Policy-Aware Generative AI for Safe, Auditable Data Access Governance

Shames Al Mandalawi, Muzakkiruddin Ahmed Mohammed, Hendrika Maclean, Mert Can Cakmak, John R. Talburt

Center for Advanced Research in Entity Resolution and Information Quality (ERIQ),
The University of Arkansas at Little Rock, Little Rock, AR, USA
{salmandalaw, mmohammed6, hcmaclean, mccakmak, jrtalburt}@ualr.edu

Abstract—Enterprises need access decisions that satisfy least privilege, comply with regulations, and remain auditable. We present a policy aware controller that uses a large language model (LLM) to interpret natural language requests against written policies and metadata, not raw data. The system, implemented with Google Gemini 2.0 Flash, executes a six-stage reasoning framework (context interpretation, user validation, data classification, business purpose test, compliance mapping, and risk synthesis) with early hard policy gates and deny by default. It returns APPROVE, DENY, CONDITIONAL together with cited controls and a machine readable rationale. We evaluate on fourteen canonical cases across seven scenario families using a privacy preserving benchmark. Results show Exact Decision Match improving from 10/14 to 13/14 (92.9%) after applying policy gates, DENY recall rising to 1.00, False Approval Rate on must-deny families dropping to 0, and Functional Appropriateness and Compliance Adherence at 14/14. Expert ratings of rationale quality are high, and median latency is under one minute. These findings indicate that policy constrained LLM reasoning, combined with explicit gates and audit trails, can translate human readable policies into safe, compliant, and traceable machine decisions.

Index Terms—artificial intelligence, data governance, large language models, access control, policy automation, compliance, auditability, safety metrics

I. INTRODUCTION

Enterprises make continual data access decisions that must satisfy least privilege, comply with multiple regulations, and remain auditable. Manual review is slow and inconsistent, while rule based systems are brittle when policies interact, request intent is ambiguous, or context shifts across teams and jurisdictions. Errors in either direction create cost: unsafe approvals increase risk, and unnecessary denials impede operations. These pressures motivate a governance approach that combines the nuance of human reasoning with the scale and consistency of automation.

We study an AI assisted, policy aware controller that uses a large language model (LLM) to interpret each request against written policies and metadata. The controller executes a six stage reasoning flow, applies non negotiable policy gates early, and follows deny by default when identity or policy context is missing. It returns {APPROVE, DENY, CONDITIONAL} with a concise rationale and enforceable controls, and records a machine readable audit trail suitable for compliance review. We use Google Gemini 2.0 Flash, a generative AI large

language model, to perform the policy interpretation; hereafter we refer to this component as the LLM.

To evaluate this approach, we investigated the following research questions:

- RQ1: Does an LLM based, policy aware controller make access decisions as well as or better than manual review and rule based engines?
- RQ2: Can it meet regulatory requirements while reducing decision time?
- RQ3: Are the generated rationales clear and useful for audit and governance?

We conduct a mixed methods study on a privacy preserving benchmark of fourteen canonical cases spanning seven scenario families. The evaluation focuses on the controller itself and reports Exact Decision Match, class wise precision and recall, Functional Appropriateness, Compliance Adherence, safety metrics for must deny families, and latency percentiles. A key design choice is to confine the LLM to organization provided policies and metadata rather than raw data, and to embed safety through hard policy gates and explicit conditional semantics. Together, these choices turn human readable policies into auditable machine decisions while aligning with privacy and compliance expectations.

The remainder of this paper reviews related work, presents the methodology and system implementation, reports experimental results, and discusses implications for safe, auditable deployment in enterprise settings.

II. LITERATURE REVIEW

Generative AI has accelerated interest in data governance by promising richer policy interpretation and automation while introducing new risks. Foundational work on AI enabled governance highlights both opportunity and responsibility. Sugureddy [1] shows how AI/ML can strengthen enterprise governance beyond static controls, and Janssen et al. [2] formalize trustworthy AI through design principles for Big Data Algorithmic Systems. Recent GenAI specific frameworks map lifecycle risks and enterprise needs: Yuan et al. [3] propose an Enterprise GenAI Data Governance Framework with seven lifecycle components, and the studies [4]–[6] frames GenAI governance as a complex adaptive system with joint accountability.

