Hence, tracking large datasets and maintaining the data lineage from various pipelines are unique challenges in tracking and tracing data in the AI governance landscape. Therefore, the implementation of robust mechanisms for data traceability and continuous data auditing is necessary as this framework adapts and evolves.

Furthermore, an evolving landscape of AI regulations is needed as AI technology has evolved rapidly. Hence, there is a need for global coordination to address regulatory gaps, and there is potential to change AI regulations to mitigate the risk of fostering innovation [279]. A new policy mandate is essential for AI developers to enhance the model for more detailed transparency and explainability in critical sectors such as healthcare, finance, and autonomous systems that need explainable artificial intelligence to promote ethical uses of AI [280]. In the coming years, stronger data protection laws will be required for the automated decision-making output of the model. In cross-border data governance, due to multilingual data, uniform data regulation bodies and strict policies are needed with each local privacy law to fill the gaps between various languages based on data regulation.

However, existing research is being conducted to finalize a new integration pattern between blockchain and AI data governance for secure and auditable data governance. As shown in Figure 11, blockchain technology with the use of a new integration approach (a conceptual framework) with a data governance framework will help, offering a transparent track of all transactions and data interactions, which is essential for monitoring AI algorithms, ensuring the integrity and transparency of data, obtaining an auditable trail of transactions, implementing a hybrid governance approach, and ensuring adherence to ethical standards [247,281].

The blockchain-driven regulatory framework is an essential part of protecting the digital ecosystem against AI-generated content, which has addressed security concerns in the digital ecosystem; however, this existing framework improves audit qualification and efficiency through deep data mining and the security of audit problem clues [282,283]. More discovery is needed in the hybrid AI data regulation process with a multilayer approach in the governance data framework. Furthermore, promoting interdisciplinary research on AI governance is essential for creating extensive and effective regulatory frameworks (e.g., the ETHOS framework [284] and decentralized governance innovation framework, which offers scalability and prompting trust) while addressing the significant gaps between the evolving AI technologies in LLMs and the existing legal framework (e.g., combining legal principles, ethical considerations, technological advancements, and sociological insights to create comprehensive frameworks for AI governance) [285].

How to find the start, changes, and lineage of very big and different datasets is hard and has not been solved yet. We need to move forward with ongoing audits and clear data traceability tools to make sure that LLM administration is responsible and that the data are correct.

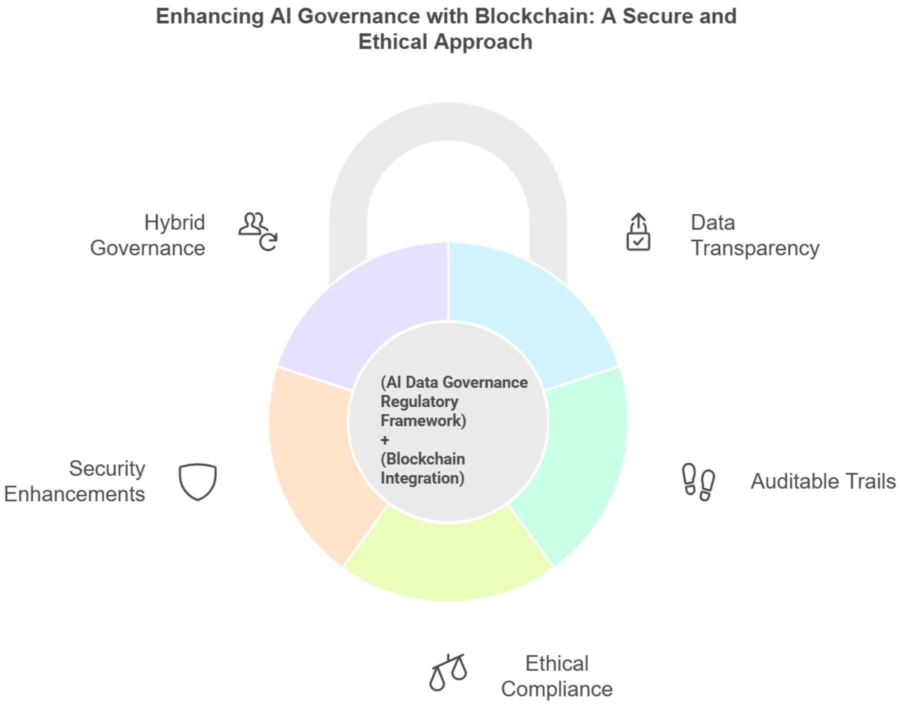
Enhancing AI Governance with Blockchain: A Secure and Ethical Approach
Hybrid Governance
Data Transparency
(AI Data Governance Regulatory Framework) + (Blockchain Integration)
Security Enhancements
Auditable Trails
Ethical Compliance

Figure 11. Enhancing data governance with AI and blockchain integration.

8.5. Human–AI Collaboration in Data Governance

The necessity of human–AI collaboration in data management is becoming more widely acknowledged as a critical factor in the maintenance of ethical standards, data fairness, data accuracy, and the improvement in decision-making processes with the use of human–AI collaboration in the data governance framework. In an effort to resolve obstacles such as ethical dilemmas and cognitive inaccuracies in data management and mitigate misinformation risks from AI-automated systems, this collaboration leverages the strengths of both human cognitive abilities and machine-computational AI capacity. Through human oversight, cognitive biases that may arise as a consequence of automated systems can be mitigated and enhance the quality of decisions and increase public trust [203,286]. Future research steps are important to investigate human-in-the-loop governance models, which require collaborations between human review and AI systems to ensure responsible AI utilization. This approach will balance automatically generated output with human judgment and refine the escalation, mitigate the risk of misinformation, and uphold ethical standards. We need to create good person-in-the-loop governance models that integrate the smarts of AI with the right decisions made by people. To reduce false information, cognitive biases, and ethical problems, as well as to increase trust and responsibility, frameworks for adding human oversight should be studied.

8.6. Data Quality and Bias Mitigation

LLMs frequently develop biases from their training data, which can result in ethical and impartiality concerns. One study demonstrates that LLMs exhibit performance disparities as a consequence of US-centric training data, revealing biases influenced by sociodemographic factors [287,288]. It emphasizes the importance of diverse training data and impartiality metrics in order to address ethical concerns and ensure that the models perform fairly, and it needs to ensure data quality and data reparation by applying preprocessing techniques and utilizing post-processing corrections, which are vital steps in curating diverse datasets and a bias mitigation approach [64,206]. The authors of one study show a way to remove bias by choosing datasets that are balanced between cultures. This reduces visual bias and makes the models more fair. By making sure everyone is treated equally, this method increases the number of true positives for underrepresented groups without lowering general accuracy. It shows that fixing data bias where it starts makes model results more fair and useful [289].

Another author introduces the parity benchmark, which checks for flaws in large language models (LLMs) based on things like race, gender, and disability. It tests models such as GPT-4, Claude 3.5 Sonnet, and Llama 3. It shows differences in success and emphasizes the need for ongoing strategies to reduce bias [290].

Additional research is required to develop adaptive models that dynamically evaluate and correct biases throughout the end-to-end AI lifecycle (e.g., identifying the unknown bias pattern, data opacity alert mechanism, adaptive bias correction approach, etc.), ensuring transparency and accountability in the decision-making process of the LLM. Biases can have a significant impact on society, which is why future research methods are crucial to ensure impartiality and accountability in AI systems across various domains (e.g., healthcare, finance, pharmaceutical, and others). Biases that come from training data that are not uniform are still a big problem. Scientists should come up with ways to find and fix adaptive bias that work all the time, no matter how long an AI resides. This would make AI more fair and easy to understand for a wider range of people and uses.

8.7. Gaps and Potential Future Research Directions

The illustration below in Figure 12 provides the five important things that must be in place for large language models (LLMs) to be responsibly governed, such as ethical data stewardship accountable for data collection and usage to enhance fairness and minimize biases, privacy, and security by design to ensure data security via encryption, anonymization, and privacy compliance, such as in accordance with the GDPR, HIPAA, and others. Among others, continuous performance and risk monitoring are related to ongoing checks for accuracy, bias detection scores, possible errors with human oversight, and a mitigation approach. Moreover, regulatory compliance and transparency make sure that laws are followed, that there are clear reporting trails, and ensure stakeholder collaboration, adaptability, and that experts and users are involved to make governance fit for different businesses in various sectors. Together, all of these parts work to ensure that LLMs are responsible, follow the law, perform well, and can be trusted in a wide range of areas.

All in all, the current landscape of AI data governance for LLMs is marked by several critical shortcomings. These include the lack of standardized global frameworks, limited transparency and explainability, insufficient mechanisms for detecting and mitigating bias, and challenges in ensuring data lineage, traceability, and real-time auditing. Existing governance models often fail to scale effectively alongside the growing complexity of LLMs, particularly in federated or cross-border environments where regulatory requirements vary significantly. Future research should prioritize the development of standardized, scalable AI governance methods that incorporate principles of Explainable AI, enable dynamic auditing and adaptive bias correction, and improve systems for tracking data provenance. Moreover, exploring federated governance frameworks, harmonizing international legal and ethical standards, and building trustworthy data marketplaces could play a significant role in advancing the secure, equitable, and accountable deployment of LLMs across diverse domains.

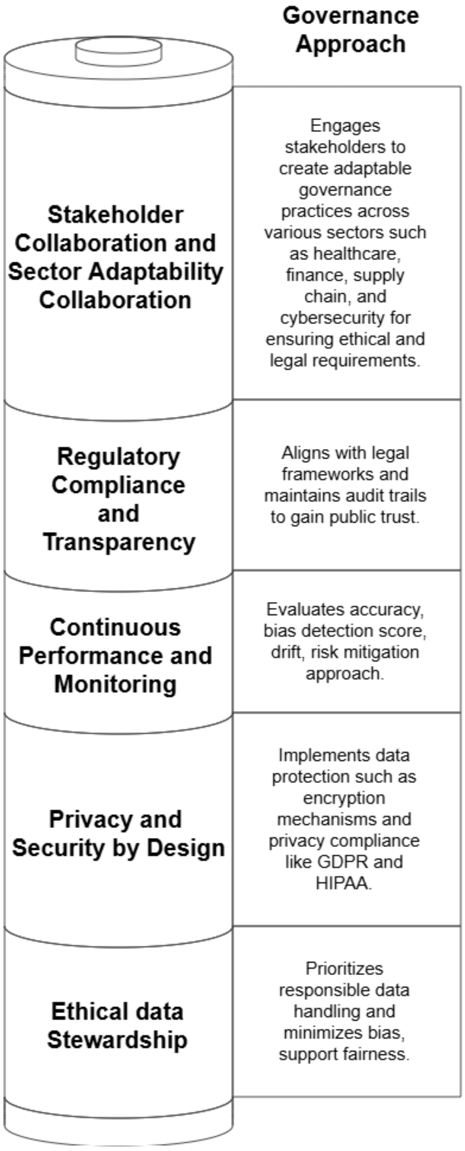
Governance Approach
Stakeholder Collaboration and Sector Adaptability Collaboration
Engages stakeholders to create adaptable governance practices across various sectors such as healthcare, finance, supply chain, and cybersecurity for ensuring ethical and legal requirements.
Regulatory Compliance and Transparency
Aligns with legal frameworks and maintains audit trails to gain public trust.
Continuous Performance and Monitoring
Evaluates accuracy, bias detection score, drift, risk mitigation approach.
Privacy and Security by Design
Implements data protection such as encryption mechanisms and privacy compliance like GDPR and HIPAA.
Ethical data Stewardship
Prioritizes responsible data handling and minimizes bias, support fairness.

