Review Not peer-reviewed version

The Importance of AI Data Governance in Large Language Models

Saurabh Pahune , Zahid Akhtar * , Venkatesh Mandapati , Kamran Siddique

Posted Date: 2 April 2025

doi: 10.20944/preprints202504.0219.v1

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

 doi:10.20944/preprints202504.0219.v1

Article

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
[2] Department of Electrical and Computer Engineering, State University of New York Polytechnic Institute, Utica, NY 13502, USA
[3] FedEx, Memphis, TN 38017, USA
[4] Department of Computer Science and Engineering, University of Alaska Anchorage, AK 99508, USA
* Correspondence: akhtarz@sunypoly.edu; Tel.: +1-315-792-7238

Abstract: AI data governance is a crucial framework for ensuring that data is utilized in the life cycle of large language models (LLMs) activity from the development process, end-to-end testing process, model validation, secure deployment, and operations. This requires being managed responsibly, confidentially, securely, and ethically. The main objective of data governance is to implement the robust and intelligent data governance framework for LLMs which tends to impact on data quality management, fine-tuning of model performance, biases, data privacy laws, security protocols, ethical AI practices, and regulatory compliance process 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 is needed 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

1. Introduction

As a current trend, the use of large language models like GPT-3 and GPT-4 in software development cycles is 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 that are advancing trends in the medical domain [4], and enhance the examination of medical records by managing massive amounts of medical data [5,6] (eg: unstructured clinical notes, diverse data types of medical image, hospital guide, telehealth and electronic health records (EHR)). The LLM integration approach (GPT-4, BERT) into the medical system that handles a large amount of healthcare data 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], Med42-v2 [12].

Meanwhile, the evolution of LLMs across many industries is gaining in importance, such as in the financial sector, there are various financial-based LLMs present to handle the complexities of

 doi:10.20944/preprints202504.0219.v1

financial tasks. BloombergGPT [13], FinBERT [14], FinGPT [15], which needs a large amount of data and benchmarks to train this model with a powerful infrastructure. There are studies that highlight LLM-based financial sentimental analysis (FSA), built on LLaMA2 [16], A synthesized LLM multiagent system [17], the multi-document financial question and answer [18], which improves the improvement in complex financial tasks. The study demonstrates that LLMs focus on the travel mode choice task (TourLLM [19], Tourism Recommender Systems (TRS) using LLM's based RAG pipeline [20]), designed to improve travel choice modeling, enhance general public transport services, forecast task 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], e-Commerce [30,31], fairness of techniques, policy guidelines, and data security are the must-have priorities that are required as part of data governance technologies in LLMs.

1.1. How Data Is Crucial to Build LLMs Performance?

Data are the fundamental and crucial step in training the millions, billions of parameters of the LLM model to evaluate performance. In a recent study by Yin et al. [32] conclude that selecting the right data for training LLMs (redundancy, contradiction, prioritize data subsets with low compression ratio) plays a vital role in improving model performance. The paper emphasizes, by Kumar et al. [33] the importance of high quality data preparations (deduplications on crawl data) and effective tokenization optimization startergies plays an important step for 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 LLM. In this article Jiao et al. [36] enhance the open source PandaLLM with the use of an instruction-tunning approach based on training data factors (quantity, quality and linguistic distribution) that affect model training. The article proposed [37] the importance of synthetic data generation that fills the gaps after LLM post-training, which tends to contribute to the better performance of LLM. Wood et al. [38] introduce the Data Prep Kit (DPK) toolkit, built for the data preparation for LLM that enhances the performance of fine-tuning models using RAG.

In order to build and improve the performance of LLMs, data is 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 (eg., cultural biases), 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 LLM are "Hallucination" while performing the output response based on input query.
- The other vital issue is "Data misuse" that 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 bias approach in LLM.
- Lack of data governance framework leads to "Data breach and lack of data security (security concern)" activity which increase a risk of various adversarial attacks (backdoor attacks, data-poisoning attacks, model inversion attacks, transfer based black-box attacks etc.).
- Also, it impacts an "Ethical implications and legal concerns" in LLM due to lack of data governance framework.

 doi:10.20944/preprints202504.0219.v1

- Failure of LLM, while deploying in production pipeline, requires strong LLMOps pipeline with the assistance of a solid data governance approach.

To avoid data misuse, bias nature, hallucination, deployment issues, lack of data security, ethical challenges, and misinformation. This 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 emerging of LLM in this digital era of a 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 LLM has potential challenges in terms of data misuse, biases, and ethical challenges. Addressing critical issues and understanding the various factors and implementation of robust data governance frameworks are crucial steps. Hence given below are the impacted behavior of LLM that needs to be enhanced and provides a more potential solution for foundation of 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 LLM	[39–41]
Data privacy and security concerns	[42–44]
Hallucination in LLM	[45–48]
Ethical implications and misinformation	[49–51]
Failure deployment of LLMs	[52–55]
Regulatory compliance and legal concerns	[56–59]
Unintended destructive outputs	[60–62]
Lack of data validation and data quality control	[63–66]
Data evolution and drift creates a lack of performance	[67–70]

1.3. Problem Statement

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

The absence of data governance in healthcare care 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, legal liabilities, and without structured policies, it is a large risk of data misuse [42,43]. This paper has discussed hallucination detection in LLM, this problem tends to occur due to the absence of data governance which leads to lack of data quality control during LLM training and evaluation [45]. The lack of the data governance framework in LLM, which causes an issue with unintended destructive output generation of LLM called data dysphoria (due to poor data quality and validity) [60], without defining clear policies and defined roles it can result in mismanagement of data assets (such as data integrity, data quality, data security) [63]. The 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 [71], and organization struggle to meet the regulation like General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), which are requirements for data privacy in Information Technology (IT) audits [56]. The scalable and flexible governance model adapts the regulation like GDPR, CCPA. It is a best practice to adapt the framework to protect safe data and resources in a cloud environment [72]. The author discussed data contamination occurring in LLM that affects the overestimation of model performance and the

 doi:10.20944/preprints202504.0219.v1

importance of the data governance framework that encourages the detection of this problem using audit tools (to detect and address data contamination) [73]. This article [74] presented a detailed review of key challenges in LLM such as misleading information, duplication of content, and personal information through the web-mined copra. It requires a proper methodology (e.g., data cleaning, bias detection) to mitigate the issues in LLM. The paper [75] focuses on the urgent need to provide a solid dynamic auditing system, which requires transparency in the implementation of the LLM model. As its a crucial step for distinct ethical challenges (privacy and fairness, hallucination, verifiable accountability, decoding censorship complexity in LLM). The cited article [76] focuses on securing LLMs are most vital steps to avoid prompt attacks (e.g. jailbreak attacks, adversarial attacks as a prompt injection), focus on accuracy, bias issue. As its growing impressively across various fields, a defense mechanism and safe guarding is 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 elements of AI data governance for LLMs. It encompasses the management of data of quality control and data privacy, regulatory and compliance, mitigation of biases, risk for successful deployment of LLMs, ethical challenges, security and privacy concerns.

The list of various key aspects that leverage AI-driven data governance that involves LLMs are mentioned below. Uses in various sectors like healthcare, finance, e-Commerce, travel sectors are given below, which are essential to use this methodology.

- The paper proposed the use of an AI data governance framework in the context of LLMs to improve the detection of suspicious transactions (money laundering, anomaly detection in financial transactions) [77].
- The use of AI-driven intelligent data framework that substantially improves operational efficiency, compliance accuracy, and data integrity for the future development of AI-based work [78].
- The author provides a criticality to the use of centering implementation of AI data governance in LLMs, which is more effective for model performance [79].
- The 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) [80].
- The use of AI data governance frameworks automates the process of managing data quality in the banking sector to improve model performance [81].
- The use of data-centric governance throughout the model learning life cycle, responsible for the deployment of AI system which reduces the risk of deployment failure, reduces the deployment process, and increases the solution design approach [82].
- The integration of AI driven data governance framework with banking system, that enhance data is accurate, reliable and securable, which creates trust accountability in financial sector [83].
- As AI is evolving very rapidly in daily life and lots of manual tasks reduces due to automation capabilities. Therefore, there is trust in the AI system 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 [84].

 doi:10.20944/preprints202504.0219.v1

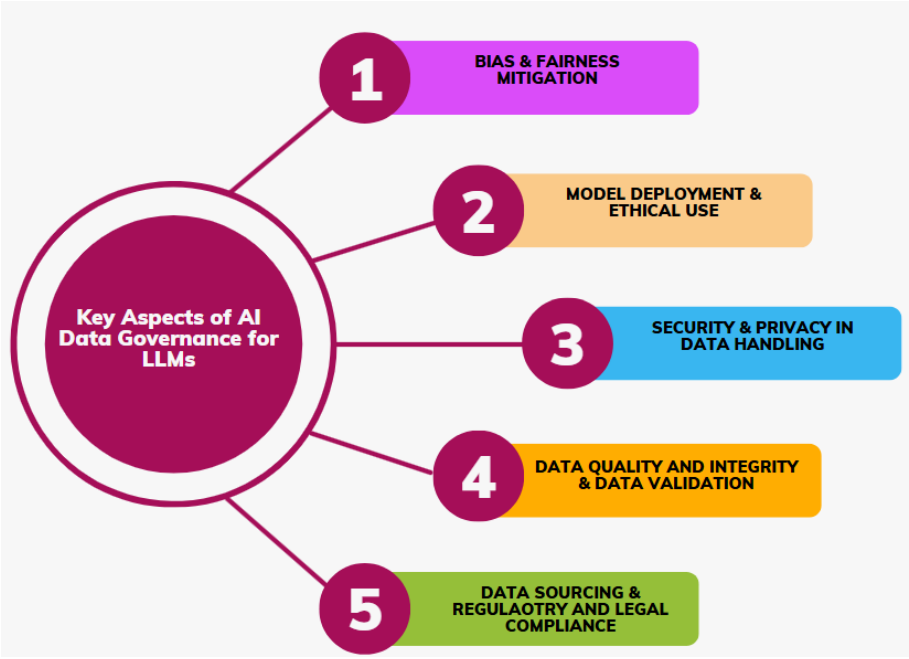

Figure 1. Key Aspects of AI Data Governance for LLMs.

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 in many aspects such as security and privacy data handling process, bias and fairness mitigation, regulator and legal compliance, and safe guarding ethical approach. The scope of AI data governance are 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 uses across the AI model through out 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, AIRMF.
Ethical and Fair AI Practices	The implementation of AI data governance ensures that AI models and systems operates with transparency, fairness without any discrimination 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, encrypted mechanism to mitigate data breach activity. Also, prevents with various cyber threats and several attacks (eg., 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, assist with debugging the issue for root cause analysis.
More Secure End-to-End Model Deployment	The use of this data governance approach assist with secure and confidence deployment of AI model via various pipelines (DevOps, MLOps, LLMOps) from initial phase, robust model training, testing and validation, deployment phase, post deployment phase.

 doi:10.20944/preprints202504.0219.v1

The remainder of this article is structured as follows. Section 2 presents the foundations of AI data governance. In Section 3, 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, regulatory and ethical considerations are discussed. Section 6 outlines best practices for AI data governance methodology. Section 7 describes case studies on the implementation of data governance in LLMs. However, Section 8 presents open issues and future directions, emerging technologies, and interdisciplinary research to address AI governance. The conclusions are described in Section 9.

2. Foundations of AI Data Governance

Foundations of AI data governance frameworks are most crucial steps in the digital era of AI during the building of a model. This step is a core of the process to ensure responsible development and management of the AI model lifecycle. The focus of model building using with the data centric governance approach develops the dynamic capabilities to adapt technology advancement with a more secure and flexible way. In addition, it makes an AI system ethically and effectively for legal compliance and regulatory processes. Nowadays, building a LLM based applications to gain trustworthiness, secure of data, ethical and fair answers, various attacks preventions are needed.

There are various frameworks of AI data governance categorize 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 2 mentioned in the following, related to various types of AI data governance categorization. Whereas, Table 3 outlines the detailed key aspects of various types of AI data governance.