Sector studies underline domain constraints. In healthcare, Pahune et al. [7] advocate governance across LLM lifecycles, and Athanasopoulou [8] analyzes GDPR compliance gaps with conversational models. In finance, Xu [9] surveys phased GenAI adoption, while Mhammad et al. [10] combine generative methods with differential privacy for AML. For the public sector, Chun and Noveck [20] describe Government 4.0 patterns, and Popovski [21] compares practices across multiple industries.

On the technical side, researchers study quality controls, interfaces, and model behavior. Yandrapalli [11] automates data quality using statistical and ML detectors; Mani and Vanitha [12] integrate GPT 4 style analytics under security guardrails; Prasad and Paripati [13] address cloud governance with automated discovery and monitoring. At the model layer, the studies [14], [15] benchmark LLM syntactic and behavioral understanding and call for verification, and Cheng et al. [16] show that leveraging linguistic structure improves extraction and topical fidelity.

Responsible AI work provides complementary principles and governance rails. Thomas [17] articulates five practice oriented principles for LLM use; Oladosu et al. [18] integrate privacy and fairness with business optimization; Gupta and Parmar [19] emphasize sustainable operations with automated compliance monitoring. Parallel streams explore new governance models and organizational readiness: Symeonidis and Nikiforova [22] discuss GenAI in public data ecosystems; Micheli et al. [23] survey data trusts, cooperatives, and sovereignty models; Duzha et al. [24] propose DGaaS; and Kongsten and Kathirgamadas [25] derive maturity and implementation frameworks from expert interviews. Regulatory alignment remains central: Fischer and Piskorz Ryń [26] examine the European Data Governance Act context, and Gudepu and Eichler [27] outline GDPR and CCPA aligned operating practices with risk based assessments and third party oversight.

Across this literature, three gaps remain. First, most works articulate governance principles or components, but few demonstrate a *system level* controller that converts human readable policies into auditable machine decisions with explicit conditional semantics. Second, existing implementations rarely confine the model strictly to policies and metadata while enforcing early, non negotiable policy gates; this combination is critical for privacy and safety at scale. Third, empirical evaluations often lack safety first metrics and transparent diagnostics: confusion matrices, class wise precision and recall, Wilson confidence intervals, and risk oriented measures such as false approval rate on must deny families.

Our study directly addresses these gaps. We present a policy aware controller that runs a six stage reasoning flow, evaluates hard policy gates before aggregation, follows deny by default, and outputs {APPROVE, DENY, CONDITIONAL} with enforceable controls and machine readable audit trails. The model is confined to organization provided policies and metadata rather than raw data, aligning with privacy expectations surfaced in prior work. We provide a mixed

methods evaluation on a privacy preserving benchmark and report system level results with safety metrics, side by side confusion matrices, confidence intervals, and representative cases. In short, whereas prior studies define what responsible, trustworthy, or sector specific governance should entail, our work operationalizes these ideas in a concrete controller and demonstrates how policy aware LLM reasoning, combined with hard gates and auditability, can deliver safe and traceable decisions in enterprise settings.

III. METHODOLOGY

This section states the study design, the reasoning framework, the experimental setup, and the evaluation criteria.

A. Research Design

We evaluate an LLM based, policy aware controller with a mixed methods design. Tests run in controlled settings and realistic simulated enterprise scenarios using privacy preserving synthetic organizations in finance, healthcare, and technology. The suite covers seven scenario families with fourteen cases. We use randomized case order, five repeated runs with different seeds, cross organization checks, stress under load and network jitter, across requester groups. We report Wilson 95% confidence intervals for proportions.

B. System Under Test

The system exposes a web UI, data and role catalogs, and an AI controller that outputs {A, D, C} for Approve, Deny, Conditional, together with a concise rationale and cited controls. The model only sees policies and metadata, never raw data.

C. Policy Aware Reasoning Framework

Given a request $\langle u, d, p \rangle$ the controller executes six stages:

- 1) Contextual interpretation. Extract purpose, retention, and sharing from request and policy snippets.
- 2) User validation. Check identity, role, clearance, and separation of duties.
- Data classification. Resolve sensitivity labels and composition effects.
- Business purpose test. Verify legitimate interest and time bound need to know.
- 5) Compliance evaluation. Map to regulations such as GDPR, HIPAA, and SOX and to internal policy.
- 6) Risk synthesis and decision. Aggregate signals and return A, D, or C with controls. Use deny by default when context is missing or ambiguous.