Figure 12. Toward effective data governance in LLMs: a framework for implementation.

9. Conclusions

LLMs are growing rapidly, and to foster the trustworthiness of AI models from the user's side, it is essential to integrate LLMs with a robust data governance framework to ensure ethical data management, ensure a good model performance, avoid biases, follow privacy laws, follow regulatory compliance, have a robust impact on data privacy, and avoid security breaches and hallucinations in AI models. In this article, we explored the core importance of the data governance framework, including various rules and regulations on AI governance and the challenges of implementing data governance in LLMs. We also provided the importance of stakeholder collaboration in shaping policies for the ethical data approach. Moving forward, it is essential that the data governance framework continues to be refined and adapted to various sectors of LLM-based AI applications, such as healthcare, pharmaceutical, finance, supply chain, and cybersecurity, to adapt the robust ethical approach and to ensure legal requirements are consistently met. There is a future necessity to create adaptable and scalable data governance frameworks that can accommodate various LLM scalability adapting methodologies. Moreover, efficient human-in-the-loop governance frameworks are crucial for integrating AI capabilities with educated human judgment, consequently mitigating misinformation, cognitive biases, and ethical dilemmas.

Author Contributions: Conceptualization, S.P. and Z.A.; validation, S.P.; formal analysis, S.P.; investigation, S.P. and V.M.; resources, Z.A.; writing—original draft preparation, S.P. and V.M.; writing—review and editing, S.P., Z.A. and K.S.; visualization, S.P., V.M. and Z.A.; supervision, Z.A.; project administration, Z.A.; funding acquisition, Z.A. and K.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable.

Conflicts of Interest: Saurabh Pahune was employed by the company Cardinal Health, Dublin, OH 43017, USA. Venkatesh Mandapati was employed by the company FedEx Memphis, Collierville, TN 38017, USA. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
CCPA	California Consumer Privacy Act
FCRA	Fair Credit Reporting Act
MDM	Master data management
FSA	Financial sentiment analysis
IT	Information Technology
OECD	Organization for Economic Cooperation and Development
ENISA	European Union Agency for Cybersecurity
NIST	National Institute of Standards and Technology
CRS	Conversational recommender system
BCBS	Basel Committee on Banking Supervision
SCM	Supply chain management
LLMDB	LLM-enhanced data management paradigm
FDA	Food and Drug Administration
MLOps	Machine learning operations
LLMOps	Large language model operations
GPU	Graphics Processing Unit
TPU	Tensor Processing Unit
LLM	Large language model
AIRMF	AI risk management framework
DLP	Data Loss Prevention
RBAC	Role-Based Access Control
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
MFA	Multi-Factor Authentication
KYC	Know Your Customer
TLS	Transport Layer Security
ML	Machine learning
ZTS	Zero Trust Security

BCBS	Basel Committee on Banking Supervision
GS1	Global Standards for supply chain and data management
SOX	Sarbanes–Oxley Act
RBAC	Role-Based Access Control
PHI	Protected Health Information
CTI	Cyber threat intelligence
EHRs	Electronic health records
EU	European Union
PIPL	Personal Information Protection Law
CPRA	California Privacy Rights Act
AI	Artificial intelligence
NIST	National Institute of Standards and Technology
SOC	Service Organization Focus
MDM	Master data management
TKG	Telecom Knowledge Governance
RAG	Retrieval-Augmented Generation
LGPD	Lei Geral de Proteção de Dados (General Data Protection Law)
HHH	Helpful, honest, and harmless
PII	Personal identifiable information
DVD	Data validation document
EAI	Explainable artificial intelligence
WHO	World Health Organization
AU	African Union
EU	European Union
DPK	Data Prep Kit
DLG	Data lineage graphs
ETHOS	Ethical Technology and Holistic Oversight System
KYC	Know Your Customer
DataBOM	Data Bill of Materials
HAIRA	Healthcare AI governance readiness assessment
GRC	Governance, risk, and compliance
PII	Personally identifiable information
DLP	Data Loss Prevention
SCC	Standard Contractual Clauses

References

1. Haque, M.A. LLMs: A Game-Changer for Software Engineers? *arXiv* **2024**, arXiv:2411.00932. [CrossRef]
2. Meduri, S. Revolutionizing Customer Service: The Impact of Large Language Models on Chatbot Performance. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2024**, *10*, 721–730. [CrossRef]
3. Pahune, S.; Chandrasekharan, M. Several categories of large language models (llms): A short survey. *arXiv* **2023**, arXiv:2307.10188. [CrossRef]
4. Vavekanand, R.; Karttunen, P.; Xu, Y.; Milani, S.; Li, H. Large Language Models in Healthcare Decision Support: A Review. *SSRN*, 2024. Available online: https://ssrn.com/abstract=4892593 (accessed on 22 May 2025).
5. Veigulis, Z.P.; Ware, A.D.; Hoover, P.J.; Blumke, T.L.; Pillai, M.; Yu, L.; Osborne, T.F. Identifying Key Predictive Variables in Medical Records Using a Large Language Model (LLM). *Research Square*. 2024. Available online: https://www.researchsquare.com/article/rs-4957517/v1 (accessed on 22 May 2025).
6. Yuan, M.; Bao, P.; Yuan, J.; Shen, Y.; Chen, Z.; Xie, Y.; Zhao, J.; Li, Q.; Chen, Y.; Zhang, L.; et al. Large language models illuminate a progressive pathway to artificial intelligent healthcare assistant. *Med. Plus* **2024**, *1*, 100030. [CrossRef]
7. Zhang, K.; Meng, X.; Yan, X.; Ji, J.; Liu, J.; Xu, H.; Zhang, H.; Liu, D.; Wang, J.; Wang, X.; et al. Revolutionizing Health Care: The Transformative Impact of Large Language Models in Medicine. *J. Med. Internet Res.* **2025**, *27*, e59069. [CrossRef]
8. Acosta, J.N.; Falcone, G.J.; Rajpurkar, P.; Topol, E.J. Multimodal biomedical AI. *Nat. Med.* **2022**, *28*, 1773–1784. [CrossRef]
9. Huang, K.; Altosaar, J.; Ranganath, R. Clinicalbert: Modeling clinical notes and predicting hospital readmission. *arXiv* **2019**, arXiv:1904.05342.

10. Lee, J.; Yoon, W.; Kim, S.; Kim, D.; Kim, S.; So, C.H.; Kang, J. BioBERT: A pre-trained biomedical language representation model for biomedical text mining. *Bioinformatics* **2020**, *36*, 1234–1240. [CrossRef]
11. Santos, T.; Tariq, A.; Das, S.; Vayalpati, K.; Smith, G.H.; Trivedi, H.; Banerjee, I. PathologyBERT-pre-trained vs. a new transformer language model for pathology domain. In Proceedings of the AMIA Annual Symposium Proceedings, Washington, DC, USA, 29 April 2023; Volume 2022, p. 962.
12. Christophe, C.; Kanithi, P.K.; Raha, T.; Khan, S.; Pimentel, M.A. Med42-v2: A suite of clinical llms. *arXiv* **2024**, arXiv:2408.06142.
13. Wu, S.; Irsoy, O.; Lu, S.; Dabravolski, V.; Dredze, M.; Gehrmann, S.; Kambadur, P.; Rosenberg, D.; Mann, G. Bloomberggpt: A large language model for finance. *arXiv* **2023**, arXiv:2303.17564.
14. Araci, D. FinBERT: Financial Sentiment Analysis with Pre-trained Language Models. *arXiv* **2019**, arXiv:1908.10063.
15. Yang, H.; Liu, X.Y.; Wang, C.D. Fingpt: Open-source financial large language models. *arXiv* **2023**, arXiv:2306.06031. [CrossRef]
16. Zhao, Z.; Welsch, R.E. Aligning LLMs with Human Instructions and Stock Market Feedback in Financial Sentiment Analysis. *arXiv* **2024**, arXiv:2410.14926.
17. Yu, Y.; Yao, Z.; Li, H.; Deng, Z.; Cao, Y.; Chen, Z.; Suchow, J.W.; Liu, R.; Cui, Z.; Xu, Z.; et al. Fincon: A synthesized llm multi-agent system with conceptual verbal reinforcement for enhanced financial decision making. *arXiv* **2024**, arXiv:2407.06567.
18. Shah, S.; Ryali, S.; Venkatesh, R. Multi-Document Financial Question Answering using LLMs. *arXiv* **2024**, arXiv:2411.07264.
19. Wei, Q.; Yang, M.; Wang, J.; Mao, W.; Xu, J.; Ning, H. Tourllm: Enhancing llms with tourism knowledge. *arXiv* **2024**, arXiv:2407.12791.
20. Banerjee, A.; Satish, A.; Wörndl, W. Enhancing Tourism Recommender Systems for Sustainable City Trips Using Retrieval-Augmented Generation. *arXiv* **2024**, arXiv:2409.18003.
21. Wang, J.; Shalaby, A. Leveraging Large Language Models for Enhancing Public Transit Services. *arXiv* **2024**, arXiv:2410.14147.
22. Zhang, Z.; Sun, Y.; Wang, Z.; Nie, Y.; Ma, X.; Sun, P.; Li, R. Large language models for mobility in transportation systems: A survey on forecasting tasks. *arXiv* **2024**, arXiv:2405.02357.
23. Zhai, X.; Tian, H.; Li, L.; Zhao, T. Enhancing Travel Choice Modeling with Large Language Models: A Prompt-Learning Approach. *arXiv* **2024**, arXiv:2406.13558.
24. Mo, B.; Xu, H.; Zhuang, D.; Ma, R.; Guo, X.; Zhao, J. Large language models for travel behavior prediction. *arXiv* **2023**, arXiv:2312.00819.
25. Nie, Y.; Kong, Y.; Dong, X.; Mulvey, J.M.; Poor, H.V.; Wen, Q.; Zohren, S. A Survey of Large Language Models for Financial Applications: Progress, Prospects and Challenges. *arXiv* **2024**, arXiv:2406.11903.
26. Papasotiriou, K.; Sood, S.; Reynolds, S.; Balch, T. AI in Investment Analysis: LLMs for Equity Stock Ratings. In Proceedings of the 5th ACM International Conference on AI in Finance, Brooklyn, NY, USA, 14–17 November 2024; pp. 419–427.
27. Fatemi, S.; Hu, Y.; Mousavi, M. A Comparative Analysis of Instruction Fine-Tuning LLMs for Financial Text Classification. *arXiv* **2024**, arXiv:2411.02476.
28. Gebreab, S.A.; Salah, K.; Jayaraman, R.; ur Rehman, M.H.; Ellaham, S. Llm-based framework for administrative task automation in healthcare. In Proceedings of the 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 29–30 April 2024; pp. 1–7.
29. Cascella, M.; Montomoli, J.; Bellini, V.; Bignami, E. Evaluating the feasibility of ChatGPT in healthcare: An analysis of multiple clinical and research scenarios. *J. Med. Syst.* **2023**, *47*, 33. [CrossRef] [PubMed]
30. Palen-Michel, C.; Wang, R.; Zhang, Y.; Yu, D.; Xu, C.; Wu, Z. Investigating LLM Applications in E-Commerce. *arXiv* **2024**, arXiv:2408.12779.
31. Fang, C.; Li, X.; Fan, Z.; Xu, J.; Nag, K.; Korpeoglu, E.; Kumar, S.; Achan, K. Llm-ensemble: Optimal large language model ensemble method for e-commerce product attribute value extraction. In Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval, New York, NY, USA, 14–18 July 2024; pp. 2910–2914.
32. Yin, M.; Wu, C.; Wang, Y.; Wang, H.; Guo, W.; Wang, Y.; Liu, Y.; Tang, R.; Lian, D.; Chen, E. Entropy law: The story behind data compression and llm performance. *arXiv* **2024**, arXiv:2407.06645.
33. Kumar, R.; Kakde, S.; Rajput, D.; Ibrahim, D.; Nahata, R.; Sowjanya, P.; Kumar, D. Pretraining Data and Tokenizer for Indic LLM. *arXiv* **2024**, arXiv:2407.12481.
34. Lu, K.; Liang, Z.; Nie, X.; Pan, D.; Zhang, S.; Zhao, K.; Chen, W.; Zhou, Z.; Dong, G.; Zhang, W.; et al. Datasculpt: Crafting data landscapes for llm post-training through multi-objective partitioning. *arXiv* **2024**, arXiv:2409.00997.
35. Choe, S.K.; Ahn, H.; Bae, J.; Zhao, K.; Kang, M.; Chung, Y.; Pratapa, A.; Neiswanger, W.; Strubell, E.; Mitamura, T.; et al. What is Your Data Worth to GPT? LLM-Scale Data Valuation with Influence Functions. *arXiv* **2024**, arXiv:2405.13954.
36. Jiao, F.; Ding, B.; Luo, T.; Mo, Z. Panda llm: Training data and evaluation for open-sourced chinese instruction-following large language models. *arXiv* **2023**, arXiv:2305.03025.