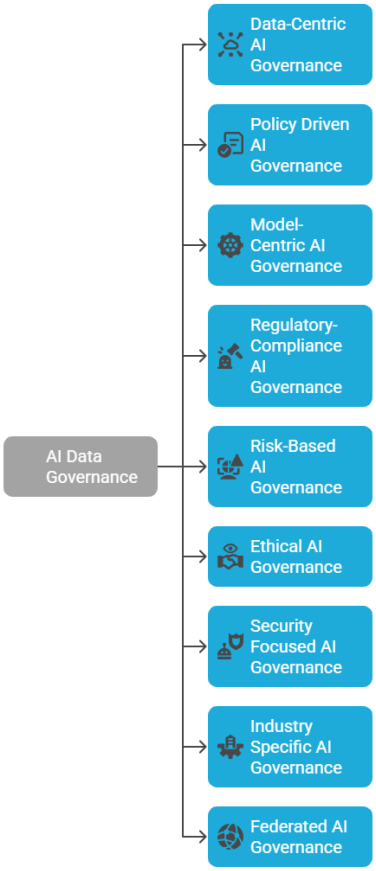

Figure 2. Types of AI Data Governance Frameworks.

 doi:10.20944/preprints202504.0219.v1

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.	[85,86]
Data-Centric Governance	Data Quality and Integrity: Ensure data fairness, accuracy and bias mitigation approach	Master Data Management, Data Encryption, Third-Party Data Sharing Policies.	[79,82,87]
Model-Centric Governance	Model Explainability: Focus on models lifecycle from initial phase to secure deployment phase.	Model Lifecycle Management (MLOps, LLMOps), Model Performance and Accuracy.	[87–89]
Risk-Based Governance	AI Risk Management: Identifies potential AI risk (e.g., algorithmic bias, data privacy breaches, security vulnerabilities) and applies data governance controls.	Financial and Operational Risk, Security and Cyber Risk Management, Algorithmic Risk Management.	[90,91]
Federated AI Governance	Decentralized AI Systems: AI model training with securing confidential data (e.g, Train AI model without sharing confidential patient data).	Decentralized Model Governance and Accountability, Security and Trust in Federated Systems, Decentralized Model Governance and Accountability.	[92,93]
Regulatory-Compliance Governance	Adherence to Laws: Ensure models not breaking rights, privacy and laws	Healthcare AI to comply must with HIPAA regulations.	[94,95]
Ethical AI Governance	Fairness and Bias Prevention: Identifies the biased, unfairness and other discrimination metrics.	Transparency and Explainability, Ethical Guidelines and Frameworks (e.g., OECD AI Principles), Safety and Robustness.	[96,97]
Security-Focused Governance	AI Cybersecurity and attacks: To prevent models with various attacks (e.g.,model inversion, prompt injection)	Model Security and Integrity, Cybersecurity Act (e.g., NIST, ENISA), Secure AI Model Development and Post Deployment Security.	[98–101]
Industry-Specific Governance	Domain-based AI rules: Ensure compliance are align with domain specific regulation (e.g., Pharma, Healthcare domain)	AI-driven drug discovery follows FDA, Healthcare AI must go with HIPAA, Finance with GDPR regulation.	[102–104]

2.1. Core Principles of AI Data Governance Relevance to LLMs

As LLMs are widely used in various domains (e.g. healthcare and pharmaceutical [105–107] by analyzing and training a large number of clinical data sets, genomic analysis of biological data, reshaping molecular biology and drug development. ShennongGPT [108] trained in distilled drug database and allowed patients to respond as human-like decision to personalize drug advice and adverse drug reactions. The overall, LLM's in healthcare sector to avoid biases, inaccuracies in generated output, data security, and privacy concerns (e.g., patient data privacy), the robustness of AI data governance are needed to understand the capabilities and limitations of the models in healthcare applications.

Whereas in finance [109–111] LLM's are re-shaping the financial market analysis, risk assessment, investment decision making based on vast amount of financial data (e.g., FinLLM [112], KemenkeuGPT [113], BloombergGPT [13], FinGPT [15]). In addition to cybersecurity [114–117] it is providing cyber thereat intelligence (CTI) analysis, ability to detect automate threat detection, mitigate approach on random threats, vulnerability assessments. However, future research is needed for safeguarding data, social ethics, robust encryption, enhance authentication methods and legal norms

 doi:10.20944/preprints202504.0219.v1

to defend LLM's against adversarial attacks, token manipulation [118,119]. 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 integration of data governance that significant impacts to transform the business operations (e.g., Inventory management, supply chain optimization, to avoid supply chain risk, early detection vulnerabilities in software supply chains, automate contract renewal, etc.) [120–122]. In personalizing recommendations and enhancing the ability to work on large scale, multi dimensional dataset (e.g. e-commerce chatbots [123–125] for personalize recommendation based on users historical data, conversational recommender system (CRS) [126]), education is transforming as new digital era via intelligent tutoring system by us of LLMs [127–129], and several areas that effectively shape industry operations. Hence, the role of AI data governance is the crucial step in ensuring the AI model that is used to train LLMs with billions/millions of parameters responsible for creating the various content generation outputs such as text to multimedia content generation [130,131] that encompasses the various outputs (image-to-video, video-to-image, audio-to-image or cross model content generation). To obtain refined LLM outputs, where it needs fairness, reliability, transparency, compliance, trustworthiness, unbias, safety, prevention of adversarial threats and aligned 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

As shown in Figure 3 , provides an overview of various core principles of AI data governance, and various components details are mentioned below.

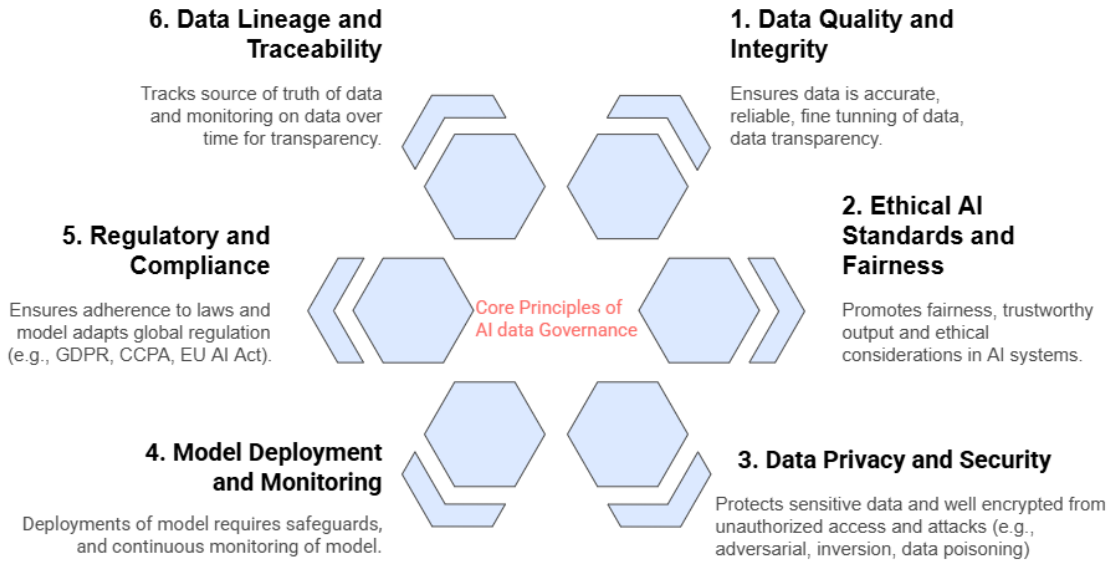

Figure 3. Core principles of AI data governance.

2.2.1. Data Quality and Integrity

Data Quality is critical for reliable LLM performance. For training corpora, Yao et al. [132] proposed methods that can mitigate the undesired data properties during the generation, cleaning, and training data to improve the data quality for LLM. 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

 doi:10.20944/preprints202504.0219.v1

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 the trust in the LLM outputs. The paper by Nazi and Peng [133] 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

The 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 risks associated, including ethical standards and intellectual property [134]. LLMs can be biased based on their training data which raise 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 don't set ethical standards. Using alignment techniques, Liu et al. [135] mentioned that LLMs can be more reliable, safe, fair, and attuned to human values that will foster greater trust among its users. Notable general guidelines "HHH" principal advocates alignment that is Helpful, Honest, and Harmless.

2.2.3. Data Privacy and Security

If the LLMs are trained in 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 its source. Carlini et al. [136] shared how LLM models 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. [137] 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 the 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 [52,138,139]. Multidimensional evaluation techniques must be used to measure technical performance, data privacy, input stability, and calibration and output alignment, and find out about possible restrictions and how to meet legal requirements and compliance [140].

The 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 [141]. The study focuses on a complete model monitoring framework that uses Grafana (analyze data from various sources across various domains [142]) and Dynatrace (a real-time software intelligence platform that detects model drifts, data quality issues [143]) 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 [144].

 doi:10.20944/preprints202504.0219.v1

2.2.5. Regulatory and Compliance

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 of data access [145,146]. Data governance is a key part of making sure that the 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 GDPR (General Data Protection Regulation) and California Consumer Privacy Act (CCPA) regulations imposed to meet the requirements on ML models. Users must agree to the use of their personal data, have the right to have it deleted, and be aware of how LLMs use their data to follow the rules (MemoAnalyzer in LLMs that enables the user to delete, modify sensitive information leading to increased user awareness [147]). Data privacy rules are being pushed to their limits by the speed with which LLM models are being built. Information about people who can be identified (PII) is used to train the LLM model (the adaptive PII framework can be used for LLM to mitigate the risk of personal identifiable information to meet with compliance [148]). 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 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.

The lack of data lineage, the lack of knowledge of exactly the sources of the training data, and the scenarios that could make it difficult to address any problems. One method is to apply IDs or hashes to the data samples for the data set training for data traceability (HashGraph [149]). Adoption of new data version and control systems would be helpful in tracking the state of the data set and documenting changes [150]. Mirchandani et al. [151] 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 the training data, and lineage also supports attribution, which can give credit to its contributors. Chen et al. [152], mentioned keeping track of the data is an essential for data flow vision, hence the use of data lineage graphs (DLGs) make 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 4 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:

 doi:10.20944/preprints202504.0219.v1

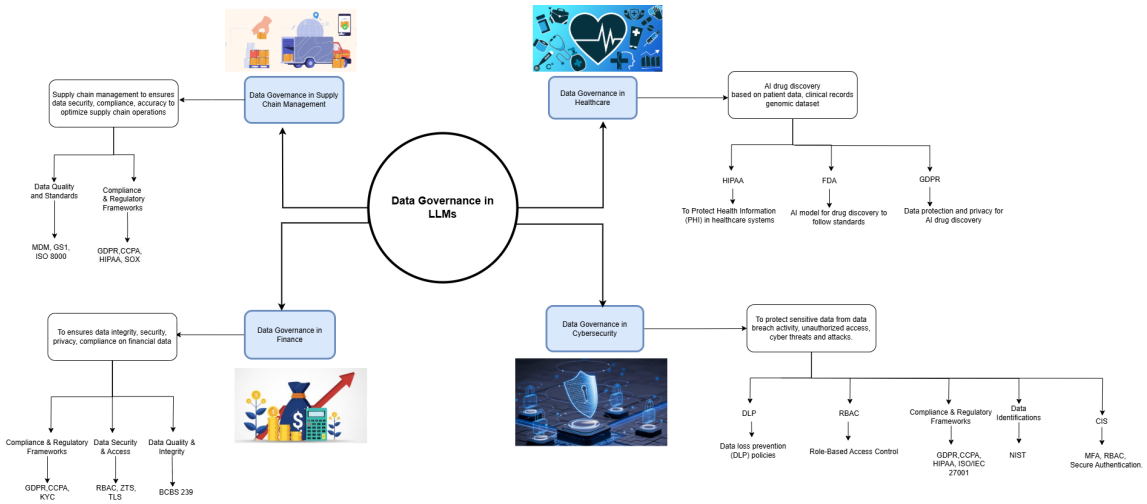

Figure 4. Data governance in various domains.

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 the adherence to data privacy laws and the preservation of quality and safety standards [153]. The 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 [154]. The 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 [155]. 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 [156].