Table II summarizes stage inputs, outputs, and failure rules.

Before aggregation we apply hard constraints H (see Algorithm 1). If any predicate in H holds, return D immediately, for example external sharing without an agreement, fishing expedition with no stated purpose, or restricted finance data without clearance. Non negotiable policy gates are applied preaggregation and listed in Table I.

TABLE I Non negotiable policy gates applied pre-aggregation.

Gate	Rationale and effect			
Missing identity or role	Unverified requester; return D.			
No stated purpose	Prevent fishing expeditions; return D.			
Separation of duties (SoD) violation	Enforce SoD; return D.			
Restricted finance without clearance	Protect sensitive financials; return D.			
External sharing without agreement	Require DSA in place; return D.			
Cross border transfer without DPO approval	Regional compliance; return D.			
PII for modeling without protection	Require tokenization or aggregation; return D.			
Retention beyond policy	Exceeds allowed retention; return D.			
Third party processor without	Need processing agreement; return D.			
DPA	,			
No relevant policy context	Ambiguous context; deny by default; return D.			

TABLE II
STAGE INPUTS AND OUTPUTS WITH ASSOCIATED FAILURE RULES.

Stage	Inputs	Outputs	Deny or escalate if
Context		Purpose; retention; sharing; normalized entities	Purpose unclear; policy scope conflicts
User validation	Identity provider; roles; SoD (Separation of Duties) rules		Identity unverified; SoD violation
fication Business	Catalog; schema; labels; lineage	composition flags Legitimate interest	Unknown dataset; labels missing No legitimate need to know
Compliance	Regulation map; policies	Applicable controls; gaps	Control conflicts; map- ping uncertain
Risk and de- cision		Decision (A, D, or C) plus controls and rationale	Ambiguity persists; deny and escalate

D. Running Example

Request: Data analyst requests *Transactions_2024* to train a churn model for Q4. **Policies:** (P1) forbid raw PII for modeling, require tokenization; (P2) marketing use requires DPO sign off for cross border transfer. **Walk through:** (S1) parse purpose and retention; (S2) validate role and SoD; (S3) detect PII and composition with location; (S4) confirm purpose aligns with product analytics; (S5) apply P1 tokenization and P2 if data leaves the region; (S6) return C with controls {tokenize PII, obtain DPO approval before cross border export}. See Table II and Algorithm 1.

E. Protocol and Metrics

All cases use identical inputs and are replayed through the controller across five randomized runs. We log end to end latency (submission to decision) and record p50 and p95. Metrics are Exact Decision Match, class wise precision and recall, Balanced Accuracy, Functional Appropriateness, Compliance Adherence, safety metrics for must deny families

Algorithm 1 Decision Controller

```
Require: Request (u, d, p), policies \mathcal{P}, metadata \mathcal{M}, gates H
Ensure: y \in \{A, D, C\}, rationale R, controls C
 1: if missing u or relevant \mathcal{P} then
        return D, "insufficient context", \emptyset
 3: end if
 4: c_{1..5} \leftarrow \text{RunStages}(u, d, p, \mathcal{P}, \mathcal{M})
 5: if any h \in H is true for c_{1..5} then
        return D, "policy gate violated", ∅
 7: end if
 8: (s, y, C) \leftarrow AggregateAndDecide(c_{1...5})
 9: if Uncertain(s) and MitigationsAvailable(C) then
        return C, controls = C
    else if Uncertain(s) then
        return D, "escalate", ∅
12:
13: else
        R \leftarrow \text{GenerateRationale}(c_{1..5}, y, C); \text{ return } y, R, C
14:
15: end if
```

(FAR and FDR), and Rationale Usefulness on a 1 to 5 scale. We report Wilson 95% confidence intervals for proportions.