37. Gan, Z.; Liu, Y. Towards a Theoretical Understanding of Synthetic Data in LLM Post-Training: A Reverse-Bottleneck Perspective. *arXiv* **2024**, arXiv:2410.01720.
38. Wood, D.; Lublinsky, B.; Roytman, A.; Singh, S.; Adam, C.; Adebayo, A.; An, S.; Chang, Y.C.; Dang, X.H.; Desai, N.; et al. Data-Prep-Kit: Getting your data ready for LLM application development. *arXiv* **2024**, arXiv:2409.18164.
39. Liu, Z. Cultural Bias in Large Language Models: A Comprehensive Analysis and Mitigation Strategies. *J. Transcult. Commun.* **2024**, *3*, 224–244. [CrossRef]
40. Khola, J.; Bansal, S.; Punia, K.; Pal, R.; Sachdeva, R. Comparative Analysis of Bias in LLMs through Indian Lenses. In Proceedings of the 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 12–14 July 2024; pp. 1–6. [CrossRef]
41. Talboy, A.N.; Fuller, E. Challenging the appearance of machine intelligence: Cognitive bias in LLMs and Best Practices for Adoption. *arXiv* **2023**, arXiv:2304.01358.
42. Faridoon, A.; Kechadi, M.T. Healthcare Data Governance, Privacy, and Security-A Conceptual Framework. In Proceedings of the EAI International Conference on Body Area Networks, Milan, Italy, 5–6 February 2024; Springer: Berlin/Heidelberg, Germany, 2024; pp. 261–271.
43. Gavgani, V.Z.; Pourrasmi, A. Data Governance Navigation for Advanced Operations in Healthcare Excellence. *Depiction Health* **2024**, *15*, 249–254. [CrossRef]
44. Raza, M.A. Cyber Security and Data Privacy in the Era of E-Governance. *Soc. Sci. J. Adv. Res.* **2024**, *4*, 5–9. [CrossRef]
45. Du, X.; Xiao, C.; Li, Y. Haloscope: Harnessing unlabeled llm generations for hallucination detection. *arXiv* **2024**, arXiv:2409.17504.
46. Li, R.; Bagade, T.; Martinez, K.; Yasmin, F.; Ayala, G.; Lam, M.; Zhu, K. A Debate-Driven Experiment on LLM Hallucinations and Accuracy. *arXiv* **2024**, arXiv:2410.19485.
47. Liu, X. A Survey of Hallucination Problems Based on Large Language Models. *Appl. Comput. Eng.* **2024**, *97*, 24–30. [CrossRef]
48. Reddy, G.P.; Pavan Kumar, Y.V.; Prakash, K.P. Hallucinations in Large Language Models (LLMs). In Proceedings of the 2024 IEEE Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 25 April 2024; pp. 1–6. [CrossRef]
49. Zhui, L.; Fenghe, L.; Xuehu, W.; Qining, F.; Wei, R. Ethical considerations and fundamental principles of large language models in medical education. *J. Med. Internet Res.* **2024**, *26*, e60083. [CrossRef]
50. Shah, S.B.; Thapa, S.; Acharya, A.; Rauniyar, K.; Poudel, S.; Jain, S.; Masood, A.; Naseem, U. Navigating the Web of Disinformation and Misinformation: Large Language Models as Double-Edged Swords. *IEEE Access* **2024**, 1. [CrossRef]
51. Ma, T. LLM Echo Chamber: Personalized and automated disinformation. *arXiv* **2024**, arXiv:2409.16241.
52. Pahune, S.; Akhtar, Z. Transitioning from MLOps to LLMOps: Navigating the Unique Challenges of Large Language Models. *Information* **2025**, *16*, 87. [CrossRef]
53. Tie, J.; Yao, B.; Li, T.; Ahmed, S.I.; Wang, D.; Zhou, S. LLMs are Imperfect, Then What? An Empirical Study on LLM Failures in Software Engineering. *arXiv* **2024**, arXiv:2411.09916.
54. Menshawy, A.; Nawaz, Z.; Fahmy, M. Navigating Challenges and Technical Debt in Large Language Models Deployment. In Proceedings of the 4th Workshop on Machine Learning and Systems—EuroMLSys '24, New York, NY, USA, 22 April 2024; pp. 192–199. [CrossRef]
55. Chen, T. Challenges and Opportunities in Integrating LLMs into Continuous Integration/Continuous Deployment (CI/CD) Pipelines. In Proceedings of the 2024 5th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Nanjing, China, 29–31 March 2024; pp. 364–367. [CrossRef]
56. Hu, S.; Wang, P.; Yao, Y.; Lu, Z. "I Always Felt that Something Was Wrong": Understanding Compliance Risks and Mitigation Strategies when Professionals Use Large Language Models. *arXiv* **2024**, arXiv:2411.04576.
57. Berger, A.; Hillebrand, L.; Leonhard, D.; Deußer, T.; De Oliveira, T.B.F.; Dilmaghani, T.; Khaled, M.; Kliem, B.; Loitz, R.; Bauckhage, C.; et al. Towards Automated Regulatory Compliance Verification in Financial Auditing with Large Language Models. In Proceedings of the 2023 IEEE International Conference on Big Data (BigData), Sorrento, Italy, 15–18 December 2023; pp. 4626–4635. [CrossRef]
58. Fakeyede, O.G.; Okeleke, P.A.; Hassan, A.; Iwuanyanwu, U.; Adaramodu, O.R.; Oyewole, O.O. Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *Int. J. Res. Eng. Sci.* **2023**, *11*, 184–192.
59. Aaronson, S.A. Data Dysphoria: The Governance Challenge Posed by Large Learning Models. 2023. Available online: https://ssrn.com/abstract=4554580 (accessed on 23 May 2025). [CrossRef]
60. Cheong, I.; Caliskan, A.; Kohno, T. Envisioning legal mitigations for LLM-based intentional and unintentional harms. In Proceedings of the 1st Workshop on Generative AI and Law (ICML 2022), Honolulu, HI, USA, 2022.
61. Glukhov, D.; Han, Z.; Shumailov, I.; Papyan, V.; Papernot, N. Breach By A Thousand Leaks: Unsafe Information Leakage inSafe'AI Responses. *arXiv* **2024**, arXiv:2407.02551.
62. Madhavan, D. Enterprise Data Governance: A Comprehensive Framework for Ensuring Data Integrity, Security, and Compliance in Modern Organizations. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2024**, *10*, 731–743. [CrossRef]