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. The 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 [157]. 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 [158]. The study analyzes the imperative for an AI governance framework in healthcare care 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 [159]. The study stresses the importance of comprehensive data governance frameworks in AI-driven healthcare care, emphasizing obstacles such as privacy issues and regulatory limitations. Promotes more transparency, public knowledge, and adaptable regulatory frameworks to cultivate trust and ethical AI implementation [80]. The

 doi:10.20944/preprints202504.0219.v1

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 [160]. The 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 [161]. 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 safety, legality, and protection of fundamental rights in the use of health data [162].

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. The 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 [163]. The work highlights the importance of resilient governance frameworks in AI-enhanced cybersecurity, guaranteeing adherence to data protection regulations such as GDPR and CCPA. It emphasizes the necessity for algorithmic transparency and ethical data use to cultivate consumer trust and mitigate hazards [164]. 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 [165]. The 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 response to improve data security and cybersecurity strategies across various sectors [166]. 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 [167]. The article emphasizes the imperative of aligning data governance regulations with AI standards respecting 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 [168]. 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 [169].

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. The 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 [170]. The 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

 doi:10.20944/preprints202504.0219.v1

breaches and regulatory non-compliance, fostering a culture of compliance and employing innovative technology for improved capabilities [171]. 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 [172].

4. Challenges in Data Governance for LLMs

Figure 5, 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 trains on millions/billions of parameters, hence it needs a high computational load with the powerful infrastructure requirements of GPUs/TPUs (high-performance computing clusters are needed for 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.

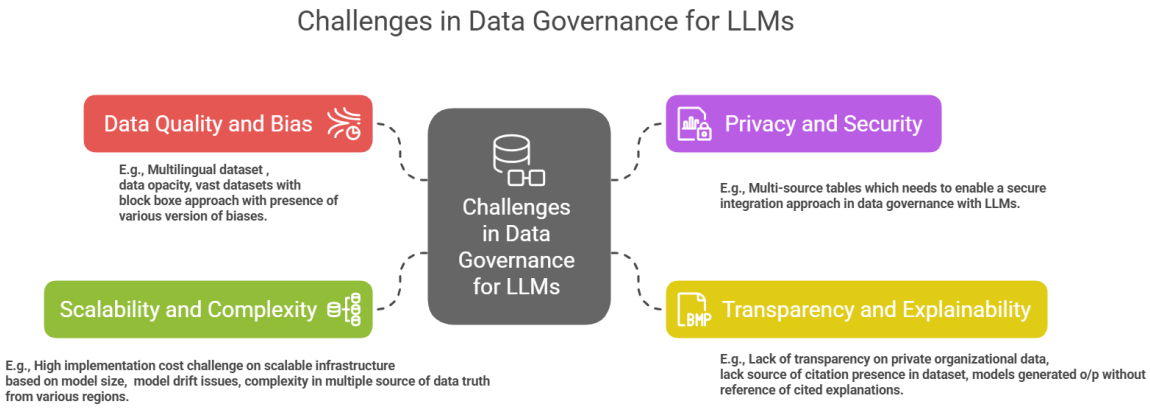

Figure 5. Challenges in Data Governance for LLMs.

Zhou et al. [173] 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 LLM consisting of hallucination, high operational cost, and low performance in complex tasks. As LLMs train on vast amounts of dataset from multiple public, open source data (web, articles, etc.), and private domain (e.g., billions of tokens from various sources), it is difficult to track the data sourcing and ownership issue. Hence, it has an impact on crates legal actions on copyright data and challenges related to ethical concerns over data ownership issues to suit with 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 act, data quality, ownership issues, and transparency to act sensible are the biggest challenge 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 diversity of data sources and bias present in the data set, is a significant challenge in data governance for LLMs. The quality of the data used to train LLM has inherent biases from the dataset that can lead to misinformation about the results and ethical concerns. The study reveals [174] 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, content moderation) within the data governance framework. Using a data governance approach to analyze and optimize LLM training dataset curation that leads to biased and low quality content output from models that impacts performance [175]. The context of non-English datasets that have less information

 doi:10.20944/preprints202504.0219.v1

of source (e.g., Chinese, Korean context) creates hurdles for data governance to ensure data scarcity, accuracy, unclear idea on the fairness of the data and trusted sources issues that lead to impacts model performance as well [176]. LLM trained on multilingual datasets are considered "black boxes", which means difficult-to-understand datasets and expected output of the models [177].

4.2. Privacy and Security

LLMs trains on vast amount of data (e.g., millions, billions parameter) in various domains and data is crucial part to tune 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 have been mentioned below.

- As LLM has the ability to train on large datasets and can create by mistakes memorize the data and regenerate the information from the personal sensory data such as patient details, medical records, leakage of financial information and others (e.g., data-poisoning attacks) [178].
- 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 the various malicious attacks (e.g., privacy breaches in model training and prediction phase, membership inference attacks, model inference attacks) [179].
- The strict guidelines and regulations of (RBAC) to prevent access role of these models based on users profile, if the untrained person gets the access to write, retrieve data that will create an issue of a data exposure risk [180,181].
- Due to a rapid increase in data volumes, implementation is a big challenge for LLM in data governance framework, as data come from multi-source tables which needs to enable a secure integration approach. [182].

4.3. Transparency and Explainability

The LLM integration with a data governance framework consists of significant challenges related to transparency and explainability, as it is difficult to trust models, 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 truth of the data, which comes from several tables (e.g., dark data, data opacity, data gap, algorithmic bias).

- Most LLM are trained in private organizational enterprise data; hence most of these data are dark data, not accessible to the public. This is vague to gain trust in the source of data and model output that creates challenges in transparency, regulation and trust [183].
- Financial chatbots trained on historical financial market data analysis (e.g. stock prices, forex, etc.), various corporate reports (e.g., balance sheets, income statements, etc.) with the lack of a source of citation raising large concerns about data transparency [184–186].
- Healthcare chabots for patient recommendation trained on public healthcare datasets, research papers and medical literature (PubMed, WHO guidelines), EHR's. However, this chatbot model cannot provide insight into the output result reference that makes a model decision opaque [187].
- LLMs like GPT-4, BERT and others remain the black box of the system (e.g., trained on billions or millions of parameter, model generates output without citing source details) which tends to create a very big challenge to implement the data governance framework approach, as example, the EU AI act and US AI bill of rights need transparency and explainability behind each decision [188–190].

4.4. Scalability and Complexity

LLMs integration with data governance frameworks approach are big concerns to keep a track on enterprise data ecosystem. As this large model replies on vast, diverse domain and unstructured data

 doi:10.20944/preprints202504.0219.v1

(e.g., image, video, audio), it makes it difficult to manage and governing these diverse scalable and complex data pattern.

- 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 that makes it harder to implement a data governance approach at the enterprise level [191].
- The LLMs are continuously learning and logging memory data and evolving efficiently with a learn-and-evolve approach. As models are consistently growing as a model drift which creates a challenge to implement data governance framework [192,193].
- 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 data governance methodology [194,195].

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 LLM is developed, trained, and tested securely. Ensures several key components, such as privacy, security, and ethical use of data to gain the trust of the user. Figure 6, presented 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.

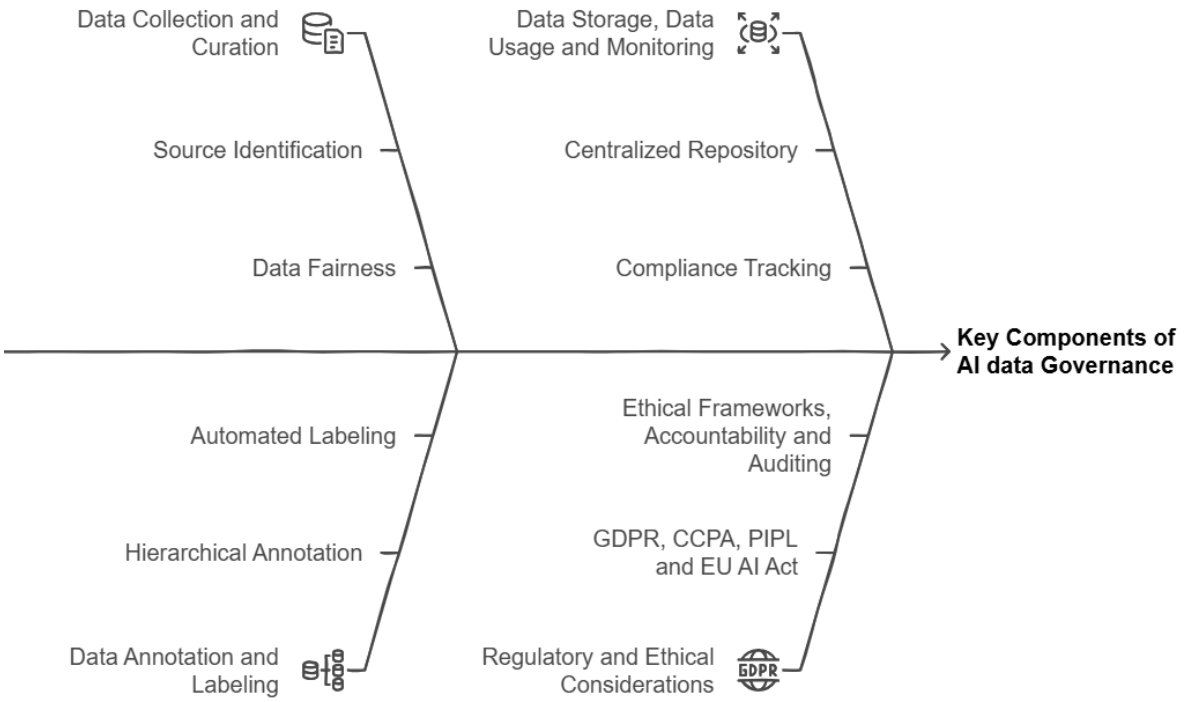

Figure 6. Key Components of AI data Governance.

5.1. Data Collection and Curation

- Source Identification: Effective governance to ensure that data used for training, the data source that is used for fine tuning that comes with high quality [196], diversity is crucial to selecting data samples to enhance model training [197], data must have ethical sources that comply with data protection laws (e.g. GDPR, HIPAA, CCPA, and others) [198], human curated data indicates high quality of the data [199,200], and data fairness are important steps as part of core components of data governance for LLM, however role of data cataloging ensures the data lineage tracking and use of metadata management approach [201].

 doi:10.20944/preprints202504.0219.v1

5.2. Data Annotation and Labeling

- LLM in enterprise data can benefit from using hierarchical annotation of structure data, where instead of using a single label, it is classified at multiple levels based on label granularity. Instead of using a single label, a tree structure benefits LLM to improve scalability and better performance output [183,202]. Hence, leveraging hierarchical annotation allows for the identification of complex relationships and patterns within the dataset.
- AI data governance for LLMs in which 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 [203]. 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 [204,205].

5.3. Data Storage and Management

- Data storage is a crucial step to the impact of AI data governance to maintain 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 data set [206] to minimize the risk of data leakage and helps to maintain data security using the central data approach.
- This work emphasizes the impact of the data governance framework on a secure data leak mitigation approach via the centralization of the data repository for vast data sets, transforming enterprise data management through the unified data governance methodology [207].
- This paper proposed a qualified compliance to align ISO/IEC 5259 standards with 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 [208].
- 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 [209]. Using advanced machine learning technologies can enhance data governance capabilities with multisource data integration patterns by using reference tools for data quality check, data profiling, data cleaning, and continuous monitoring [210].

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. An effective data governance impacts the data filtering and data monitoring approach to work closely from training, testing, to the secure AI deployment pipeline of large models [154].
- Recommendation of the data governance mechanism based on the detection of unauthorized data and 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 [43,211].
- 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 [212].
- Data protection regulation policies such as GDPR and CCPA reshape data usage that enhance customer trust. Due to the importance of regulation-aware dateset (e.g., C3A) is managed effectively to comply with relevant regulation, policies standards, and ethical guidelines [213,214].

 doi:10.20944/preprints202504.0219.v1

5.5. Regulatory and Ethical Considerations

5.5.1. 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.