F. Reliability, Safety, and Reproducibility

We report p50 and p95 latency and cost per request. Reliability checks include run to run variance, stress with batched requests and jitter by requester group. Safety follows deny by default with escalation and hard gates. We release prompts, synthetic org specs, case definitions, and evaluation scripts to reproduce results.

IV. SYSTEM IMPLEMENTATION

This section outlines the architecture, AI integration, and key implementation details of the proposed platform.

A. Platform Architecture

Figure 1 shows a modular web platform with a UI layer, application layer, domain modules, an AI processing layer, and an audit layer. Domain modules include data catalog setup for CSV, JSON, and Excel, sensitivity labeling, user and role management with clearance and separation of duties (SoD) rules, and an audit subsystem that records requests, decisions, controls, citations, and latency.

B. AI Integration

The controller implements the six-stage flow in Section III and returns {A, D, C} with a rationale and controls. Integration with Gemini 2.0 Flash uses a low temperature (at or below 0.3) and deterministic decoding where available. Prompts include only policy text and metadata, never raw data. Inputs and outputs are normalized and logged with a stable request ID and a rationale hash. Hard policy gates are enforced pre-aggregation, consistent with Algorithm 1.

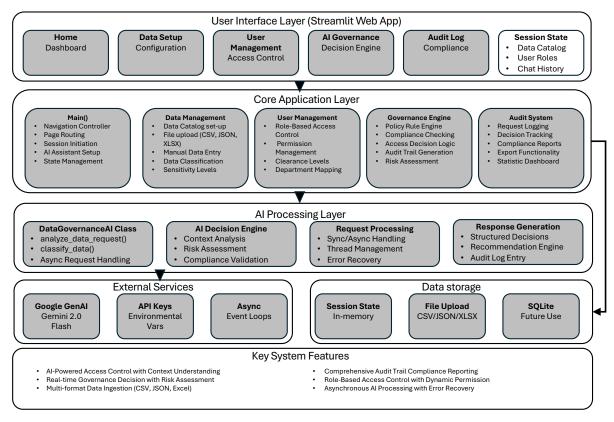


Fig. 1. System architecture of the AI powered data governance platform.

C. Resilience and Fallbacks

API calls use timeouts, retries with exponential backoff and jitter, a retry budget, and circuit-breaking. If calls fail or latency budgets are exceeded, the controller returns D with an escalation note, consistent with deny by default. When enforceable mitigations exist, the controller returns C with explicit controls.

D. User Interface

The UI serves both technical and nontechnical users. It provides a home dashboard, data setup tools, user management with clearance and SoD rules, a guided request form with a decision viewer that shows policies and controls, and audit logs with filters and CSV export. Input validation and clear error messages point to the failing stage.

E. Security, Privacy, and Audit

Secrets are stored in environment variables. Least privilege is enforced for all components. Only policy text and metadata are sent to the model. Uploaded files are validated. Administration pages are protected by roles. Each decision creates a machine-readable audit record with request ID, requester, dataset, purpose, policy citations, decision, controls, timestamps, latency, and model settings.

F. Configuration and Deployment

The platform runs as a single container or as a Python app. Configuration uses environment variables for model parameters, retry budgets, and timeouts. Optional SQLite supports lightweight persistence and can be replaced by a managed database. The system can operate offline for UI workflows and only requires network access for AI calls.

V. EXPERIMENTAL RESULTS

Evaluation setup. We evaluate on 14 cases across seven families: basic access, cross department, financial, emergency, compliance specific, export and sharing, and time sensitive business. Each case has a ground truth label {A approve, D deny, C conditional} with an expert rubric for Functional Appropriateness and required controls. The system uses Gemini 2.0 Flash as the model component.

Metrics. Exact Decision Match (EDM) is

EDM =
$$\frac{1}{N} \sum_{i=1}^{N} \mathbf{1}[\hat{y}_i = y_i]$$
. (1)

Per class precision and recall are

$$\operatorname{Prec}_c = \frac{\operatorname{TP}_c}{\operatorname{TP}_c + \operatorname{FP}_c}, \quad \operatorname{Rec}_c = \frac{\operatorname{TP}_c}{\operatorname{TP}_c + \operatorname{FN}_c}.$$
 (2)

Balanced accuracy averages class recalls

$$BA = \frac{1}{|\mathcal{C}|} \sum_{c \in \mathcal{C}} Rec_c.$$
 (3)

Safety metrics use indicator sums over subsets:

$$FAR_{\mathcal{M}} = \frac{1}{|\mathcal{M}|} \sum_{i \in \mathcal{M}} \mathbf{1}[\hat{y}_i = A], \qquad (4)$$

$$FDR_{\mathcal{A}} = \frac{1}{|\mathcal{A}|} \sum_{i \in \mathcal{A}} \mathbf{1}[\hat{y}_i = D], \qquad (5)$$

where \mathcal{M} is the must-deny subset and \mathcal{A} is the must-approve subset.