63. Rejeleene, R.; Xu, X.; Talburt, J. Towards trustable language models: Investigating information quality of large language models. *arXiv* **2024**, arXiv:2401.13086.
64. Yang, J.; Wang, Z.; Lin, Y.; Zhao, Z. Problematic Tokens: Tokenizer Bias in Large Language Models. In Proceedings of the 2024 IEEE International Conference on Big Data (BigData), Washington, DC, USA, 15–18 December 2024; pp. 6387–6393.
65. Balloccu, S.; Schmidtová, P.; Lango, M.; Dušek, O. Leak, cheat, repeat: Data contamination and evaluation malpractices in closed-source LLMs. *arXiv* **2024**, arXiv:2402.03927.
66. Abdelnabi, S.; Fay, A.; Cherubin, G.; Salem, A.; Fritz, M.; Paverd, A. Are you still on track!? Catching LLM Task Drift with Activations. *arXiv* **2024**, arXiv:2406.00799.
67. Würsch, M.; David, D.P.; Mermoud, A. Monitoring Emerging Trends in LLM Research. In *Large Language Models in Cybersecurity*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 153–161. [CrossRef]
68. Mannapur, S.B. Machine Learning Drift Detection and Concept Drift Analysis: Real-time Monitoring and Adaptive Model Maintenance. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2024**, *11*.
69. Pai, Y.T.; Sun, N.E.; Li, C.T.; Lin, S.d. Incremental Data Drifting: Evaluation Metrics, Data Generation, and Approach Comparison. *ACM Trans. Intell. Syst. Technol.* **2024**, *15*, 1–26. [CrossRef]
70. Sharma, V.; Mousavi, E.; Gajjar, D.; Madathil, K.; Smith, C.; Matos, N. Regulatory framework around data governance and external benchmarking. *J. Leg. Aff. Disput. Resolut. Eng. Constr.* **2022**, *14*, 04522006.
71. Vardia, A.S.; Chaudhary, A.; Agarwal, S.; Sagar, A.K.; Shrivastava, G. Cloud Security Essentials: A Detailed Exploration. *Emerg. Threat. Countermeas. Cybersecur.* **2025**, *14*, 413–432.
72. Sainz, O.; Campos, J.A.; García-Ferrero, I.; Etxaniz, J.; de Lacalle, O.L.; Agirre, E. Nlp evaluation in trouble: On the need to measure llm data contamination for each benchmark. *arXiv* **2023**, arXiv:2310.18018.
73. Perełkiewicz, M.; Poświata, R. A Review of the Challenges with Massive Web-mined Corpora Used in Large Language Models Pre-Training. *arXiv* **2024**, arXiv:2407.07630.
74. Jiao, J.; Afroogh, S.; Xu, Y.; Phillips, C. Navigating llm ethics: Advancements, challenges, and future directions. *arXiv* **2024**, arXiv:2406.18841.
75. Peng, B.; Chen, K.; Li, M.; Feng, P.; Bi, Z.; Liu, J.; Niu, Q. Securing large language models: Addressing bias, misinformation, and prompt attacks. *arXiv* **2024**, arXiv:2409.08087.
76. Mhammad, A.F.; Agarwal, R.; Columbo, T.; Vigorito, J. Generative & Responsible AI—LLMs Use in Differential Governance. In Proceedings of the 2023 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 13–25 December 2023; pp. 291–295. [CrossRef]
77. Kumari, B. Intelligent Data Governance Frameworks: A Technical Overview. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2024**, *10*, 141–154. [CrossRef]
78. Gupta, R.; Walker, L.; Corona, R.; Fu, S.; Petryk, S.; Napolitano, J.; Darrell, T.; Reddie, A.W. Data-Centric AI Governance: Addressing the Limitations of Model-Focused Policies. *arXiv* **2024**, arXiv:2409.17216.
79. Arigbabu, A.T.; Olaniyi, O.O.; Adigwe, C.S.; Adebiyi, O.O.; Ajayi, S.A. Data governance in AI-enabled healthcare systems: A case of the project nightingale. *Asian J. Res. Comput. Sci.* **2024**, *17*, 85–107. [CrossRef]
80. Yandrapalli, V. AI-Powered Data Governance: A Cutting-Edge Method for Ensuring Data Quality for Machine Learning Applications. In Proceedings of the 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 22–23 February 2024; pp. 1–6. Available online: https://ieeexplore.ieee.org/abstract/document/10493601 (accessed on 23 May 2025).
81. McGregor, S.; Hostetler, J. Data-centric governance. *arXiv* **2023**, arXiv:2302.07872.
82. Nathan, C.; Alalyani, A.; Serbanoiu, A.A.; Khan, D. AI-Powered Data Governance: Ensuring Integrity in Banking's Technological Frontier. *ResearchGate*. 2023. Available online: https://www.researchgate.net/publication/373296863_AI-Powered_Data_Governance_Ensuring_Integrity_in_Banking%27s_Technological_Frontier (accessed on 23 May 2025).
83. Tjondronegoro, D.W. Strategic AI Governance: Insights from Leading Nations. *arXiv* **2024**, arXiv:2410.01819.
84. Schiff, D.; Biddle, J.; Borenstein, J.; Laas, K. What's next for ai ethics, policy, and governance? A global overview. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, New York, NY, USA, 7–9 February 2020; pp. 153–158.
85. Arnold, G.; Ludwick, S.; Mohsen Fatemi, S.; Krause, R.; Long, L.A.N. Policy entrepreneurship for transformative governance. In *European Policy Analysis*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2024.
86. Jakubik, J.; Vössing, M.; Kühl, N.; Walk, J.; Satzger, G. Data-centric artificial intelligence. In *Business Information Systems Engineering*; Springer: Berlin/Heidelberg, Germany, 2024; Volume 66, pp. 507–515. [CrossRef]
87. Majeed, A.; Hwang, S.O. Technical analysis of data-centric and model-centric artificial intelligence. *IT Prof.* **2024**, *25*, 62–70. [CrossRef]
88. Gisolfi, N. Model-Centric Verification of Artificial Intelligence. Ph.D. Thesis, Carnegie Mellon University, Pittsburgh, PA, USA, 13 January 2022; pp. 1–237. Available online: https://www.ri.cmu.edu/app/uploads/2022/01/CMU-RI-TR-22-02.pdf (accessed on 23 May 2025).

89. Currie, N. Risk Based Approaches to Artificial Intelligence. *Crowe Data Management*. 2019. Available online: https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/Risk-Approaches-to-AI.pdf (accessed on 23 May 2025).
90. Lütge, C.; Hohma, E.; Boch, A.; Poszler, F.; Corrigan, C. On a Risk-Based Assessment Approach to AI Ethics Governance. Institute for Ethics in Artificial Intelligence, Technical University of Munich. 2022. Available online: https://www.ieai.sot.tum.de/wp-content/uploads/2022/06/IEAI-White-Paper-on-Risk-Management-Approach_2022-FINAL.pdf (accessed on 23 May 2025).
91. Lee, C.A.; Chow, K.; Chan, H.A.; Lun, D.P.K. Decentralized governance and artificial intelligence policy with blockchain-based voting in federated learning. *Front. Res. Metrics Anal.* **2023**, *8*, 1035123. [CrossRef]
92. Pencina, M.J.; McCall, J.; Economou-Zavlanos, N.J. A federated registration system for artificial intelligence in health. *JAMA* **2024**, *332*, 789–790. [CrossRef] [PubMed]
93. Lim, H.Y.F. Regulatory compliance. In *Artificial Intelligence*; Edward Elgar Publishing: London, UK, 17 March 2022; pp. 85–108. Available online: https://www.elgaronline.com/edcollchap/edcoll/9781800371712/9781800371712.00017.xml (accessed on 23 May 2025).
94. Aziza, O.R.; Uzougbo, N.S.; Ugwu, M.C. The impact of artificial intelligence on regulatory compliance in the oil and gas industry. *World J. Adv. Res. Rev.* **2023**, *19*, 1559–1570. [CrossRef]
95. Eitel-Porter, R. Beyond the promise: Implementing ethical AI. *AI Ethics* **2021**, *1*, 73–80. [CrossRef]
96. Daly, A.; Hagendorff, T.; Hui, L.; Mann, M.; Marda, V.; Wagner, B.; Wang, W.; Witteborn, S. Artificial intelligence governance and ethics: Global perspectives. *arXiv* **2019**, arXiv:1907.03848. [CrossRef]
97. Sidhpurwala, H.; Mollett, G.; Fox, E.; Bestavros, M.; Chen, H. Building Trust: Foundations of Security, Safety and Transparency in AI. *arXiv* **2024**, arXiv:2411.12275. [CrossRef]
98. Singh, K.; Saxena, R.; Kumar, B. AI Security: Cyber Threats and Threat-Informed Defense. In Proceedings of the 2024 8th Cyber Security in Networking Conference (CSNet), Paris, France, 4–6 December 2024; pp. 305–312.
99. Bowen, G.; Sothinathan, J.; Bowen, R. Technological Governance (Cybersecurity and AI): Role of Digital Governance. In *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 143–161.
100. Savaş, S.; Karataş, S. Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *Int. Cybersecur. Law Rev.* **2022**, *3*, 7–34. [CrossRef] [PubMed]
101. Lal, S.; Singh, B.; Kaunert, C. Role of Artificial Intelligence (AI) and Intellectual Property Rights (IPR) in Transforming Drug Discovery and Development in the Life Sciences: Legal and Ethical Concerns. *Libr. Prog. Libr. Sci. Inf. Technol. Comput.* **2024**, *44*, 7070. Available online: https://openurl.ebsco.com/EPDB%3Agcd%3A11%3A19455179/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A180917877&crl=c&link_origin=scholar.google.com (accessed on 23 May 2025).
102. Mirakhori, F.; Niazi, S.K. Harnessing the AI/ML in Drug and Biological Products Discovery and Development: The Regulatory Perspective. *Pharmaceuticals* **2025**, *18*, 47. [CrossRef] [PubMed]
103. Price, W.; Nicholson, I. Distributed governance of medical AI. *SMU Sci. Tech. L Rev.* **2022**, *25*, 3. [CrossRef]
104. Han, Y.; Tao, J. Revolutionizing Pharma: Unveiling the AI and LLM Trends in the Pharmaceutical Industry. *arXiv* **2024**, arXiv:2401.10273.
105. Tripathi, S.; Gabriel, K.; Tripathi, P.K.; Kim, E. Large language models reshaping molecular biology and drug development. *Chem. Biol. Drug Des.* **2024**, *103*, e14568. [CrossRef]
106. Liu, J.; Wang, C.; Liu, S. Applications of Large Language Models in Clinical Practice: Path, Challenges, and Future Perspectives. *OSF Preprints*. Center for Open Science. 2024. Available online: https://osf.io/preprints/osf/82bjd_v1 (accessed on 23 May 2025).
107. Dou, Y.; Zhao, X.; Zou, H.; Xiao, J.; Xi, P.; Peng, S. ShennongGPT: A Tuning Chinese LLM for Medication Guidance. In Proceedings of the 2023 IEEE International Conference on Medical Artificial Intelligence (MedAI), Beijing, China, 18–19 November 2023; pp. 67–72.
108. Zhao, H.; Liu, Z.; Wu, Z.; Li, Y.; Yang, T.; Shu, P.; Xu, S.; Dai, H.; Zhao, L.; Mai, G.; et al. Revolutionizing finance with llms: An overview of applications and insights. *arXiv* **2024**, arXiv:2401.11641.
109. Li, Y.; Wang, S.; Ding, H.; Chen, H. Large language models in finance: A survey. In Proceedings of the fourth ACM International Conference on AI in Finance, Brooklyn, NY, USA, 27–29 November 2023; pp. 374–382.
110. Kong, Y.; Nie, Y.; Dong, X.; Mulvey, J.M.; Poor, H.V.; Wen, Q.; Zohren, S. Large Language Models for Financial and Investment Management: Models, Opportunities, and Challenges. *J. Portf. Manag.* **2024**, *51*, 211–231. Available online: https://web.media.mit.edu/~xdong/paper/jpm24c.pdf (accessed on 23 May 2025). [CrossRef]
111. Yuan, Z.; Wang, K.; Zhu, S.; Yuan, Y.; Zhou, J.; Zhu, Y.; Wei, W. FinLLMs: A Framework for Financial Reasoning Dataset Generation with Large Language Models. *arXiv* **2024**, arXiv:2401.10744. [CrossRef]
112. Febrian, G.F.; Figueredo, G. KemenkeuGPT: Leveraging a Large Language Model on Indonesia's Government Financial Data and Regulations to Enhance Decision Making. *arXiv* **2024**, arXiv:2407.21459.