- General Data Protection Regulation (GDPR): GDPR sets a high standard for data protection law 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 brach notifications, data storage to ensure transparency and accountability.
  The key components of GDPR are data protection rights, breach notification, lawful processing, extraterritorial reach, data subject rights (e.g, Right to Access, Right to Rectifications) [215,216]. By integrating GDPR and EU AI Act within the global regulatory landscape that enhances compliance strategies, strengthen data protection and trustworthy AI system [217].
- 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 [218,219]. 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 how different ways of handling privacy problems in the digital world today [220]. This law was subsequently revised and expanded by the California Privacy Rights Act (CPRA), which introduced enhanced consumer protections and enforcement mechanisms [221].
- China's Personal Information Protection Law (PIPL): PIPL is a comprehensive framework and a significant step in China for data protection, data classification and user rights within digital platforms [222]. The main components of 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, classification of data, and remedies for data violations, and is based on the principle of proportionality to improve data security and privacy rights [223]. 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 [224].

5.5.2. 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, researcher, developer, organization and business) with the principle of responsible AI development (e.g., transparency, fairness, 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., CCPA, GDPR, EU AI Act, and others) to implement sustainable development [225]. The use of stakeholder participation is critical by participating in brainstorming sessions, consultations to clarify ethical responsibilities, and addressing ethical conflicts [226]. 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 [227]. 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 [228].
- 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 safeguard

 doi:10.20944/preprints202504.0219.v1

of model deployment, prevents biasing in the model, and the discrimination 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 [229]. 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 [230,231].

5.5.3. 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 [232]. 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 [233]. The study indicates that internal audits conduct periodic self-assessments to ensure adherence to data protection regulations in the implementation of GDPR to ensure compliance with data protection measures [234,235]. In order to improve the quality of national statistics and data curation, the 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 (an international standard for information security management systems), SOC 2, and NIST to ensure accountability and a rigorous auditing process [236,237].

6. Best Practices for AI Data Governance in LLMs

AI data governance plays an important role in LLM, providing strong guidelines and regulatory authority for data management via end-to-end lifecycle management in LLM to ensure compliance, regulatory, secure, auditing methodology, and ethical approach. The best practices of effective data governance to implement 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 assist organizations in minimizing risk, providing trustworthiness in AI application from user side, maintaining data integrity, secure data against adversarial attacks, and continuously monitoring data pipelines for anomalies. As shown in Figure 7, an overview of best practices for AI data governance at the high level and the key components are outlined below.

 doi:10.20944/preprints202504.0219.v1

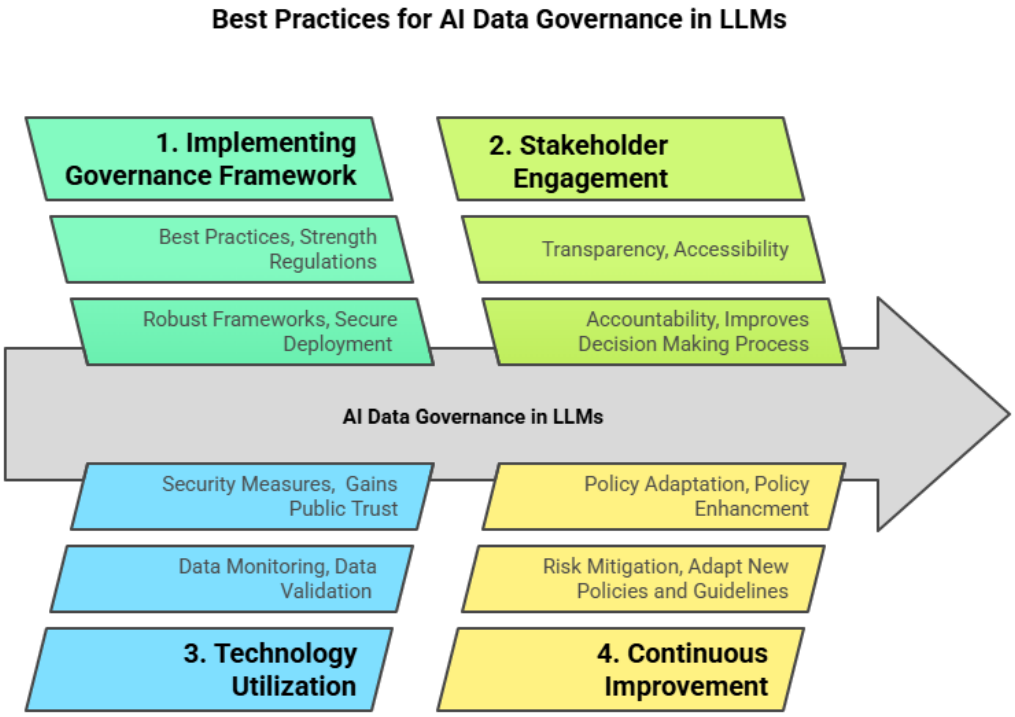

Figure 7. Best Practices for AI Data Governance in LLMs.

6.1. Developing a Governance Framework

A well structured governance framework defined a crucial role in protecting sensitive information in the data quality management-based approach [238] that enhances decision-making and facilitates the compliance approach. By implementing the integration of the data governance framework that strengthens the compliance and regulations that build trust between the user and AI applications [239, 240]. In every step of LLM lifecycle management, data ownership, transparency, accountability, and secure deployment are the keys to the success of LLM, defined as a clear role using a data governance [241,242].

6.2. Stakeholder Engagement

Stakeholder involvement, which includes early input from all participants (e.g., AI engineers, compliance officers, data scientists, 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 [243,244]. The paper demonstrates the importance of ongoing stakeholder engagement, particular 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, assist in brainstorming on various concerns to be addressed and improve the decision-making process [245,246].

6.3. Leveraging Technology

As LLMs on large scale utilize and perform complex operations, in that case, the use of technology within the data governance methodology plays a critical role. The use of advanced technologies such as AI-driven tools for an automation approach to audit and monitor the regulation approach with respect to maintaining data integrity. An AI-driven data analysis that enhances the identification of trends and patterns and assists in policy making criteria, policy evaluation, improved transparency,

 doi:10.20944/preprints202504.0219.v1

and public trust in governance [247]. 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 closely, and facilitates compliance and regulatory standards. Overall use of AI-driven technology improves an operation process and supports large-scale data-driven governance.

6.4. Continuous Improvement

As LLMs use fine-tuning mechanisms (allows LLMs to take advantage of both labeled and unlabeled data [248]) to adapt a specific task and evolve performance and applicability. As AI data governance has an iterative approach to assist with the iteration and feedback-based mechanism and requires a continuous monitoring and refinement approach to LLM 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 that help mitigate the risk associated with data bias, model inaccuracies, and security breaches [249]. Hence, a continuous improvement approach in a data governance framework plays a critical role in aligning with current processes and future process updates.

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 [250]. 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 [251]. Microsoft Azure implements the new opportunities for modern AI data governance to integrate LLM with transparency, accountability, security, and a focus on fairness in AI decision-making abilities [252,253].

The proposed framework in the financial industry via (e.g., IBM watsonx.governance ([254]) with the implementation of AI governance in LLM 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, high-level design and methodology to manage organization in the blueprinting phase, end-to-end model development guidelines with the use of guidance and regulation throughout the LLM life cycle from design, development, testing and validation, deployment, monitoring, and enhancement of models are crucial in the advancement of ethical and responsible AI. The author proposed Nickerson's framework [255] development process that captured the scope of building a model (data, model, system, people targets and scope, organizational scope and targets), outline, and governance mechanism (structural, procedural, relational), model targets (e.g., RAG), antecedents, consequences (risk management, performance effects) and mitigation risk while integrating with 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 [256]. The author of intelligent data governance has proposed a modern framework [257] built on modular microservice architecture deployed on scalable cloud infrastructure. This method with the use of this architecture and design pattern (e.g., modular microservices, scalable cloud infrastructure) provides organizations with the ability to rapidly adapt to evolving data governance requirements, providing unparalleled scalability, integration, and flexibility. The research proposed [258] blueprinting for auditing LLMs using a three-layered approach such as governance audit, model audit, and application audit, the adoption of this AI governance model in LLM collectively addresses ethical, legal, and technical challenges, as shown in Figure 8.

 doi:10.20944/preprints202504.0219.v1

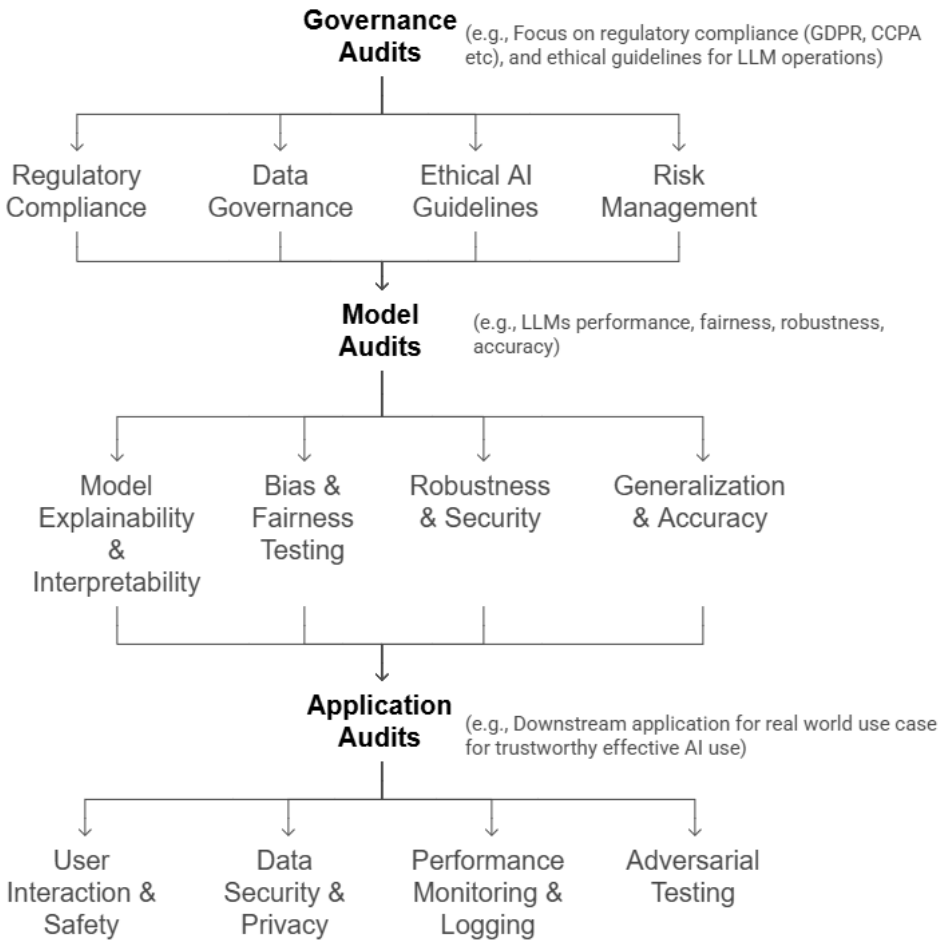

Figure 8. Auditing Data Governance Framework for LLMs: A three-layered approach [258].

The 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 [259]. 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 [209]. The paper presents case studies on highlighting the significant challenges in LLMs related to privacy and security concerns, hence it needs to implement GDPR, CCPA data protection laws. In this work, the author has proposed a framework referred to as 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 [260]. 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 (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 [261].

 doi:10.20944/preprints202504.0219.v1

8. Open Challenges and Future Research Opportunities

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

8.1. Scalability of Data Governance Framework

As LLM models scale up and 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 data set 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 a clear and refined data governance compliance and regulation.

8.2. Security Risks and Data Breaches

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

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), CCPA (California), and 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 have developed multilingual compliance frameworks and automated translation tools as prospective actions to overcome the challenge in data governance framework.

8.4. Data Provenance and Traceability

It is challenging to determine the source of truth of the data, which is derived from multiple tables (e.g. dark data, data opacity, data gap, algorithmic bias), as LLMs are trained on large data sources and the data is 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 co-ordination to address regulatory gaps, and there is a potential to change AI regulation to mitigate the risk of fostering innovation [262]. 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 an explainable artificial intelligence to promote ethical use of AI [263]. 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 9, blockchain technology with the use of new integration approach (conceptual framework) with data governance framework which will help, offering a transparent track of all transactions and

 doi:10.20944/preprints202504.0219.v1

data interactions, essential for monitoring AI algorithms, the use of integrity and transparency of data, auditable trail of transactions, hybrid governance approach and ensuring adherence to ethical standards [264,265].