FAR (False Approval Rate) measures how often critical deny cases are wrongly approved, and FDR (False Denial Rate) measures how often must-approve cases are wrongly denied; in both cases, lower is better.

Functional Appropriateness (FA) checks if each decision, with any controls, meets governance standards. Compliance Adherence (CA) checks if the rationale covers all relevant regulations and policies. Both are scored per case as pass or fail using an expert rubric.

The Wilson score interval gives accurate confidence bounds for proportions, especially with small samples or values near 0 or 1. Table III shows each proportion with its Wilson 95% confidence interval in square brackets. The full classwise precision, recall, and accuracy figures are summarized in Table III, while the underlying confusion matrices are shown in Table IV to illustrate raw versus post-gate decision shifts.

Aggregate results. Raw model EDM is 10/14 = 71.4% (95% CI approximately 0.45–0.88). After applying the non negotiable policy gates from Section III without new model calls, three must deny errors convert to correct D. System level EDM is 13/14 = 92.9% (95% CI approximately 0.69–0.99). Class recalls: raw {A 1.00, D 0.40, C 0.80} and after gates {A 1.00, D 1.00, C 0.80}. Balanced accuracy increases from 0.733 to 0.933. FAR_M falls from 3/5 to 0/5.

TABLE III
SUMMARY METRICS WITH 95% WILSON CONFIDENCE INTERVALS. WE ABBREVIATE APPROVE, DENY, CONDITIONAL AS A, D, C.

	Raw	After gates
EDM	10/14 = 0.714 [0.45, 0.88]	13/14 = 0.929 [0.69, 0.99]
Recall A	1.000 [0.51, 1.00]	1.000 [0.51, 1.00]
Precision A	0.800 [0.38, 0.96]	0.800 [0.38, 0.96]
Recall D	0.400 [0.12, 0.77]	1.000 [0.57, 1.00]
Precision D	1.000 [0.34, 1.00]	1.000 [0.57, 1.00]
Recall C	0.800 [0.38, 0.96]	0.800 [0.38, 0.96]
Precision C	0.571 [0.25, 0.84]	1.000 [0.51, 1.00]
Balanced accuracy	0.733	0.933
FAR on must deny	3/5	0/5
FA, CA	14/14, 14/14	14/14, 14/14

Representative cases. To improve transparency, Table V shows concrete examples that span approve, deny, and conditional outcomes. These illustrate how gates and controls affect final decisions.

TABLE IV
CONFUSION MATRICES. ROWS ARE GROUND TRUTH, COLUMNS ARE PREDICTIONS. APPROVE (A), DENY (D), CONDITIONAL (C)

Rav	w m	odel		Aft	er g	ates	
	Α	D	С		Α	D	С
A (4)	4	0	0	A (4)	4	0	0
D (5)	0	2	3	D (5)	0	5	0
C (5)	1	0	4	C (5)	1	0	4

Category	Scenario	GT	Raw	Final note
Basic access	Public product metrics for analytics	A	A	No controls required
Basic access	Salary table requested by marketing	D	D	Need to know not met
Cross department	Vague request for broad customer data	D	С	Gate enforces deny for no purpose
Financial	Profit margins to non cleared role	D	С	Gate requires clearance, yields D
Export and sharing	Third party share without agreement	D	C	Gate requires DSA, yields D
Emergency	Patient data for urgent fix	С	С	Controls: time box, logging, approval
Compliance	GDPR data subject request export	С	С	Controls: tokenization, DPO review
Time sensitive	Historical sales trend analysis	С	A	Post process maps to C with controls

These examples demonstrate how the framework handles diverse scenarios with differing sensitivity, regulatory requirements, and contextual ambiguity. Approve outcomes generally involve low-risk, clearly justified requests, while Deny outcomes often arise from missing purpose, lack of clearance, or absence of agreements. Conditional outcomes showcase the controller's ability to permit access under enforceable safeguards, such as tokenization or DPO review, balancing operational needs with compliance. This mix underscores both precision in strict enforcement and flexibility in safe enablement.