113. Clairoux-Trepanier, V.; Beauchamp, I.M.; Ruellan, E.; Paquet-Clouston, M.; Paquette, S.O.; Clay, E. The use of large language models (llm) for cyber threat intelligence (cti) in cybercrime forums. *arXiv* **2024**, arXiv:2408.03354.
114. Shafee, S.; Bessani, A.; Ferreira, P.M. Evaluation of llm chatbots for osint-based cyber threat awareness. *arXiv* **2024**, arXiv:2401.15127. [CrossRef]
115. Wang, F. Using large language models to mitigate ransomware threats. *Preprints*. 2023. Available online: https://www.preprints.org/manuscript/202311.0676/v1 (accessed on 23 May 2025).
116. Zangana, H.M. Harnessing the Power of Large Language Models. In *Application of Large Language Models (LLMs) for Software Vulnerability Detection*; IGI Global: Hershey, PA, USA, 2024; ISBN 9798369393130.
117. Yang, J.; Chi, Q.; Xu, W.; Yu, H. Research on adversarial attack and defense of large language models. *Appl. Comput. Eng.* **2024**, *93*, 105–113. [CrossRef]
118. Abdali, S.; Anarfi, R.; Barberan, C.; He, J. Securing Large Language Models: Threats, Vulnerabilities and Responsible Practices. *arXiv* **2024**, arXiv:2403.12503.
119. Ashiwal, V.; Finster, S.; Dawoud, A. Llm-based vulnerability sourcing from unstructured data. In Proceedings of the 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Vienna, Austria, 8–12 July 2024; pp. 634–641.
120. Srivastava, S.K.; Routray, S.; Bag, S.; Gupta, S.; Zhang, J.Z. Exploring the Potential of Large Language Models in Supply Chain Management: A Study Using Big Data. *J. Glob. Inf. Manag. (JGIM)* **2024**, *32*, 1–29. [CrossRef]
121. Wang, S.; Zhao, Y.; Hou, X.; Wang, H. Large language model supply chain: A research agenda. *ACM Trans. Softw. Eng. Methodol.* **2024**, *9*, 123–145. Available online: https://dl.acm.org/doi/abs/10.1145/3708531 (accessed on 23 May 2025). [CrossRef]
122. Xu, W.; Xiao, J.; Chen, J. Leveraging large language models to enhance personalized recommendations in e-commerce. In Proceedings of the 2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia, 30–31 October 2024; pp. 1–6.
123. Zhu, J.; Lin, J.; Dai, X.; Chen, B.; Shan, R.; Zhu, J.; Tang, R.; Yu, Y.; Zhang, W. Lifelong personalized low-rank adaptation of large language models for recommendation. *arXiv* **2024**, arXiv:2408.03533.
124. Mohanty, I. Recommendation Systems in the Era of LLMs. In Proceedings of the 15th Annual Meeting of the Forum for Information Retrieval Evaluation, Panjim, India, 15–18 December 2023; pp. 142–144.
125. Li, C.; Deng, Y.; Hu, H.; Kan, M.Y.; Li, H. Incorporating External Knowledge and Goal Guidance for LLM-based Conversational Recommender Systems. *arXiv* **2024**, arXiv:2405.01868.
126. Alhafni, B.; Vajjala, S.; Bannò, S.; Maurya, K.K.; Kochmar, E. Llms in education: Novel perspectives, challenges, and opportunities. *arXiv* **2024**, arXiv:2409.11917.
127. Leinonen, J.; MacNeil, S.; Denny, P.; Hellas, A. Using Large Language Models for Teaching Computing. In Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 2, Portland, OR, USA, 20–23 March 2024; p. 1901.
128. Zdravkova, K.; Dalipi, F.; Ahlgren, F. Integration of Large Language Models into Higher Education: A Perspective from Learners. In Proceedings of the 2023 International Symposium on Computers in Education (SIIE), Setúbal, Portugal, 16–18 November 2023; pp. 1–6.
129. Jadhav, D.; Agrawal, S.; Jagdale, S.; Salunkhe, P.; Salunkhe, R. AI-Driven Text-to-Multimedia Content Generation: Enhancing Modern Content Creation. In Proceedings of the 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 3–5 October 2024; pp. 1610–1615.
130. Li, S.; Li, X.; Chiariglione, L.; Luo, J.; Wang, W.; Yang, Z.; Mandic, D.; Fujita, H. Introduction to the Special Issue on AI-Generated Content for Multimedia. *IEEE Trans. Circuits Syst. Video Technol.* **2024**, *34*, 6809–6813. [CrossRef]
131. Yao, Y.; Duan, J.; Xu, K.; Cai, Y.; Sun, Z.; Zhang, Y. A survey on large language model (llm) security and privacy: The good, the bad, and the ugly. *High-Confid. Comput.* **2024**, *4*, 100211. ISSN 2667-2952. [CrossRef]
132. Nazi, Z.A.; Peng, W. Large language models in healthcare and medical domain: A review. *Informatics* **2024**, *11*, 57. [CrossRef]
133. Huang, J.; Chang, K.C.C. Citation: A key to building responsible and accountable large language models. *arXiv* **2023**, arXiv:2307.02185.
134. Liu, Y.; Yao, Y.; Ton, J.F.; Zhang, X.; Guo, R.; Cheng, H.; Klochkov, Y.; Taufiq, M.F.; Li, H. Trustworthy llms: A survey and guideline for evaluating large language models' alignment. *arXiv* **2023**, arXiv:2308.05374.
135. Carlini, N.; Tramèr, F.; Wallace, E.; Jagielski, M.; Herbert-Voss, A.; Lee, K.; Roberts, A.; Brown, T.; Song, D.; Erlingsson, Ú.; et al. Extracting Training Data from Large Language Models. In Proceedings of the 30th USENIX Security Symposium, Online, 11–13 August 2021; pp. 2633–2650, ISBN 978-1-939133-24-3. Available online: https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting (accessed on 23 May 2025).
136. Pan, X.; Zhang, M.; Ji, S.; Yang, M. Privacy risks of general-purpose language models. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; pp. 1314–1331.

137. Zimelewicz, E.; Kalinowski, M.; Mendez, D.; Giray, G.; Santos Alves, A.P.; Lavesson, N.; Azevedo, K.; Villamizar, H.; Escovedo, T.; Lopes, H.; et al. Ml-enabled systems model deployment and monitoring: Status quo and problems. In Proceedings of the International Conference on Software Quality, Vienna, Austria, 23–25 April 2024; Springer: Cham, Switzerland, 2024; pp. 112–131.
138. Bodor, A.; Hnida, M.; Najima, D. From Development to Deployment: An Approach to MLOps Monitoring for Machine Learning Model Operationalization. In Proceedings of the 2023 14th International Conference on Intelligent Systems: Theories and Applications (SITA), Casablanca, Morocco, 22–23 November 2023; pp. 1–7. [CrossRef]
139. Roberts, T.; Tonna, S.J. Extending the Governance Framework for Machine Learning Validation and Ongoing Monitoring. In *Risk Modeling: Practical Applications of Artificial Intelligence, Machine Learning, and Deep Learning*; Wiley: Hoboken, NJ, USA, 2022; Chapter 7. [CrossRef]
140. Nogare, D.; Silveira, I.F. EXPERIMENTATION, DEPLOYMENT AND MONITORING MACHINE LEARNING MODELS: APPROACHES FOR APPLYING MLOPS. *Revistaft* **2024**, *28*, 55. [CrossRef]
141. Mehdi, A.; Bali, M.K.; Abbas, S.I.; Singh, M. Unleashing the Potential of Grafana: A Comprehensive Study on Real-Time Monitoring and Visualization. In Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 6–8 July 2023; pp. 1–8. [CrossRef]
142. Samudrala, L.N.R. Automated SLA Monitoring in AWS Cloud Environments—A Comprehensive Approach Using Dynatrace. *J. Artif. Intell. Cloud Comput.* **2024**, *2*, 1–6. [CrossRef]
143. Menon, V.; Jesudas, J.; S.B, G. Model monitoring with grafana and dynatrace: A comprehensive framework for ensuring ml model performance. *Int. J. Adv. Res.* **2024**, *12*, 54–63. Available online: https://www.researchgate.net/publication/381030637_MODEL_MONITORING_WITH_GRAFANA_AND_DYNATRACE_A_COMPREHENSIVE_FRAMEWORK_FOR_ENSURING_ML_MODEL_PERFORMANCE (accessed on 23 May 2025). [CrossRef]
144. Yadav, S. Balancing Profitability and Risk: The Role of Risk Appetite in Mitigating Credit Risk Impact. *Int. Sci. J. Econ. Manag.* **2024**, *3*, 1–7. ISSN 2583-6129. Available online: https://isjem.com/download/balancing-profitability-and-risk-the-role-of-risk-appetite-in-mitigating-credit-risk-impact/ (accessed on 23 May 2025). [CrossRef]
145. Anil, V.K.S.; Babatope, A. Data privacy, security, and governance: A global comparative analysis of regulatory compliance and technological innovation. *Glob. J. Eng. Technol. Adv.* **2024**, *21*, 190–202. [CrossRef]
146. Zhang, S.; Ye, L.; Yi, X.; Tang, J.; Shui, B.; Xing, H.; Liu, P.; Li, H. "Ghost of the past": Identifying and resolving privacy leakage from LLM's memory through proactive user interaction. *arXiv* **2024**, arXiv:2410.14931.
147. Asthana, S.; Mahindru, R.; Zhang, B.; Sanz, J. Adaptive PII Mitigation Framework for Large Language Models. *arXiv* **2025**, arXiv:2501.12465.
148. Kalinin, M.; Poltavtseva, M.; Zegzhda, D. Ensuring the Big Data Traceability in Heterogeneous Data Systems. In Proceedings of the 2023 International Russian Automation Conference (RusAutoCon), Sochi, Russia, 10–16 September 2023; pp. 775–780. [CrossRef]
149. Falster, D.; FitzJohn, R.G.; Pennell, M.W.; Cornwell, W.K. Versioned data: Why it is needed and how it can be achieved (easily and cheaply). *PeerJ Prepr.* **2017**, *5*, e3401v1.
150. Mirchandani, S.; Xia, F.; Florence, P.; Ichter, B.; Driess, D.; Arenas, M.G.; Rao, K.; Sadigh, D.; Zeng, A. Large language models as general pattern machines. *arXiv* **2023**, arXiv:2307.04721.
151. Chen, Y.; Zhao, Y.; Li, X.; Zhang, J.; Long, J.; Zhou, F. An open dataset of data lineage graphs for data governance research. *Vis. Inform.* **2024**, *8*, 1–5. [CrossRef]
152. Kramer, S.G. Artificial Intelligence in the Supply Chain: Legal Issues and Compliance Challenges. *J. Supply Chain. Manag. Logist. Procure.* **2024**, *7*, 139–148. [CrossRef]
153. Hausenloy, J.; McClements, D.; Thakur, M. Towards Data Governance of Frontier AI Models. *arXiv* **2024**, arXiv:2412.03824.
154. Liu, Y.; Zhang, D.; Xia, B.; Anticev, J.; Adebayo, T.; Xing, Z.; Machao, M. Blockchain-Enabled Accountability in Data Supply Chain: A Data Bill of Materials Approach. In Proceedings of the 2024 IEEE International Conference on Blockchain (Blockchain), Copenhagen, Denmark, 19–22 August 2024; pp. 557–562.
155. Azari, M.; Arif, J.; Moustabchir, H.; Jawab, F. Navigating Challenges and Leveraging Future Trends in AI and Machine Learning for Supply Chains. In *AI and Machine Learning Applications in Supply Chains and Marketing*; Masengu, R., Tsikada, C., Garwi, J., Eds.; IGI Global Scientific Publishing: Hershey, PA, USA 2025; pp. 257–282. [CrossRef]
156. Hussein, R.; Zink, A.; Ramadan, B.; Howard, F.M.; Hightower, M.; Shah, S.; Beaulieu-Jones, B.K. Advancing Healthcare AI Governance: A Comprehensive Maturity Model Based on Systematic Review. *medRxiv* **2024**.
157. Singh, B.; Kaunert, C.; Jermsittiparsert, K. Managing Health Data Landscapes and Blockchain Framework for Precision Medicine, Clinical Trials, and Genomic Biomarker Discovery. In *Digitalization and the Transformation of the Healthcare Sector*; Wickramasinghe, N., Ed.; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 283–310. [CrossRef]
158. Hassan, M.; Borycki, E.M.; Kushniruk, A.W. Artificial intelligence governance framework for healthcare. *Healthc. Manag. Forum* **2024**, *38*, 125–130. [CrossRef]