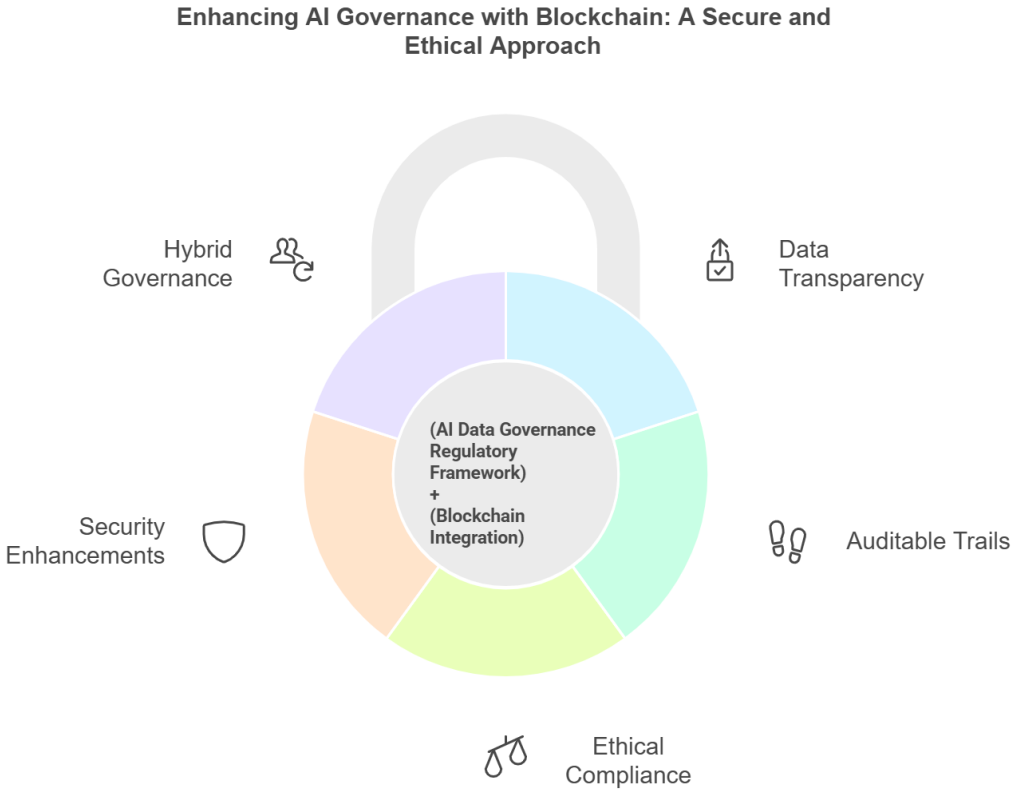

Figure 9. Enhancing Data Governance with AI and Blockchain Integration.

The blockchain-driven regulatory framework is an essential part in 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 security of audit problem clues [266,267]. 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 [268] decentralized governance innovation framework which offers scalable and prompting trust), while addressing the significant gaps between the evolving AI technologies in LLM and the existing legal framework (e.g., combining legal principles, ethical considerations, technological advancements, and sociological insights to create comprehensive frameworks for AI governance) [269].

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 of 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 system. This human 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

 doi:10.20944/preprints202504.0219.v1

systems can be mitigated and enhance the quality of decisions and increase public trust [195,270]. 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 automated generated output with human judgment and refines the escalation, mitigates the risk of misinformation, and upholds ethical standards.

8.6. Data Quality and Bias Mitigation

LLMs frequently develop biases from their training data, which can result in ethical and impartiality concerns. The study demonstrates that LLMs exhibit performance disparities as a consequence of US-centric training data, revealing biases influenced by sociodemographic factors [271,272]. 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 pre-processing techniques and utilizing post-processing corrections are vital steps in curating diverse datasets and bias mitigation approach [65,199,273,274].

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 model. 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).

9. Conclusions

LLMs are growing rapidly to foster the trustworthiness of AI models from the user side; It is essential to integrate LLM with a robust data governance framework for ethical data management, model performance, biases, privacy laws, regulatory compliance, robust impact on data privacy, and avoid security breaches and hallucinations in AI models. This paper has 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 LLM. This paper 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 refine and adapt 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.

Author Contributions: Conceptualization, S.P. and Z.A.; methodology, S.P.; 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, Z.A. and K.S.; visualization, S.P. and 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 not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

 doi:10.20944/preprints202504.0219.v1

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 Sentimental 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's
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
EHR: 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

 doi:10.20944/preprints202504.0219.v1

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

References

1. Haque, M.A. LLMs: A Game-Changer for Software Engineers? *arXiv preprint arXiv:2411.00932* **2024**.
2. Meduri, S. Revolutionizing Customer Service: The Impact of Large Language Models on Chatbot Performance. *International Journal of Scientific Research in Computer Science Engineering and Information Technology* **2024**, *10*, 721–730. https://doi.org/10.32628/CSEIT241051057.
3. Pahune, S.; Chandrasekharan, M. Several categories of large language models (llms): A short survey. *arXiv preprint arXiv:2307.10188* **2023**.
4. Vavekanand, R.; Karttunen, P.; Xu, Y.; Milani, S.; Li, H. Large Language Models in Healthcare Decision Support: A Review **2024**.
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) **2024**.
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. *Medicine Plus* **2024**, p. 100030.
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. *Journal of Medical Internet Research* **2025**, *27*, e59069.
8. Acosta, J.N.; Falcone, G.J.; Rajpurkar, P.; Topol, E.J. Multimodal biomedical AI. *Nature Medicine* **2022**, *28*, 1773–1784.
9. Huang, K.; Altosaar, J.; Ranganath, R. Clinicalbert: Modeling clinical notes and predicting hospital readmission. *arXiv preprint arXiv:1904.05342* **2019**.
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.
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, 2023, Vol. 2022, p. 962.
12. Christophe, C.; Kanithi, P.K.; Raha, T.; Khan, S.; Pimentel, M.A. Med42-v2: A suite of clinical llms. *arXiv preprint arXiv:2408.06142* **2024**.
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 preprint arXiv:2303.17564* **2023**.
14. Araci, D. FinBERT: Financial Sentiment Analysis with Pre-trained Language Models. *arXiv preprint arXiv:1908.10063* **2019**.
15. Yang, H.; Liu, X.Y.; Wang, C.D. Fingpt: Open-source financial large language models. *arXiv preprint arXiv:2306.06031* **2023**.
16. Zhao, Z.; Welsch, R.E. Aligning LLMs with Human Instructions and Stock Market Feedback in Financial Sentiment Analysis. *arXiv preprint arXiv:2410.14926* **2024**.
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 preprint arXiv:2407.06567* **2024**.
18. Shah, S.; Ryali, S.; Venkatesh, R. Multi-Document Financial Question Answering using LLMs. *arXiv preprint arXiv:2411.07264* **2024**.
19. Wei, Q.; Yang, M.; Wang, J.; Mao, W.; Xu, J.; Ning, H. Tourllm: Enhancing llms with tourism knowledge. *arXiv preprint arXiv:2407.12791* **2024**.

 doi:10.20944/preprints202504.0219.v1

20. Banerjee, A.; Satish, A.; Wörndl, W. Enhancing Tourism Recommender Systems for Sustainable City Trips Using Retrieval-Augmented Generation. *arXiv preprint arXiv:2409.18003* **2024**.
21. Wang, J.; Shalaby, A. Leveraging Large Language Models for Enhancing Public Transit Services. *arXiv preprint arXiv:2410.14147* **2024**.
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 preprint arXiv:2405.02357* **2024**.
23. Zhai, X.; Tian, H.; Li, L.; Zhao, T. Enhancing Travel Choice Modeling with Large Language Models: A Prompt-Learning Approach. *arXiv preprint arXiv:2406.13558* **2024**.
24. Mo, B.; Xu, H.; Zhuang, D.; Ma, R.; Guo, X.; Zhao, J. Large language models for travel behavior prediction. *arXiv preprint arXiv:2312.00819* **2023**.
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 preprint arXiv:2406.11903* **2024**.
26. Papasotiriou, K.; Sood, S.; Reynolds, S.; Balch, T. AI in Investment Analysis: LLMs for Equity Stock Ratings. In Proceedings of the Proceedings of the 5th ACM International Conference on AI in Finance, 2024, pp. 419–427.
27. Fatemi, S.; Hu, Y.; Mousavi, M. A Comparative Analysis of Instruction Fine-Tuning LLMs for Financial Text Classification. *arXiv preprint arXiv:2411.02476* **2024**.
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). IEEE, 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. *Journal of medical systems* **2023**, *47*, 33.
30. Palen-Michel, C.; Wang, R.; Zhang, Y.; Yu, D.; Xu, C.; Wu, Z. Investigating LLM Applications in E-Commerce. *arXiv preprint arXiv:2408.12779* **2024**.
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 Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval, 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 preprint arXiv:2407.06645* **2024**.
33. Kumar, R.; Kakde, S.; Rajput, D.; Ibrahim, D.; Nahata, R.; Sowjanya, P.; Kumar, D. Pretraining Data and Tokenizer for Indic LLM. *arXiv preprint arXiv:2407.12481* **2024**.
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 e-prints* **2024**, pp. arXiv–2409.
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 preprint arXiv:2405.13954* **2024**.
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 preprint arXiv:2305.03025* **2023**.
37. Gan, Z.; Liu, Y. Towards a Theoretical Understanding of Synthetic Data in LLM Post-Training: A Reverse-Bottleneck Perspective. *arXiv preprint arXiv:2410.01720* **2024**.
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 preprint arXiv:2409.18164* **2024**.
39. Liu, Z. Cultural Bias in Large Language Models: A Comprehensive Analysis and Mitigation Strategies. *Journal of Transcultural Communication* **2024**.
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), 2024, pp. 1–6. https://doi.org/10.1109/CONECCT62155.2024.10677324.
41. Talboy, A.N.; Fuller, E. Challenging the appearance of machine intelligence: Cognitive bias in LLMs and Best Practices for Adoption. *arXiv preprint arXiv:2304.01358* **2023**.
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. Springer, 2024, pp. 261–271.

 doi:10.20944/preprints202504.0219.v1

43. Gavgani, V.Z.; Pourrasmi, A. Data Governance Navigation for Advanced Operations in Healthcare Excellence. *Depiction of Health* **2024**, *15*, 249–254.
44. Raza, M.A. Cyber Security and Data Privacy in the Era of E-Governance. *Social Science Journal for Advanced Research* **2024**, *4*, 5–9.
45. Du, X.; Xiao, C.; Li, Y. Haloscope: Harnessing unlabeled llm generations for hallucination detection. *arXiv preprint arXiv:2409.17504* **2024**.
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 preprint arXiv:2410.19485* **2024**.
47. Liu, X. A Survey of Hallucination Problems Based on Large Language Models. *Applied and Computational Engineering* **2024**, *97*, 24–30.
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), April 2024, pp. 1–6. https://doi.org/10.1109/eStream61684.2024.10542617.
49. Zhui, L.; Fenghe, L.; Xuehu, W.; Qining, F.; Wei, R. Ethical considerations and fundamental principles of large language models in medical education. *Journal of Medical Internet Research* **2024**, *26*, e60083.
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**, pp. 1–1. https://doi.org/10.1109/ACCESS.2024.3406644.
51. Ma, T. LLM Echo Chamber: personalized and automated disinformation. *arXiv preprint arXiv:2409.16241* **2024**.
52. Pahune, S.; Akhtar, Z. Transitioning from MLOps to LLMOps: Navigating the Unique Challenges of Large Language Models. *Information* **2025**, *16*, 87. https://doi.org/10.3390/info16020087.
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 preprint arXiv:2411.09916* **2024**.
54. Menshawy, A.; Nawaz, Z.; Fahmy, M. Navigating Challenges and Technical Debt in Large Language Models Deployment. In Proceedings of the Proceedings of the 4th Workshop on Machine Learning and Systems, New York, NY, USA, 2024; EuroMLSys '24, p. 192–199. https://doi.org/10.1145/3642970.3655840.
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), 2024, pp. 364–367. https://doi.org/10.1109/AINIT61980.2024.10581784.
56. 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. *International Journal of Research in Engineering and Science* **2023**, *11*.
57. 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 preprint arXiv:2411.04576* **2024**.
58. Hassani, S. Enhancing legal compliance and regulation analysis with large language models. In Proceedings of the 2024 IEEE 32nd International Requirements Engineering Conference (RE). IEEE, 2024, pp. 507–511.
59. 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), 2023, pp. 4626–4635. https://doi.org/10.1109/BigData59044.2023.10386518.
60. Aaronson, S.A. Data Dysphoria: The Governance Challenge Posed by Large Learning Models. *Available at SSRN 4554580* **2023**.
61. Cheong, I.; Caliskan, A.; Kohno, T. Envisioning legal mitigations for LLM-based intentional and unintentional harms. *Adm. Law J* **2022**.
62. Glukhov, D.; Han, Z.; Shumailov, I.; Papyan, V.; Papernot, N. Breach By A Thousand Leaks: Unsafe Information Leakage inSafe'AI Responses. *arXiv preprint arXiv:2407.02551* **2024**.
63. Madhavan, D. Enterprise Data Governance: A Comprehensive Framework for Ensuring Data Integrity, Security, and Compliance in Modern Organizations. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* **2024**. https://doi.org/10.32628/cseit241051062.
64. Rejeleene, R.; Xu, X.; Talburt, J. Towards trustable language models: Investigating information quality of large language models. *arXiv preprint arXiv:2401.13086* **2024**.