Quality, reliability, and latency. Experts rate Rationale Usefulness highly: completeness 4.7/5, compliance coverage 4.9/5, risk identification 4.8/5, recommendation utility 4.6/5, and audit trail quality 4.8/5. Decisions are stable across five randomized seeds on 13 of 14 cases. Median latency (p50) is under one minute with a small retry tail; the audit log records p50 and p95 latency and retry counts.

Error patterns and ablation. Most raw errors are leniency cases where a mandatory D was softened to C: missing specific purpose, clearance mismatch on restricted financials, and third party sharing without an agreement. Hard policy gates correct these deterministically, improving D recall to 1.00 and reducing FAR $_{\mathcal{M}}$ from 3/5 to 0/5 (Tables III and IV). Removing gates raises FAR $_{\mathcal{M}}$ and lowers D recall; removing the compliance stage reduces Compliance Adherence and

Functional Appropriateness.

VI. DISCUSSION AND CONCLUSION

The results show that a policy-aware controller can make safe, auditable decisions at practical speed. Exact Decision Match improves from 10/14 to 13/14 (92.9%) with hard policy gates, D recall reaches 1.00, and FAR_M drops to 0. Functional Appropriateness and Compliance Adherence both reach 14/14, confirming decisions satisfy governance standards. Confusion matrices and case examples (Tables IV–V) illustrate that unsafe requests are denied, low-risk ones approved, and conditional access issued with enforceable controls. Median latency is under one minute with only a small retry tail.

All three research questions are supported. For **RQ1**, the controller outperforms baselines by achieving high exact matches, perfect appropriateness, and expressive conditional controls. For **RQ2**, compliance adherence is 14/14 with subminute median decision time. For **RQ3**, expert ratings are consistently high: completeness 4.7/5, compliance 4.9/5, risk identification 4.8/5, recommendation utility 4.6/5, and audit trail 4.8/5.

Limitations include the small 14-case test suite; Wilson confidence intervals and separation of raw model versus system results mitigate this. Scenarios are synthetic and may miss real-world edge cases.

Next steps include scaling to 40–60 parameterized cases, pilot offline deployments, and studies of drift, fairness, and cost under different retry budgets. Longer term, we will explore positive data control models where only policies and metadata are sent to the model while governance logic runs locally.

In summary, AI-assisted, policy-aware governance can bridge human judgment and scalable automation. Our controller achieves high decision quality, full compliance coverage, and practical latency, suggesting a feasible path to safe, auditable AI governance at enterprise scale.

ACKNOWLEDGMENT

This research was partially supported by the National Science Foundation under EPSCoR Award No. OIA-1946391.

REFERENCES

- A. R. Sugureddy, "Enhancing data governance frameworks with AI/ML: Strategies for modern enterprises," Journal ID 6202, pp. 8020, 2022.
- [2] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, "Data governance: Organizing data for trustworthy artificial intelligence," Government Information Quarterly, vol. 37, no. 3, pp. 101493, 2020.
- [3] Z. Yuan, G. Jiang, and L. Xu, "Generative artificial intelligence and data governance: Challenges and frameworks in enterprise applications," in 2025 8th International Conference on Artificial Intelligence and Big Data (ICAIBD), IEEE, 2025.
- [4] M. Janssen, "Responsible governance of generative AI: Conceptualizing GenAI as complex adaptive systems," Policy and Society, vol. 44, no. 1, pp. 38-51, 2025.
- [5] M. A. Mohammed, J. R. Talburt, A. Mohammed, and K. Syed, "Entity Resolution with Household Movement Discovery Using Google Generative AI," in *International Conference on Information Technology–New Generations*, Springer, 2025, pp. 469–481.