159. Chakraborty, A.; Karhade, M. Global AI Governance in Healthcare: A Cross-Jurisdictional Regulatory Analysis. *arXiv* **2024**, arXiv:2406.08695.
160. Kim, J.; Kim, S.Y.; Kim, E.A.; Sim, J.; Lee, Y.; Kim, H. Developing a Framework for Self-regulatory Governance in Healthcare AI Research: Insights from South Korea. *Asia-Pac. Biotech Res. (ABR)* **2024**, *16*, 391–406. [CrossRef] [PubMed]
161. Olimid, A.P.; Georgescu, C.M.; Olimid, D.A. Legal Analysis of EU Artificial Intelligence Act (2024): Insights from Personal Data Governance and Health Policy. *Access Just. E. Eur.* **2024**, *7*, 120.
162. Kolade, T.M.; Aideyan, N.T.; Oyekunle, S.M.; Ogungbemi, O.S.; Dapo-Oyewole, D.L.; Olaniyi, O.O. Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security. *Asian J. Res. Comput. Sci.* **2024**, *17*, 36–57. [CrossRef]
163. Mbah, G.O.; Evelyn, A.N. AI-powered cybersecurity: Strategic approaches to mitigate risk and safeguard data privacy. *World J. Adv. Res. Rev.* **2024**, *24*, 310–327. [CrossRef]
164. Folorunso, A.; Adewumi, T.; Adewa, A.; Okonkwo, R.; Olawumi, T.N. Impact of AI on cybersecurity and security compliance. *Glob. J. Eng. Technol. Adv.* **2024**, *21*, 167–184. [CrossRef]
165. Jabbar, H.; Al-Janabi, S.; Syms, F. AI-Integrated Cyber Security Risk Management Framework for IT Projects. In Proceedings of the 2024 International Jordanian Cybersecurity Conference (IJCC), Amman, Jordan, 17–18 December 2024; pp. 76–81. [CrossRef]
166. Muhammad, M.H.B.; Abas, Z.B.; Ahmad, A.S.B.; Sulaiman, M.S.B. AI-Driven Security: Redefining Security Information Systems within Digital Governance. *Int. J. Res. Inf. Secur. Syst. (IJRISS)* **2024**, *8090245*, 2923–2936. [CrossRef]
167. Effoduh, J.; Akpudo, U.; Kong, J. Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa. *Data Policy* **2024**, *6*, e34. [CrossRef]
168. Jyothi, V.E.; Sai Kumar, D.L.; Thati, B.; Tondepu, Y.; Pratap, V.K.; Praveen, S.P. Secure Data Access Management for Cyber Threats using Artificial Intelligence. In Proceedings of the 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 1–3 December 2022; pp. 693–697. [CrossRef]
169. Boggarapu, N.B. Modernizing Banking Compliance: An Analysis of AI-Powered Data Governance in a Hybrid Cloud Environment. *CSEIT* **2024**, *10*, 2434. [CrossRef]
170. Akokodaripon, D.; Alonge-Essiet, F.O.; Aderoju, A.V.; Reis, O. Implementing Data Governance in Financial Systems: Strategies for Ensuring Compliance and Security in Multi-Source Data Integration Projects. *CSI Trans. ICT Res.* **2024**, *5*, 1631. [CrossRef]
171. Chukwurah, N.; Ige, A.B.; Adebayo, V.I.; Eyieyien, O.G. Frameworks for Effective Data Governance: Best Practices, Challenges, and Implementation Strategies Across Industries. *Comput. Sci. IT Res. J.* **2024**, *5*, 1666–1679. [CrossRef]
172. Li, Y.; Yu, X.; Koudas, N. Data Acquisition for Improving Model Confidence. *Proc. Acm Manag. Data* **2024**, *2*, 1–25. [CrossRef]
173. Barrenechea, O.; Mendieta, A.; Armas, J.; Madrid, J.M. Data Governance Reference Model to streamline the supply chain process in SMEs. In Proceedings of the 2019 IEEE XXVI International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Lima, Peru, 12–14 August 2019; pp. 1–4.
174. Aghaei, R.; Kiaei, A.A.; Boush, M.; Vahidi, J.; Barzegar, Z.; Rofoosheh, M. The Potential of Large Language Models in Supply Chain Management: Advancing Decision-Making, Efficiency, and Innovation. *arXiv* **2025**, arXiv:2501.15411.
175. Tse, D.; Chow, C.k.; Ly, T.p.; Tong, C.y.; Tam, K.w. The challenges of big data governance in healthcare. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1632–1636.
176. Tripathi, S.; Mongeau, K.; Alkhulaifat, D.; Elahi, A.; Cook, T.S. Large language models in health systems: Governance, challenges, and solutions. *Acad. Radiol.* **2025**, *32*, 1189–1191. [CrossRef] [PubMed]
177. Salman, A.; Creese, S.; Goldsmith, M. Position Paper: Leveraging Large Language Models for Cybersecurity Compliance. In Proceedings of the 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Vienna, Austria, 8–12 July 2024; pp. 496–503.
178. McIntosh, T.R.; Susnjak, T.; Liu, T.; Watters, P.; Xu, D.; Liu, D.; Nowrozy, R.; Halgamuge, M.N. From cobit to iso 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Comput. Secur.* **2024**, *144*, 103964. [CrossRef]
179. Tavasoli, A.; Sharbaf, M.; Madani, S.M. Responsible Innovation: A Strategic Framework for Financial LLM Integration. *arXiv* **2025**, arXiv:2504.02165.
180. Chu, Z.; Guo, H.; Zhou, X.; Wang, Y.; Yu, F.; Chen, H.; Xu, W.; Lu, X.; Cui, Q.; Li, L.; et al. Data-centric financial large language models. *arXiv* **2023**, arXiv:2310.17784.
181. Zhou, X.; Zhao, X.; Li, G. LLM-Enhanced Data Management. *arXiv* **2024**, arXiv:2402.02643.
182. Gorti, A.; Chadha, A.; Gaur, M. Unboxing Occupational Bias: Debiasing LLMs with US Labor Data. In *Proceedings of the AAAI Symposium Series, Arlington, Virginia, 20 August 2024*; AAAI Press: Washington, DC, USA, 2024; Volume 4, pp. 48–55.
183. de Dampierre, C.; Mogoutov, A.; Baumard, N. Towards Transparency: Exploring LLM Trainings Datasets through Visual Topic Modeling and Semantic Frame. *arXiv* **2024**, arXiv:2406.06574.

184. Yang, J.; Wang, Z.; Lin, Y.; Zhao, Z. Global Data Constraints: Ethical and Effectiveness Challenges in Large Language Model. *arXiv* **2024**, arXiv:2406.11214.
185. Li, C.; Zhuang, Y.; Qiang, R.; Sun, H.; Dai, H.; Zhang, C.; Dai, B. Matryoshka: Learning to Drive Black-Box LLMs with LLMs. *arXiv* **2024**, arXiv:2410.20749.
186. Alber, D.A.; Yang, Z.; Alyakin, A.; Yang, E.; Rai, S.; Valliani, A.A.; Zhang, J.; Rosenbaum, G.R.; Amend-Thomas, A.K.; Kurland, D.B.; et al. Medical large language models are vulnerable to data-poisoning attacks. *Nat. Med.* **2025**, *31*, 618–626. [CrossRef]
187. Wu, F.; Cui, L.; Yao, S.; Yu, S. Inference Attacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions. *arXiv* **2024**, arXiv:2406.02027.
188. Subramaniam, P.; Krishnan, S. Intent-Based Access Control: Using LLMs to Intelligently Manage Access Control. *arXiv* **2024**, arXiv:2402.07332.
189. Mehra, T. The Critical Role of Role-Based Access Control (RBAC) in securing backup, recovery, and storage systems. *Int. J. Sci. Res. Arch.* **2024**, *13*, 1192–1194. [CrossRef]
190. Li, L.; Chen, H.; Qiu, Z.; Luo, L. Large Language Models in Data Governance: Multi-source Data Tables Merging. In Proceedings of the 2024 IEEE International Conference on Big Data (BigData), Washington, DC, USA, 15–18 December 2024; pp. 3965–3974.
191. Kayali, M.; Wenz, F.; Tatbul, N.; Demiralp, Ç. Mind the Data Gap: Bridging LLMs to Enterprise Data Integration. *arXiv* **2024**, arXiv:2412.20331.
192. Erdem, O.; Hassett, K.; Egriboyun, F. Evaluating the Accuracy of Chatbots in Financial Literature. *arXiv* **2024**, arXiv:2411.07031.
193. Ruke, A.; Kulkarni, H.; Patil, R.; Pote, A.; Shedage, S.; Patil, A. Future Finance: Predictive Insights and Chatbot Consultation. In Proceedings of the 2024 4th Asian Conference on Innovation in Technology (ASIANCON), Pimari Chinchwad, India, 23–25 August 2024; pp. 1–5. [CrossRef]
194. Zheng, Z. ChatGPT-style Artificial Intelligence for Financial Applications and Risk Response. *Int. J. Comput. Sci. Inf. Technol.* **2024**, *3*, 179–186. [CrossRef]
195. Kushwaha, P.K.; Kumar, R.; Kumar, S. AI Health Chatbot using ML. *Int. J. Sci. Res. Eng. Manag. (IJSREM)* **2024**, *8*, 1–5. [CrossRef]
196. Hassani, S. Enhancing Legal Compliance and Regulation Analysis with Large Language Models. In Proceedings of the 2024 IEEE 32nd International Requirements Engineering Conference (RE), Reykjavik, Iceland, 24–28 June 2024; pp. 507–511. [CrossRef]
197. Kumar, B.; Roussinov, D. NLP-based Regulatory Compliance–Using GPT 4.0 to Decode Regulatory Documents. *arXiv* **2024**, arXiv:2412.20602.
198. Kaur, P.; Kashyap, G.S.; Kumar, A.; Nafis, M.T.; Kumar, S.; Shokeen, V. From Text to Transformation: A Comprehensive Review of Large Language Models' Versatility. *arXiv* **2024**, arXiv:2402.16142.
199. Zhu, H. Architectural Foundations for the Large Language Model Infrastructures. *arXiv* **2024**, arXiv:2408.09205.
200. Koppichetti, R.K. Framework of Hub and Spoke Data Governance Model for Cloud Computing. *J. Artif. Intell. Cloud Comput.* **2024**, *2*, 1–4. Available online: https://onlinescientificresearch.com/articles/framework-of-hub-and-spoke-data-governance-model-for-cloud-computing.pdf (accessed on 23 May 2025). [CrossRef]
201. Li, D.; Sun, Z.; Hu, X.; Hu, B.; Zhang, M. CMT: A Memory Compression Method for Continual Knowledge Learning of Large Language Models. *arXiv* **2024**, arXiv:2412.07393. [CrossRef]
202. Folorunso, A.; Babalola, O.; Nwatu, C.E.; Ukonne, U. Compliance and Governance issues in Cloud Computing and AI: USA and Africa. *Glob. J. Eng. Technol. Adv.* **2024**, *21*, 127–138. [CrossRef]
203. Alsaigh, R.; Mehmood, R.; Katib, I.; Liang, X.; Alshanqiti, A.; Corchado, J.M.; See, S. Harmonizing AI governance regulations and neuroinformatics: Perspectives on privacy and data sharing. *Front. Neuroinformatics* **2024**, *18*, 1472653. [CrossRef]
204. Zhang, C.; Zhong, H.; Zhang, K.; Chai, C.; Wang, R.; Zhuang, X.; Bai, T.; Qiu, J.; Cao, L.; Fan, J.; et al. Harnessing Diversity for Important Data Selection in Pretraining Large Language Models. *arXiv* **2024**, arXiv:2409.16986.
205. Rajasegar, R.; Gouthaman, P.; Ponnusamy, V.; Arivazhagan, N.; Nallarasan, V. Data Privacy and Ethics in Data Analytics. In *Data Analytics and Machine Learning: Navigating the Big Data Landscape*; Springer: Berlin/Heidelberg, Germany, 2024; Volume 145, pp. 195–213. [CrossRef]
206. Pang, J.; Wei, J.; Shah, A.P.; Zhu, Z.; Wang, Y.; Qian, C.; Liu, Y.; Bao, Y.; Wei, W. Improving data efficiency via curating llm-driven rating systems. *arXiv* **2024**, arXiv:2410.10877.
207. Seedat, N.; Huynh, N.; van Breugel, B.; van der Schaar, M. Curated llm: Synergy of llms and data curation for tabular augmentation in ultra low-data regimes. In Proceedings of the International Conference on Learning Representations (ICLR) 2024, Vienna, Austria, 7–11 May 2024. Available online: https://openreview.net/forum?id=ynguffsGfa (accessed on 23 May 2025).
208. Oktavia, T.; Wijaya, E. Strategic Metadata Implementation: A Catalyst for Enhanced BI Systems and Organizational Effectiveness. *Hightech Innov. J.* **2025**, *6*, 21–41. [CrossRef]
209. Walshe, T.; Moon, S.Y.; Xiao, C.; Gunawardana, Y.; Silavong, F. Automatic Labelling with Open-source LLMs using Dynamic Label Schema Integration. *arXiv* **2025**, arXiv:2501.12332.