 doi:10.20944/preprints202504.0219.v1

65. 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). IEEE, 2024, pp. 6387–6393.
66. Balloccu, S.; Schmidtová, P.; Lango, M.; Dušek, O. Leak, cheat, repeat: Data contamination and evaluation malpractices in closed-source LLMs. *arXiv preprint arXiv:2402.03927* **2024**.
67. Abdelnabi, S.; Fay, A.; Cherubin, G.; Salem, A.; Fritz, M.; Paverd, A. Are you still on track!? Catching LLM Task Drift with Activations. *arXiv preprint arXiv:2406.00799* **2024**.
68. Würsch, M.; David, D.P.; Mermoud, A. Monitoring Emerging Trends in LLM Research. *Large* **2024**, p. 153.
69. Mannapur, S.B. Machine Learning Drift Detection and Concept Drift Analysis: Real-time Monitoring and Adaptive Model Maintenance. *CSEIT* **2024**. https://doi.org/https://doi.org/10.32628/CSEIT25111239.
70. 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*. https://doi.org/10.1145/3655630.
71. Sharma, V.; Mousavi, E.; Gajjar, D.; Madathil, K.; Smith, C.; Matos, N. Regulatory framework around data governance and external benchmarking. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction* **2022**, *14*, 04522006.
72. Vardia, A.S.; Chaudhary, A.; Agarwal, S.; Sagar, A.K.; Shrivastava, G. Cloud Security Essentials: A Detailed Exploration. *Emerging Threats and Countermeasures in Cybersecurity* **2025**, pp. 413–432.
73. 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 preprint arXiv:2310.18018* **2023**.
74. Perełkiewicz, M.; Poświata, R. A Review of the Challenges with Massive Web-mined Corpora Used in Large Language Models Pre-Training. *arXiv preprint arXiv:2407.07630* **2024**.
75. Jiao, J.; Afroogh, S.; Xu, Y.; Phillips, C. Navigating llm ethics: Advancements, challenges, and future directions. *arXiv preprint arXiv:2406.18841* **2024**.
76. 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 preprint arXiv:2409.08087* **2024**.
77. 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). IEEE, 2023, pp. 291–295.
78. Kumari, B. Intelligent Data Governance Frameworks: A Technical Overview. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* **2024**. https://doi.org/10.32628/cseit24106161.
79. 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 preprint arXiv:2409.17216* **2024**.
80. 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 Journal of Research in Computer Science* **2024**, *17*, 85–107.
81. 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). IEEE, 2024, pp. 1–6.
82. McGregor, S.; Hostetler, J. Data-centric governance. *arXiv preprint arXiv:2302.07872* **2023**.
83. Khan, I. Ai-powered data governance: ensuring integrity in banking's technological frontier **2023**.
84. Tjondronegoro, D.W. Strategic AI Governance: Insights from Leading Nations. *arXiv preprint arXiv:2410.01819* **2024**.
85. Schiff, D.; Biddle, J.; Borenstein, J.; Laas, K. What's next for ai ethics, policy, and governance? a global overview. In Proceedings of the Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 2020, pp. 153–158.
86. Arnold, G.; Ludwick, S.; Mohsen Fatemi, S.; Krause, R.; Long, L.A.N. Policy entrepreneurship for transformative governance. *European Policy Analysis* **2024**.
87. Jakubik, J.; Vössing, M.; Kühl, N.; Walk, J.; Satzger, G. Data-centric artificial intelligence. *Business & Information Systems Engineering* **2024**, pp. 1–9.
88. Majeed, A.; Hwang, S.O. Technical analysis of data-centric and model-centric artificial intelligence. *IT Professional* **2024**, *25*, 62–70.
89. Gisolfi, N. Model-centric verification of artificial intelligence. PhD thesis, Carnegie Mellon University, 2022.
90. Currie, N. Risk based approaches to artificial intelligence. *Crowe Data Management* **2019**.
91. Lütge, C.; Hohma, E.; Boch, A.; Poszler, F.; Corrigan, C. On a Risk-Based Assessment Approach to AI Ethics Governance **2022**.

 doi:10.20944/preprints202504.0219.v1

92. 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. *Frontiers in Research Metrics and Analytics* **2023**, *8*, 1035123.
93. Pencina, M.J.; McCall, J.; Economou-Zavlanos, N.J. A federated registration system for artificial intelligence in health. *JAMA* **2024**, *332*, 789–790.
94. Lim, H.Y.F. Regulatory compliance. In *Artificial Intelligence*; Edward Elgar Publishing, 2022; pp. 85–108.
95. Aziza, O.R.; Uzougbo, N.S.; Ugwu, M.C. The impact of artificial intelligence on regulatory compliance in the oil and gas industry. *World Journal of Advanced Research and Reviews* **2023**, *19*, 1559–1570.
96. Eitel-Porter, R. Beyond the promise: implementing ethical AI. *AI and Ethics* **2021**, *1*, 73–80.
97. Daly, A.; Hagendorff, T.; Hui, L.; Mann, M.; Marda, V.; Wagner, B.; Wang, W.; Witteborn, S. Artificial intelligence governance and ethics: global perspectives. *arXiv preprint arXiv:1907.03848* **2019**.
98. Sidhpurwala, H.; Mollett, G.; Fox, E.; Bestavros, M.; Chen, H. Building Trust: Foundations of Security, Safety and Transparency in AI. *arXiv preprint arXiv:2411.12275* **2024**.
99. 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). IEEE, 2024, pp. 305–312.
100. 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, 2024; pp. 143–161.
101. Savaş, S.; Karataş, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review* **2022**, *3*, 7–34.
102. 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. *Library of Progress-Library Science, Information Technology & Computer* **2024**, *44*.
103. Mirakhori, F.; Niazi, S.K. Harnessing the AI/ML in Drug and Biological Products Discovery and Development: The Regulatory Perspective. *Pharmaceuticals* **2025**, *18*, 47.
104. Price, W.; Nicholson, I. Distributed governance of medical AI. *SMU Sci. & Tech. L. Rev.* **2022**, *25*, 3.
105. Han, Y.; Tao, J. Revolutionizing Pharma: Unveiling the AI and LLM Trends in the Pharmaceutical Industry. *arXiv preprint arXiv:2401.10273* **2024**.
106. Tripathi, S.; Gabriel, K.; Tripathi, P.K.; Kim, E. Large language models reshaping molecular biology and drug development. *Chemical Biology & Drug Design* **2024**, *103*, e14568.
107. Liu, J.; Liu, S.; et al. Applications of Large Language Models in Clinical Practice: Path, Challenges, and Future Perspectives **2024**.
108. 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). IEEE, 2023, pp. 67–72.
109. 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 preprint arXiv:2401.11641* **2024**.
110. Li, Y.; Wang, S.; Ding, H.; Chen, H. Large language models in finance: A survey. In Proceedings of the Proceedings of the fourth ACM international conference on AI in finance, 2023, pp. 374–382.
111. 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. *Journal of Portfolio Management* **2024**, *51*.
112. 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 preprint arXiv:2401.10744* **2024**.
113. Febrian, G.F.; Figueredo, G. KemenkeuGPT: Leveraging a Large Language Model on Indonesia's Government Financial Data and Regulations to Enhance Decision Making. *arXiv preprint arXiv:2407.21459* **2024**.
114. 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 preprint arXiv:2408.03354* **2024**.
115. Shafee, S.; Bessani, A.; Ferreira, P.M. Evaluation of llm chatbots for osint-based cyber threat awareness. *arXiv preprint arXiv:2401.15127* **2024**.
116. Wang, F. Using large language models to mitigate ransomware threats **2023**.
117. Zangana, H.M. Harnessing the Power of Large Language Models. *Application of Large Language Models (LLMs) for Software Vulnerability Detection* **2024**, p. 1.
118. Yang, J.; Chi, Q.; Xu, W.; Yu, H. Research on adversarial attack and defense of large language models. *Applied and Computational Engineering* **2024**, *93*, 105–113.

 doi:10.20944/preprints202504.0219.v1

119. Abdali, S.; Anarfi, R.; Barberan, C.; He, J. Securing Large Language Models: Threats, Vulnerabilities and Responsible Practices. *arXiv preprint arXiv:2403.12503* **2024**.
120. 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). IEEE, 2024, pp. 634–641.
121. 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. *Journal of Global Information Management (JGIM)* **2024**, *32*, 1–29.
122. Wang, S.; Zhao, Y.; Hou, X.; Wang, H. Large language model supply chain: A research agenda. *ACM Transactions on Software Engineering and Methodology* **2024**.
123. 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). IEEE, 2024, pp. 1–6.
124. 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 preprint arXiv:2408.03533* **2024**.
125. Mohanty, I. Recommendation Systems in the Era of LLMs. In Proceedings of the Proceedings of the 15th Annual Meeting of the Forum for Information Retrieval Evaluation, 2023, pp. 142–144.
126. Li, C.; Deng, Y.; Hu, H.; Kan, M.Y.; Li, H. Incorporating External Knowledge and Goal Guidance for LLM-based Conversational Recommender Systems. *arXiv preprint arXiv:2405.01868* **2024**.
127. Alhafni, B.; Vajjala, S.; Bannò, S.; Maurya, K.K.; Kochmar, E. Llms in education: Novel perspectives, challenges, and opportunities. *arXiv preprint arXiv:2409.11917* **2024**.
128. Leinonen, J.; MacNeil, S.; Denny, P.; Hellas, A. Using Large Language Models for Teaching Computing. In Proceedings of the Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 2, 2024, pp. 1901–1901.
129. 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). IEEE, 2023, pp. 1–6.
130. 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). IEEE, 2024, pp. 1610–1615.
131. 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 Transactions on Circuits and Systems for Video Technology* **2024**, *34*, 6809–6813.
132. 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-Confidence Computing* **2024**, p. 100211.
133. Nazi, Z.A.; Peng, W. Large language models in healthcare and medical domain: A review. In Proceedings of the Informatics. MDPI, 2024, Vol. 11, p. 57.
134. Huang, J.; Chang, K.C.C. Citation: A key to building responsible and accountable large language models. *arXiv preprint arXiv:2307.02185* **2023**.
135. 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 preprint arXiv:2308.05374* **2023**.
136. Carlini, N.; Tramèr, F.; Wallace, E.; Jagielski, M.; Herbert-Voss, A.; Lee, K.; Roberts, A.; Brown, T.; Song, D.; Úlfar Erlingsson.; et al. Extracting Training Data from Large Language Models. In Proceedings of the 30th USENIX Security Symposium, 2021, pp. 2633–2650.
137. 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). IEEE, 2020, pp. 1314–1331.
138. 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. Springer, 2024, pp. 112–131.
139. 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), 2023, pp. 1–7. https://doi.org/10.1109/SITA60746.2023.10373733.