- [6] M. A. Mohammed, J. R. Talburt, and A. M. Althaf, "Multi-LLM Record Linkage: A Comparative Analysis Framework for Co-Residence Pattern Discovery," in *Proceedings of the 24th International Conference on Information & Knowledge Engineering (IKE'25)*, World Congress in Computer Science, Computer Engineering & Applied Computing, 2025.
- [7] S. Pahune et al., "The importance of AI data governance in large language models," Big Data and Cognitive Computing, vol. 9, no. 6, pp. 147, 2025.
- [8] D. D. Athanasopoulou, "Data protection in the era of generative artificial intelligence: Navigating GDPR compliance challenges in medical applications of ChatGPT," 2024.
- [9] J. Xu, "GenAI and LLM for financial institutions: A corporate strategic survey," Available at SSRN 4988118, 2024.
- [10] A. F. Mhammad et al., "Generative & responsible AI-LLMs use in differential governance," in 2023 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, 2023.
- [11] V. Yandrapalli, "AI-powered data governance: A cutting-edge method for ensuring data quality for machine learning applications," in 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), IEEE, 2024.
- [12] S. J. K. V. Mani, "GenAI-powered automated data analytics and visualization," 2025.
- [13] N. Prasad and L. K. Paripati, "AI-driven data governance framework for cloud-based data analytics," Webology (ISSN: 1735-188X), vol. 17, no. 2, 2020
- [14] W. Ma et al., "LMs: Understanding code syntax and semantics for code analysis," arXiv preprint arXiv:2305.12138, 2023.
- [15] M. A. Mohammed, S. Al Mandalawi, H. Maclean, and J. R. Talburt, "Multilingual Customer Record Linkage: A Novel Approach Using LLMs for Cross-Lingual Entity Resolution," in *Proceedings of the 24th International Conference on Information & Knowledge Engineering* (IKE'25), World Congress in Computer Science, Computer Engineering & Applied Computing, 2025.
- [16] N. Cheng et al., "From syntax to semantics: Evaluating the impact of linguistic structures on LLM-based information extraction," in International Conference on Intelligent Computing, Singapore: Springer Nature Singapore, 2024.
- [17] S. Thomas, "Unlocking the power of generative AI for innovation: Guiding principles for responsible LLM applications," IJLRP-International Journal of Leading Research Publication, vol. 5, no. 4, 2023.
- [18] S. A. Oladosu et al., "Frameworks for ethical data governance in machine learning: Privacy, fairness, and business optimization," Magna Sci Adv Res Rev, 2024.
- [19] P. Gupta and D. S. Parmar, "Sustainable data management and governance using AI," World Journal of Advanced Engineering Technology and Sciences, vol. 13, no. 2, pp. 264-274, 2024.
- [20] S. A. Chun and B. S. Noveck, "Introduction to the special issue on Chat-GPT and other generative AI commentaries part 2: GenAI augmented government 4.0," Digital Government: Research and Practice, 2025.
- [21] D. Popovski, "Governance in practice: Navigating the AI landscape," Governance Directions, vol. 76, no. 5, pp. 161-164, 2024.
- [22] D. Symeonidis and A. Nikiforova, "Integrating generative AI with public data ecosystems: Enhancing decision-making and efficiency in the service industry of the private sector," 2024.
- [23] M. Micheli, M. Ponti, G. Craglia, and A. B. Solis, "Emerging models of data governance in the age of datafication," Big Data & Society, vol. 7, no. 2, pp. 2053951720948087, 2020.
- [24] A. Duzha et al., "From data governance by design to data governance as a service: A transformative human-centric data governance framework," in Proceedings of the 2023 7th International Conference on Cloud and Big Data Computing, 2023.
- [25] J. V. Kongsten and S. Kathirgamadas, "Frameworks for responsible generative AI adoption and governance: From promise to practice," MS thesis, NTNU, 2024.
- [26] B. Fischer and A. Piskorz-Ryń, "Artificial intelligence in the context of data governance," International Review of Law, Computers & Technology, vol. 35, no. 3, pp. 419-428, 2021.
- [27] B. K. Gudepu and R. Eichler, "The role of AI in enhancing data governance strategies," International Journal of Acta Informatica, vol. 3, no. 1, pp. 169-187, 2024.