210. Cholke, P.C.; Patankar, A.; Patil, A.; Patwardhan, S.; Phand, S. Enabling Dynamic Schema Modifications Through Codeless Data Management. In Proceedings of the 2024 IEEE Region 10 Symposium (TENSYMP), New Delhi, India, 27–29 September 2024; pp. 1–9.
211. Strome, T. Data governance best practices for the AI-ready airport. *J. Airpt. Manag.* **2024**, *19*, 57–70. [CrossRef]
212. Suhra, R. Unified Data Governance Strategy for Enterprises. *Int. J. Comput. Appl.* **2024**, *186*, 36–41. Available online: https://www.ijcaonline.org/archives/volume186/number50/transforming-enterprise-data-management-through-unified-data-governance/ (accessed on 23 May 2025).
213. Aiyankovil, K.G.; Lewis, D.; Hernandez, J. Mapping Data Governance Requirements Between the European Union's AI Act and ISO/IEC 5259: A Semantic Analysis. In Proceedings of the NeXt-generation Data Governance Workshop, Amsterdam, The Netherlands, 17–19 September 2024.
214. Aiyankovil, K.G.; Lewis, D. Harmonizing AI Data Governance: Profiling ISO/IEC 5259 to Meet the Requirements of the EU AI Act. *Front. Artif. Intell. Appl.* **2024**, *395*, 363–365. [CrossRef]
215. Gupta, P.; Parmar, D.S. Sustainable Data Management and Governance Using AI. *World J. Adv. Eng. Technol. Sci.* **2024**, *13*, 264–274. [CrossRef]
216. Idemudia, C.; Ige, A.; Adebayo, V.; Eyieyien, O. Enhancing data quality through comprehensive governance: Methodologies, tools, and continuous improvement techniques. *Comput. Sci. IT Res. J.* **2024**, *5*, 1680–1694. [CrossRef]
217. Comeau, D.S.; Bitterman, D.S.; Celi, L.A. Preventing unrestricted and unmonitored AI experimentation in healthcare through transparency and accountability. *Npj Digit. Med.* **2025**, *8*, 42. [CrossRef]
218. Organisation for Economic Co-operation and Development. *Towards an Integrated Health Information System in the Netherlands*; Technical Report; Organisation for Economic Co-operation and Development (OECD): Paris, France, 2022.
219. Musa, M.B.; Winston, S.M.; Allen, G.; Schiller, J.; Moore, K.; Quick, S.; Melvin, J.; Srinivasan, P.; Diamantis, M.E.; Nithyanand, R. C3PA: An Open Dataset of Expert-Annotated and Regulation-Aware Privacy Policies to Enable Scalable Regulatory Compliance Audits. *arXiv* **2024**, arXiv:2410.03925.
220. Eshbaev, G. GDPR vs. Weakly Protected Parties in Other Countries. *Uzb. J. Law Digit. Policy* **2024**, *2*, 55–65. [CrossRef]
221. Borgesius, F.Z.; Asghari, H.; Bangma, N.; Hoepman, J.H. The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects. *SCRIPTed* **2023**, *20*, 352. [CrossRef]
222. Musch, S.; Borrelli, M.C.; Kerrigan, C. Bridging Compliance and Innovation: A Comparative Analysis of the EU AI Act and GDPR for Enhanced Organisational Strategy. *J. Data Prot. Priv.* **2024**, *7*, 14–40. [CrossRef]
223. Aziz, M.A.B.; Wilson, C. Johnny Still Can't Opt-out: Assessing the IAB CCPA Compliance Framework. *Proc. Priv. Enhancing Technol.* **2024**, *2024*, 349–363. [CrossRef]
224. Rao, S.D. The Evolution of Privacy Rights in the Digital Age: A Comparative Analysis of GDPR and CCPA. *Int. J. Law* **2024**, *2*, 40. [CrossRef]
225. Harding, E.L.; Vanto, J.J.; Clark, R.; Hannah Ji, L.; Ainsworth, S.C. Understanding the scope and impact of the california consumer privacy act of 2018. *J. Data Prot. Priv.* **2019**, *2*, 234–253. [CrossRef]
226. Charatan, J.; Birrell, E. Two Steps Forward and One Step Back: The Right to Opt-out of Sale under CPRA. *Proc. Priv. Enhancing Technol.* **2024**, *2024*, 91–105. [CrossRef]
227. Wang, G. Administrative and Legal Protection of Personal Information in China: Disadvantages and Solutions. In *Courier of Kutafin Moscow State Law University (MSAL)*; MGIMO University Press: Moscow, Russia, 2024; pp. 189–197, ISSN 2311-5998. [CrossRef]
228. Yang, L.; Lin, Y.; Chen, B. Practice and Prospect of Regulating Personal Data Protection in China. *Laws* **2024**, *13*, 78. [CrossRef]
229. Bolatbekkyzy, G. Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation. *Gron. J. Int. Law* **2024**, *11*, 129–146. [CrossRef]
230. Yalamati, S. Ensuring Ethical Practices in AI and ML Toward a Sustainable Future. In *Artificial Intelligence and Machine Learning for Sustainable Development*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2024; p. 15. [CrossRef]
231. Zhu, M.; Zhang, W.; Xu, C. Ethical Governance and Implementation Paths for Global Marine Science Data Sharing. *Front. Mar. Sci.* **2024**, *11*, 1421252. [CrossRef]
232. Sharma, K.; Kumar, P.; Özen, E. Ethical Considerations in Data Analytics: Challenges, Principles, and Best Practices. In *Data Alchemy in the Insurance Industry*; Taneja, S., Kumar, P., Reepu, Kukreti, M., Özen, E., Eds.; Emerald Publishing Limited: Leeds, UK, 2024; pp. 41–48. [CrossRef]
233. McNicol, T.; Carthouser, B.; Bongiovanni, I.; Abeysooriya, S. Improving Ethical Usage of Corporate Data in Higher Education: Enhanced Enterprise Data Ethics Framework. *Inf. Technol. People* **2024**, *37*, 2247–2278. [CrossRef]
234. Kottur, R. Responsible AI Development: A Comprehensive Framework for Ethical Implementation in Contemporary Technological Systems. *Comput. Sci. Inf. Technol.* **2024**, *10*, 1553–1561. [CrossRef]
235. Sharma, R.K. Ethics in AI: Balancing innovation and responsibility. *Int. J. Sci. Res. Arch.* **2025**, *14*, 544–551. [CrossRef]