 doi:10.20944/preprints202504.0219.v1

140. 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, 2022; chapter 7. https://doi.org/10.1002/9781119824961.ch7.
141. Nogare, D.; Silveira, I.F. EXPERIMENTATION, DEPLOYMENT AND MONITORING MACHINE LEARNING MODELS: APPROACHES FOR APPLYING MLOPS. *Revistaft* **2024**, *28*, 55. https://doi.org/10.5281/zenodo.11557655.
142. 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), 2023, pp. 1–8. https://doi.org/10.1109/ICCCNT56998.2023.10306699.
143. Samudrala, L.N.R. Automated SLA Monitoring in AWS Cloud Environments - A Comprehensive Approach Using Dynatrace. *Journal of Artificial Intelligence & Cloud Computing* **2024**.
144. Menon, V.; Jesudas, J.; S.B, G. MODEL MONITORING WITH GRAFANA AND DYNATRACE: A COMPREHENSIVE FRAMEWORK FOR ENSURING ML MODEL PERFORMANCE. *International Journal of Advanced Research* **2024**, pp. 54–63.
145. Yadav, S. Balancing Profitability and Risk: The Role of Risk Appetite in Mitigating Credit Risk Impact. *International Scientific Journal of Economics and Management* **2024**.
146. Anil, V.K.S.; Babatope, A. Global Journal of Engineering and Technology Advances. *Global Journal of Engineering and Technology Advances* **2024**, *21*, 190–202. Received on 20 November 2024; revised on 29 December 2024; accepted on 31 December 2024, https://doi.org/10.30574/gjeta.2024.21.3.0246.
147. 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 preprint arXiv:2410.14931* **2024**.
148. Asthana, S.; Mahindru, R.; Zhang, B.; Sanz, J. Adaptive PII Mitigation Framework for Large Language Models. *arXiv preprint arXiv:2501.12465* **2025**.
149. 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), 2023, pp. 775–780. https://doi.org/10.1109/RusAutoCon58002.2023.10272905.
150. 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 PrePrints* **2017**, *5*, e3401v1.
151. 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 preprint arXiv:2307.04721* **2023**.
152. Chen, Y.; Zhao, Y.; Li, X.; Zhang, J.; Long, J.; Zhou, F. An open dataset of data lineage graphs for data governance research. *Visual Informatics* **2024**, *8*, 1–5.
153. Kramer, S.G. Artificial Intelligence in the Supply Chain: Legal Issues and Compliance Challenges. *Journal of Supply Chain Management, Logistics and Procurement* **2024**, *7*. https://doi.org/10.69554/AWRA2732.
154. Hausenloy, J.; McClements, D.; Thakur, M. Towards Data Governance of Frontier AI Models. *arXiv preprint arXiv:2412.03824* **2024**.
155. 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). IEEE, 2024, pp. 557–562.
156. 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, 2025; pp. 257–282. https://doi.org/10.4018/979-8-3693-6760-5.ch011.
157. 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**, pp. 2024–12.
158. 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, 2025; pp. 283–310. https://doi.org/10.4018/979-8-3693-9641-4.ch010.
159. Hassan, M.; Borycki, E.M.; Kushniruk, A.W. Artificial intelligence governance framework for healthcare. *Healthcare Management Forum* **2024**, *38*, 125–130. https://doi.org/10.1177/08404704241291226.

 doi:10.20944/preprints202504.0219.v1

160. Chakraborty, A.; Karhade, M. Global AI Governance in Healthcare: A Cross-Jurisdictional Regulatory Analysis. *arXiv preprint arXiv:2406.08695* **2024**.
161. Kim, J.; Kim, S.Y.; Kim, E.A.; et al. Developing a Framework for Self-regulatory Governance in Healthcare AI Research: Insights from South Korea. *Asia-Pacific Biotech Research (ABR)* **2024**, *16*, 391–406. https://doi.org/10.1007/s41649-024-00281-w.
162. 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 to Just. E. Eur.* **2024**, p. 120.
163. 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. *Available at SSRN 5044032* **2024**.
164. Mbah, G.O.; Evelyn, A.N. AI-powered cybersecurity: Strategic approaches to mitigate risk and safeguard data privacy. *World Journal of Advanced Research and Reviews* **2024**, *24*, 310–327. https://doi.org/10.30574/wjarr.2024.24.3.3695.
165. Folorunso, A.; Adewumi, T.; Adewa, A.; Okonkwo, R.; Olawumi, T.N. Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances* **2024**, *21*, 167–184. Received on 11 September 2024; revised on 24 October 2024; accepted on 26 October 2024, https://doi.org/10.30574/gjeta.2024.21.1.0193.
166. 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), 2024, pp. 76–81. https://doi.org/10.1109/IJCC64742.2024.10847294.
167. 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. *International Journal of Research in Information Security and Systems (IJRISS)* **2024**, *8090245*. Received: 28 September 2024; Accepted: 01 October 2024; Published: 19 October 2024, https://doi.org/https://dx.doi.org/10.47772/IJRISS.2024.8090245.
168. 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. https://doi.org/10.1017/dap.2024.26.
169. 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, 2022, pp. 693–697. https://doi.org/10.1109/ICECA55336.2022.10009139.
170. Boggarapu, N.B. Modernizing Banking Compliance: An Analysis of AI-Powered Data Governance in a Hybrid Cloud Environment. *CSEIT* **2024**, *10*, 2434. https://doi.org/https://doi.org/10.32628/CSEIT2410612434.
171. 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 Transactions on ICT Research* **2024**, *5*, 1631. https://doi.org/https://doi.org/10.51594/csitrj.v5i10.1631.
172. Chukwurah, N.; Ige, A.B.; Adebayo, V.I.; Eyieyien, O.G. Frameworks for Effective Data Governance: Best Practices, Challenges, and Implementation Strategies Across Industries. *Computer Science & IT Research Journal* **2024**, *5*, 1666–1679. https://doi.org/https://doi.org/10.51594/csitrj.v5i7.1351.
173. Zhou, X.; Zhao, X.; Li, G. LLM-Enhanced Data Management. *arXiv preprint arXiv:2402.02643* **2024**.
174. Gorti, A.; Chadha, A.; Gaur, M. Unboxing Occupational Bias: Debiasing LLMs with US Labor Data. In Proceedings of the Proceedings of the AAAI Symposium Series, 2024, Vol. 4, pp. 48–55.
175. de Dampierre, C.; Mogoutov, A.; Baumard, N. Towards Transparency: Exploring LLM Trainings Datasets through Visual Topic Modeling and Semantic Frame. *arXiv preprint arXiv:2406.06574* **2024**.
176. Yang, J.; Wang, Z.; Lin, Y.; Zhao, Z. Global Data Constraints: Ethical and Effectiveness Challenges in Large Language Model. *arXiv preprint arXiv:2406.11214* **2024**.
177. Li, C.; Zhuang, Y.; Qiang, R.; Sun, H.; Dai, H.; Zhang, C.; Dai, B. Matryoshka: Learning to Drive Black-Box LLMs with LLMs. *arXiv preprint arXiv:2410.20749* **2024**.
178. 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. *Nature Medicine* **2025**, pp. 1–9.
179. Wu, F.; Cui, L.; Yao, S.; Yu, S. Inference Attacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions. *arXiv e-prints* **2024**, pp. arXiv–2406.
180. Subramaniam, P.; Krishnan, S. Intent-Based Access Control: Using LLMs to Intelligently Manage Access Control. *arXiv preprint arXiv:2402.07332* **2024**.

 doi:10.20944/preprints202504.0219.v1

181. Mehra, T. The Critical Role of Role-Based Access Control (RBAC) in securing backup, recovery, and storage systems. *International Journal of Science and Research Archive* **2024**, *13*, 1192–1194.
182. 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). IEEE, 2024, pp. 3965–3974.
183. Kayali, M.; Wenz, F.; Tatbul, N.; Demiralp, Ç. Mind the Data Gap: Bridging LLMs to Enterprise Data Integration. *arXiv preprint arXiv:2412.20331* **2024**.
184. Erdem, O.; Hassett, K.; Egriboyun, F. Evaluating the Accuracy of Chatbots in Financial Literature. *arXiv preprint arXiv:2411.07031* **2024**.
185. 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), 2024, pp. 1–5. https://doi.org/10.1109/ASIANCON62057.2024.10838194.
186. Zheng, Z. ChatGPT-style Artificial Intelligence for Financial Applications and Risk Response. *International Journal of Computer Science and Information Technology* **2024**, *3*, 179–186. https://doi.org/https://doi.org/10.62051/ijcsit.v3n2.20.
187. Kushwaha, P.K.; Kumar, R.; Kumar, S. AI Health Chatbot using ML. *International Journal of Scientific Research in Engineering and Management (IJSREM)* **2024**, *8*, 1. Guide: Prof. Badal Bhushan, Assistant Professor, Department of CSE, IIMT College of Engineering, Greater Noida, India, https://doi.org/10.55041/IJSREM33761.
188. Hassani, S. Enhancing Legal Compliance and Regulation Analysis with Large Language Models. In Proceedings of the 2024 IEEE 32nd International Requirements Engineering Conference (RE), June 2024, pp. 507–511. https://doi.org/10.1109/RE59067.2024.00065.
189. Kumar, B.; Roussinov, D. NLP-based Regulatory Compliance–Using GPT 4.0 to Decode Regulatory Documents. *arXiv preprint arXiv:2412.20602* **2024**.
190. 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 preprint arXiv:2402.16142* **2024**.
191. Zhu, H. Architectural Foundations for the Large Language Model Infrastructures. *arXiv preprint arXiv:2408.09205* **2024**.
192. Koppichetti, R.K. Framework of Hub and Spoke Data Governance Model for Cloud Computing. *Journal of Artificial Intelligence & Cloud Computing* **2024**.
193. Li, D.; Sun, Z.; Hu, X.; Hu, B.; Zhang, M. CMT: A Memory Compression Method for Continual Knowledge Learning of Large Language Models. *arXiv preprint arXiv:2412.07393* **2024**.
194. Folorunso, A.; Babalola, O.; Nwatu, C.E.; Ukonne, U. Compliance and Governance issues in Cloud Computing and AI: USA and Africa. *Global Journal of Engineering and Technology Advances* **2024**, *21*, 127–138. Received on 07 October 2024; revised on 19 November 2024; accepted on 21 November 2024, https://doi.org/10.30574/gjeta.2024.21.2.0213.
195. 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. *Frontiers in Neuroinformatics* **2024**, *18*, 1472653.
196. Li, Y.; Yu, X.; Koudas, N. Data Acquisition for Improving Model Confidence. *Proceedings of the ACM on Management of Data* **2024**, *2*, 1–25.
197. 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 preprint arXiv:2409.16986* **2024**.
198. 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, 2024; pp. 195–213.
199. 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 preprint arXiv:2410.10877* **2024**.
200. 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 **2023**.
201. Oktavia, T.; Wijaya, E. Strategic Metadata Implementation: A Catalyst for Enhanced BI Systems and Organizational Effectiveness. *HighTech and Innovation Journal* **2025**, *6*, 21–41.
202. Tan, Z.; Li, D.; Wang, S.; Beigi, A.; Jiang, B.; Bhattacharjee, A.; Karami, M.; Li, J.; Cheng, L.; Liu, H. Large language models for data annotation and synthesis: A survey. *arXiv preprint arXiv:2402.13446* **2024**.