236. Díaz-Rodríguez, N.; Del Ser, J.; Coeckelbergh, M.; de Prado, M.L.; Herrera-Viedma, E.; Herrera, F. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Inf. Fusion* **2023**, *99*, 101896. [CrossRef]
237. Zisan, T.I.; Pulok, M.M.K.; Borman, D.; Barmon, R.C.; Asif, M.R.H. Navigating the Future of Auditing: AI Applications, Ethical Considerations, and Industry Perspectives on Big Data. *Eur. J. Theor. Appl. Sci.* **2024**, *2*, 324–332. [CrossRef]
238. Sari, R.; Muslim, M. Accountability and Transparency in Public Sector Accounting: A Systematic Review. *AMAR Account. Manag. Rev.* **2023**, *3*, 1440. [CrossRef]
239. Felix, S.; Morais, M.G.; Fonseca, J. The role of internal audit in supporting the implementation of the general regulation on data protection—Case study in the intermunicipal communities of Coimbra and Viseu. In Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 13–16 June 2018; pp. 1–7. [CrossRef]
240. Weaver, L.; Imura, P. System and Method of Conducting Self Assessment for Regulatory Compliance. U.S. Patent App. 14/497,436, 31 March 2016.
241. Brenner, J. ISO 27001: Risk management and compliance. *Risk Manag.* **2007**, *54*, 24.
242. Malatji, M. Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In Proceedings of the 2023 International conference on cyber management and engineering (CyMaEn), Bangkok, Thailand, 26–27 January 2023; pp. 117–122.
243. Segun-Falade, O.D.; Leghemo, I.M.; Odionu, C.S.; Azubuike, C. A Review on [Insert Paper Topic]. *Int. J. Sci. Res. Arch.* **2024**, *12*, 2984–3002. [CrossRef]
244. Janssen, M.; Brous, P.; Estevez, E.; Barbosa, L.S.; Janowski, T. Data governance: Organizing data for trustworthy Artificial Intelligence. *Gov. Inf. Q.* **2020**, *37*, 101493. [CrossRef]
245. Olateju, O.; Okon, S.U.; Olaniyi, O.O.; Samuel-Okon, A.D.; Asonze, C.U. Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data. *J. Eng. Res. Rep.* **2024**, *26*, 244–268. Available online: https://journaljerr.com/index.php/JERR/article/view/1206 (accessed on 23 May 2025).
246. Friha, O.; Ferrag, M.A.; Kantarci, B.; Cakmak, B.; Ozgun, A.; Ghoualmi-Zine, N. Llm-based edge intelligence: A comprehensive survey on architectures, applications, security and trustworthiness. *IEEE Open J. Commun. Soc.* **2024**, *5*, 5799–5856. Available online: https://ieeexplore.ieee.org/abstract/document/10669603 (accessed on 23 May 2025). [CrossRef]
247. Leghemo, I.M.; Azubuike, C.; Segun-Falade, O.D.; Odionu, C.S. Data Governance for Emerging Technologies: A Conceptual Framework for Managing Blockchain, IoT, and AI. *J. Eng. Res. Rep.* **2025**, *27*, 247–267. [CrossRef]
248. O'Sullivan, K.; Lumsden, J.; Anderson, C.; Black, C.; Ball, W.; Wilde, K. A Governance Framework for Facilitating Cross-Agency Data Sharing. *Int. J. Popul. Data Sci.* **2024**, *9*. [CrossRef]
249. Bammer, G. Stakeholder Engagement. In *Sociology, Social Policy and Education 2024*; Edward Elgar Publishing: Bingley, UK, 2024; pp. 487–491. [CrossRef]
250. Demiris, G. Stakeholder Engagement for the Design of Generative AI Tools: Inclusive Design Approaches. *Innov. Aging* **2024**, *8*, 585–586. [CrossRef]
251. Siew, R. Stakeholder Engagement. In *Sustainability Analytics Toolkit for Practitioners*; Palgrave Macmillan: Singapore, 2023. [CrossRef]
252. Arora, A.; Vats, P.; Tomer, N.; Kaur, R.; Saini, A.K.; Shekhawat, S.S.; Roopak, M. Data-Driven Decision Support Systems in E-Governance: Leveraging AI for Policymaking. In *Artificial Intelligence: Theory and Applications*; Lecture Notes in Networks and Systems; Sharma, H., Chakravorty, A., Hussain, S., Kumari, R., Eds.; Springer: Singapore, 3 January 2024; Volume 844. [CrossRef]
253. Luo, J.; Luo, X.; Chen, X.; Xiao, Z.; Ju, W.; Zhang, M. SemiEvol: Semi-supervised Fine-tuning for LLM Adaptation. *arXiv* **2024**, arXiv:2410.14745.
254. Uuk, R.; Brouwer, A.; Schreier, T.; Dreksler, N.; Pulignano, V.; Bommasani, R. Effective Mitigations for Systemic Risks from General-Purpose AI. SSRN, 2024. Available online: https://ssrn.com/abstract=5021463 (accessed on 23 May 2025).
255. Nadeem, M.; Bethke, A.; Reddy, S. StereoSet: Measuring stereotypical bias in pretrained language models. *arXiv* **2020**, arXiv:2004.09456.
256. Robinson, R. Assessing gender bias in medical and scientific masked language models with StereoSet. *arXiv* **2021**, arXiv:2111.08088.
257. Bird, S.; Dudík, M.; Edgar, R.; Horn, B.; Lutz, R.; Milan, V.; Sameki, M.; Wallach, H.; Walker, K. Fairlearn: A Toolkit for Assessing and Improving Fairness in AI. Microsoft Research Technical Report MSR-TR-2020-32. 2020. Available online: https://www.microsoft.com/en-us/research/wp-content/uploads/2020/05/Fairlearn_WhitePaper-2020-09-22.pdf (accessed on 23 May 2025).
258. Saleiro, P.; Kuester, B.; Hinkson, L.; London, J.; Stevens, A.; Anisfeld, A.; Rodolfa, K.T.; Ghani, R. Aequitas: A bias and fairness audit toolkit. *arXiv* **2018**, arXiv:1811.05577.
259. Rella, B.P.R. MLOPs and DataOps integration for scalable machine learning deployment. *Int. J. Multidiscip. Res.* **2022**, *4*, 20.
260. TruEra. TruEra Monitoring Delivers Important ML Model Insights Fast. 2023. Available online: https://truera.com/ai-quality-education/ml-monitoring/truera-ml-monitoring-delivers-important-ml-model-insights/ (accessed on 18 May 2025).

261. Bate, A.B.d.A.R. Auditable Data Provenance in Streaming Data Processing. Master's Thesis, Instituto Superior Técnico, University of Lisbon, Lisbon, Portugal, 2023.
262. Zaharia, M.; Chen, A.; Davidson, A.; Ghodsi, A.; Hong, S.A.; Konwinski, A.; Murching, S.; Nykodym, T.; Ogilvie, P.; Parkhe, M.; et al. Accelerating the machine learning lifecycle with MLflow. *IEEE Data Eng. Bull.* **2018**, *41*, 39–45.
263. Gadepally, V.; Kepner, J. Technical Report: Developing a Working Data Hub. *arXiv* **2020**, arXiv:2004.00190.
264. Alvarez-Romero, C.; Martínez-García, A.; Bernabeu-Wittel, M.; Parra-Calderón, C.L. Health data hubs: An analysis of existing data governance features for research. *Health Res. Policy Syst.* **2023**, *21*, 70. [CrossRef]
265. Gade, K.R. Data Quality Metrics for the Modern Enterprise: A Data Analytics Perspective. *MZ J. Artif. Intell.* **2024**, *1*. Available online: https://mzresearch.com/index.php/MZJAI/article/view/416 (accessed on 23 May 2025).
266. Yang, W.; Fu, R.; Amin, M.B.; Kang, B. Impact and influence of modern AI in metadata management. *arXiv* **2025**, arXiv:2501.16605.
267. Muppalaneni, R.; Inaganti, A.C.; Ravichandran, N. AI-Enhanced Data Loss Prevention (DLP) Strategies for Multi-Cloud Environments. *J. Comput. Innov. Appl.* **2024**, *2*, 1–13.
268. Naik, S. Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy. *Eastasouth J. Inf. Syst. Comput. Sci.* **2023**, *1*, 69–87. [CrossRef]
269. AIMultiple Research Team. Data Governance Case Studies. 2024. Available online: https://research.aimultiple.com/data-governance-case-studies/ (accessed on 14 March 2025).
270. Google Cloud. Data Governance in Generative AI—Vertex AI. 2024. Available online: https://cloud.google.com/vertex-ai/generative-ai/docs/data-governance (accessed on 14 March 2025).
271. Microsoft. AI Principles and Approach. 2024. Available online: https://www.microsoft.com/en-us/ai/principles-and-approach (accessed on 14 March 2025).
272. Microsoft. Introducing Modern Data Governance for the Era of AI. 2024. Available online: https://azure.microsoft.com/en-us/blog/introducing-modern-data-governance-for-the-era-of-ai/ (accessed on 14 March 2025).
273. Majumder, S.; Bhattacharjee, A.; Kozhaya, J.N. Enhancing AI Governance in Financial Industry through IBM watsonx.governance. *TechRxiv*. 30 March 2024. Available online: https://www.techrxiv.org/doi/full/10.36227/techrxiv.171177466.65923432 (accessed on 14 March 2025).
274. Schneider, J.; Kuss, P.; Abraham, R.; Meske, C. Governance of generative artificial intelligence for companies. *arXiv* **2024**, arXiv:2403.08802.
275. Mökander, J.; Schuett, J.; Kirk, H.R.; Floridi, L. Auditing large language models: A three-layered approach. *AI Ethics* **2024**, *4*, 1085–1115. [CrossRef]
276. Cai, H.; Wu, S. TKG: Telecom Knowledge Governance Framework for LLM Application. *Res. Sq.* **2023**. [CrossRef]
277. Asthana, S.; Zhang, B.; Mahindru, R.; DeLuca, C.; Gentile, A.L.; Gopisetty, S. Deploying Privacy Guardrails for LLMs: A Comparative Analysis of Real-World Applications. *arXiv* **2025**, arXiv:2501.12456.
278. Mamalis, M.; Kalampokis, E.; Fitsilis, F.; Theodorakopoulosand, G.; Tarabanis, K. A Large Language Model Based Legal Assistant for Governance Applications. ResearchGate. 2024. Available online: https://www.researchgate.net/publication/383360660_A_Large_Language_Model_Agent_Based_Legal_Assistant_for_Governance_Applications (accessed on 23 May 2025).
279. Zhao, L. Artificial Intelligence and Law: Emerging Divergent National Regulatory Approaches in a Changing Landscape of Fast-Evolving AI Technologies. In *Law 17 Oct 2023*; Edward Elgar Publishing: Bingley, UK, 2023; pp. 369–399. [CrossRef]
280. Imam, N.M.; Ibrahim, A.; Tiwari, M. Explainable Artificial Intelligence (XAI) Techniques To Enhance Transparency In Deep Learning Models. *IOSR J. Comput. Eng. (IOSR-JCE)* **2024**, *26*, 29–36. [CrossRef]
281. Butt, A.; Junejo, A.Z.; Ghulamani, S.; Mahdi, G.; Shah, A.; Khan, D. Deploying Blockchains to Simplify AI Algorithm Auditing. In Proceedings of the 2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bahrain, Bahrain, 25–27 October 2023; pp. 1–6. [CrossRef]
282. Yang, F.; Abedin, M.Z.; Qiao, Y.; Ye, L. Toward Trustworthy Governance of AI-Generated Content (AIGC): A Blockchain-Driven Regulatory Framework for Secure Digital Ecosystems. *IEEE Trans. Eng. Manag.* **2024**, *71*, 14945–14962. [CrossRef]
283. Zhao, Y. Audit Data Traceability and Verification System Based on Blockchain Technology and Deep Learning. In Proceedings of the 2024 International Conference on Telecommunications and Power Electronics (TELEPE), Frankfurt, Germany, 29–31 May 2024; pp. 77–82. [CrossRef]
284. Chaffer, T.J.; von Goins II, C.; Cotlage, D.; Okusanya, B.; Goldston, J. Decentralized Governance of Autonomous AI Agents. *arXiv* **2024**, arXiv:2412.17114.
285. Nweke, O.C.; Nweke, G.I. Legal and Ethical Conundrums in the AI Era: A Multidisciplinary Analysis. *Int. Law Res. Arch.* **2024**, *13*, 1–10. [CrossRef]
286. Van Rooy, D. Human–machine collaboration for enhanced decision-making in governance. *Data Policy* **2024**, *6*, e60. [CrossRef]
287. Abeliuk, A.; Gaete, V.; Bro, N. Fairness in LLM-Generated Surveys. *arXiv* **2025**, arXiv:2501.15351.
288. Alipour, S.; Sen, I.; Samory, M.; Mitra, T. Robustness and Confounders in the Demographic Alignment of LLMs with Human Perceptions of Offensiveness. *arXiv* **2024**, arXiv:2411.08977.

289. Agarwal, S.; Muku, S.; Anand, S.; Arora, C. Does Data Repair Lead to Fair Models? Curating Contextually Fair Data To Reduce Model Bias. In Proceedings of the 2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 3–8 January 2022; pp. 3898–3907. [CrossRef]
290. Simpson, S.; Nukpezah, J.; Brooks, K.; Pandya, R. Parity benchmark for measuring bias in LLMs. *AI Ethics* **2024**. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.