 doi:10.20944/preprints202504.0219.v1

203. Walshe, T.; Moon, S.Y.; Xiao, C.; Gunawardana, Y.; Silavong, F. Automatic Labelling with Open-source LLMs using Dynamic Label Schema Integration. *arXiv preprint arXiv:2501.12332* **2025**.
204. 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). IEEE, 2024, pp. 1–9.
205. Edwards, J.; Petricek, T.; van der Storm, T.; Litt, G. Schema Evolution in Interactive Programming Systems. *arXiv preprint arXiv:2412.06269* **2024**.
206. Strome, T. Data governance best practices for the AI-ready airport. *Journal of Airport Management* **2024**, *19*, 57–70.
207. Suhra, R. Unified Data Governance Strategy for Enterprises. *International Journal of Computer Applications* **2024**, *186*, 36. https://doi.org/DOILink.
208. Aiyankovil, K.G.; Lewis, D. Harmonizing AI Data Governance: Profiling ISO/IEC 5259 to Meet the Requirements of the EU AI Act. *Frontiers in Artificial Intelligence and Applications* **2024**, *395*, 363–365. https://doi.org/10.3233/FAIA241270.
209. Gupta, P.; Parmar, D.S. Sustainable Data Management and Governance Using AI. *World Journal of Advanced Engineering Technology and Sciences* **2024**, *13*, 264–274. Received on 30 September 2024; revised on 11 November 2024; accepted on 13 November 2024, https://doi.org/10.30574/wjaets.2024.13.2.0551.
210. Idemudia, C.; Ige, A.; Adebayo, V.; Eyieyien, O. Enhancing data quality through comprehensive governance: Methodologies, tools, and continuous improvement techniques. *Computer Science & IT Research Journal* **2024**, *5*, 1680–1694.
211. Comeau, D.S.; Bitterman, D.S.; Celi, L.A. Preventing unrestricted and unmonitored AI experimentation in healthcare through transparency and accountability. *npj Digital Medicine* **2025**, *8*, 42.
212. 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), 2022. Report, 16 February 2022.
213. 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 preprint arXiv:2410.03925* **2024**.
214. ISLAM, M.; SOURAV, M.; REZA, J. The impact of data protection regulations on business analytics **2024**.
215. Eshbaev, G. GDPR vs. Weakly Protected Parties in Other Countries. *Uzbek Journal of Law and Digital Policy* **2024**, *2*, 55–65. https://doi.org/10.59022/ujldp.254.
216. 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.
217. 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. *Journal of Data Protection & Privacy* **2024**, *7*, 14–40. https://doi.org/10.69554/FWHU3837.
218. Aziz, M.A.B.; Wilson, C. Johnny Still Can't Opt-out: Assessing the IAB CCPA Compliance Framework. *Proceedings on Privacy Enhancing Technologies* **2024**, *2024*, 349–363. https://doi.org/https://doi.org/10.56553/popets-2024-0120.
219. Rao, S.D. The Evolution of Privacy Rights in the Digital Age: A Comparative Analysis of GDPR and CCPA. *International Journal of Law* **2024**, *2*, 40. https://doi.org/https://doi.org/10.36676/ijl.v2.i4.40.
220. 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. *Journal of Data Protection & Privacy* **2019**, *2*, 234–253.
221. Charatan, J.; Birrell, E. Two Steps Forward and One Step Back: The Right to Opt-out of Sale under CPRA. *Proceedings on Privacy Enhancing Technologies* **2024**, *2024*, 91–105. https://doi.org/https://doi.org/10.56553/popets-2024-0042.
222. Wang, G. Administrative and Legal Protection of Personal Information in China: Disadvantages and Solutions. *Courier of Kutafin Moscow State Law University (MSAL)* **2024**, pp. 189–197. https://doi.org/https://doi.org/10.17803/2311-5998.2024.122.10.189-197.
223. Yang, L.; Lin, Y.; Chen, B. Practice and Prospect of Regulating Personal Data Protection in China. *Laws* **2024**, *13*, 78. https://doi.org/https://doi.org/10.3390/laws13060078.
224. Bolatbekkyzy, G. Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation. *Groningen Journal of International Law* **2024**, *11*, 129–146. https://doi.org/https://doi.org/10.21827/GroJIL.11.1.129-146.

 doi:10.20944/preprints202504.0219.v1

225. 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, 2024; p. 15. https://doi.org/10.1201/9781003497189-15.
226. Ethical Governance and Implementation Paths for Global Marine Science Data Sharing. *Frontiers in Marine Science* **2024**, *11*. https://doi.org/10.3389/fmars.2024.1421252.
227. 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, 2024; pp. 41–48. https://doi.org/10.1108/978-1-83608-582-920241008.
228. McNicol, T.; Carthouser, B.; Bongiovanni, I.; Abeysooriya, S. Improving Ethical Usage of Corporate Data in Higher Education: Enhanced Enterprise Data Ethics Framework. *Information Technology & People* **2024**, *37*, 2247–2278. https://doi.org/10.1108/ITP-12-2022-0971.
229. Kottur, R. Responsible AI Development: A Comprehensive Framework for Ethical Implementation in Contemporary Technological Systems. *Computer Science and Information Technology* **2024**. https://doi.org/10.32628/CSEIT241061197.
230. Sharma, R.K. Review Article. *International Journal of Science and Research Archive* **2025**, *14*, 544–551. https://doi.org/10.30574/ijsra.2025.14.1.0122.
231. 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. *Information Fusion* **2023**, *99*, 101896.
232. 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. *European Journal of Theoretical and Applied Sciences* **2024**, *2*, 324–332. https://doi.org/10.59324/ejtas.2024.2(6).26.
233. Sari, R.; Muslim, M. Accountability and Transparency in Public Sector Accounting: A Systematic Review. *AMAR: Accounting and Management Review* **2023**, *3*, 1440. https://doi.org/10.37531/amar.v3i2.1440.
234. 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), 2018, pp. 1–7. https://doi.org/10.23919/CISTI.2018.8399475.
235. Weaver, L.; Imura, P. System and method of conducting self assessment for regulatory compliance, 2016. US Patent App. 14/497,436.
236. Križman, I.; Tissot, B. Data Governance Frameworks for Official Statistics and the Integration of Alternative Sources. *Statistical Journal of the IAOS* **2022**, *38*, 947–955. https://doi.org/10.3233/SJI-220025.
237. 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). IEEE, 2023, pp. 117–122.
238. Segun-Falade, O.D.; Leghemo, I.M.; Odionu, C.S.; Azubuike, C. A Review on [Insert Paper Topic]. *International Journal of Science and Research Archive* **2024**, *12*, 2984–3002. Received on 21 May 2024; revised on 02 July 2024; accepted on 05 July 2024, https://doi.org/10.30574/ijsra.2024.12.2.1177.
239. Janssen, M.; Brous, P.; Estevez, E.; Barbosa, L.S.; Janowski, T. Data governance: Organizing data for trustworthy Artificial Intelligence. *Government information quarterly* **2020**, *37*, 101493.
240. 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. *Available at SSRN* **2024**.
241. 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 Journal of the Communications Society* **2024**.
242. 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. *Journal of Engineering Research and Reports* **2025**, *27*, 247–267.
243. O'Sullivan, K.; Lumsden, J.; Anderson, C.; Black, C.; Ball, W.; Wilde, K. A Governance Framework for Facilitating Cross-Agency Data Sharing. *International Journal of Population Data Science* **2024**, *9*. https://doi.org/10.23889/ijpds.v9i5.2564.
244. Bammer, G. Stakeholder Engagement. In *Sociology, Social Policy and Education 2024*; Edward Elgar Publishing, 2024; pp. 487–491. https://doi.org/10.4337/9781035317967.ch107.

 doi:10.20944/preprints202504.0219.v1

245. Demiris, G. Stakeholder Engagement for the Design of Generative AI Tools: Inclusive Design Approaches. *Innovation in Aging* **2024**, *8*, 585–586. https://doi.org/10.1093/geroni/igae098.1918.
246. Siew, R. Stakeholder Engagement. In *Sustainability Analytics Toolkit for Practitioners*; Palgrave Macmillan: Singapore, 2023. https://doi.org/10.1007/978-981-19-8237-8_8.
247. Arora, A.; et al. Data-Driven Decision Support Systems in E-Governance: Leveraging AI for Policymaking. In *Artificial Intelligence: Theory and Applications*; Sharma, H.; Chakravorty, A.; Hussain, S.; Kumari, R., Eds.; Springer: Singapore, 2024; Vol. 844, *Lecture Notes in Networks and Systems*. https://doi.org/10.1007/978-981-99-8479-4_17.
248. Luo, J.; Luo, X.; Chen, X.; Xiao, Z.; Ju, W.; Zhang, M. SemiEvol: Semi-supervised Fine-tuning for LLM Adaptation. *arXiv preprint arXiv:2410.14745* **2024**.
249. Uuk, R.; Brouwer, A.; Schreier, T.; Dreksler, N.; Pulignano, V.; Bommasani, R. Effective Mitigations for Systemic Risks from General-Purpose AI. SSRN, 2024. Available at SSRN: https://ssrn.com/abstract=5021463 or http://dx.doi.org/10.2139/ssrn.5021463.
250. AIMultiple Research Team. Data Governance Case Studies, 2024. Accessed: 2025-03-14.
251. Google Cloud. Data Governance in Generative AI - Vertex AI, 2024. Accessed: 2025-03-14.
252. Microsoft. AI Principles and Approach, 2024. Accessed: 2025-03-14.
253. Microsoft. Introducing Modern Data Governance for the Era of AI, 2024. Accessed: 2025-03-14.
254. Majumder, S.; Bhattacharjee, A.; Kozhaya, J.N. Enhancing AI Governance in Financial Industry through IBM watsonx. governance. *Authorea Preprints* **2024**.
255. Schneider, J.; Kuss, P.; Abraham, R.; Meske, C. Governance of generative artificial intelligence for companies. *arXiv preprint arXiv:2403.08802* **2024**.
256. 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), 2023, pp. 291–295. https://doi.org/10.1109/CSCI62032.2023.00051.
257. Kumari, B. Intelligent Data Governance Frameworks: A Technical Overview. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* **2024**, *10*, 141–154.
258. Mökander, J.; Schuett, J.; Kirk, H.R.; Floridi, L. Auditing large language models: a three-layered approach. *AI and Ethics* **2024**, *4*, 1085–1115.
259. Cai, H.; Wu, S. TKG: Telecom Knowledge Governance Framework for LLM Application **2023**.
260. 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:cs.CY/2501.12456]. https://doi.org/10.48550/arxiv.2501.12456.
261. Mamalis, M.; Kalampokis, E.; Fitsilis, F.; Theodorakopoulosand, G.; Tarabanis, K. A Large Language Model based legal assistant for governance applications, 2024.
262. Zhao, L. Artificial Intelligence and Law: Emerging Divergent National Regulatory Approaches in a Changing Landscape of Fast-Evolving AI Technologies. In *Law 2023*; Edward Elgar Publishing, 2023; pp. 369–399. https://doi.org/10.4337/9781800884953.00033.
263. Imam, N.M.; Ibrahim, A.; Tiwari, M. Explainable Artificial Intelligence (XAI) Techniques To Enhance Transparency In Deep Learning Models. *IOSR Journal of Computer Engineering (IOSR-JCE)* **2024**, *26*, 29–36. https://doi.org/10.9790/0661-2606012936.
264. 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), 2023, pp. 1–6. https://doi.org/10.1109/ICETAS59148.2023.10346420.
265. 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. *Journal of Engineering Research and Reports* **2025**, *27*, 247–267. https://doi.org/10.9734/jerr/2025/v27i11385.
266. 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 Transactions on Engineering Management* **2024**, *71*, 14945–14962. https://doi.org/10.1109/TEM.2024.3472292.
267. 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), 2024, pp. 77–82. https://doi.org/10.1109/TELEPE64216.2024.00020.
268. Chaffer, T.J.; von Goins II, C.; Cotlage, D.; Okusanya, B.; Goldston, J. Decentralized Governance of Autonomous AI Agents. *arXiv preprint arXiv:2412.17114* **2024**.

 doi:10.20944/preprints202504.0219.v1

269. Nweke, O.C.; Nweke, G.I. Legal and Ethical Conundrums in the AI Era: A Multidisciplinary Analysis. *International Law Research Archives* **2024**, *13*, 1–10. https://doi.org/10.5539/ilr.v13n1p1.
270. Van Rooy, D. Human–machine collaboration for enhanced decision-making in governance. *Data & Policy* **2024**, *6*, e60. https://doi.org/10.1017/dap.2024.72.
271. Abeliuk, A.; Gaete, V.; Bro, N. Fairness in LLM-Generated Surveys. *arXiv preprint arXiv:2501.15351* **2025**.
272. Alipour, S.; Sen, I.; Samory, M.; Mitra, T. Robustness and Confounders in the Demographic Alignment of LLMs with Human Perceptions of Offensiveness. *arXiv preprint arXiv:2411.08977* **2024**.
273. 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), 2022, pp. 3898–3907. https://doi.org/10.1109/WACV51458.2022.00395.
274. Simpson, S.; Nukpezah, J.; Brooks, K.; et al. Parity benchmark for measuring bias in LLMs. *AI Ethics* **2024**. https://doi.org/10.1007/s43681-024-00613-4.