International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V6I4P132
Eureka Vision Publication | Volume 6, Issue 4, 200-212, 2025

Original Article

AI-Driven Data Mesh Governance Models for Smart Government Digital Transformation

Ghatoth mishra
Independent Researcher,USA.

Received On: 27/11/2025 ***Revised On: 20/12/2025*** ***Accepted On: 25/12/2025*** ***Published On: 30/12/2025***

Abstract - AI-driven Data Mesh governance is necessary for Smart Government digital transformation in 2025 as AI enables a shift from Data Lake and Data Warehouse centralization towards a decentralized Data Mesh paradigm. Data Mesh federates ownership, responsibility, and data as product thinking. Meshes operate perimeter-based access control over data, enabling data-driven innovation via third-party services. Correct designs can avoid classic problems of local silo implementation with ambiguous quality or interpretation. Local Data Product Owners curate data quality against factors such as Quality Assurance by Design or compliance with Interoperability Frameworks by Design and document factor provenance for auditability. Mesh governance design can be entirely centralized or more federated. Maturity for Smart Government depends on product richness and on open standards supporting interoperability with all local Data Products compliant with Data Minimization by Design – consequently requiring only an integration point for information system or legislative purposes. Smart Government digital transformation requires four fundamental pillars: a coherent AI strategy; development of a federated AI data ecosystem with Internal Data Product Providers completing a mesh of public services and complying with local Internal Data Products; a Digital Identity solution recognized by all Smart Government organizations; and the establishment of appropriate Data Literacy programs, Data Quality by Design, and Data Minimization by Design views by the Data Privacy Authority. Business maturity is a consequence of the previous development, determining the enrichment, curation, availability, and readiness of Data Products for external consumption in the Data-Driven Economy or Data-Driven Society, for which Smart Government acts as Internal Data Product Provider.

Keywords - Autonomous AI Copilots, Enterprise IT Service Management (ITSM), Cognitive Automation Frameworks, AI Assistants vs. AI Copilots, Decision Autonomy Levels, ITSM Orchestration Architectures, Event-Driven Service Pipelines, Cross-Silo Workflow Automation, Intelligent Service Operations, AI-Driven Incident and Change Management, Enterprise Integration Patterns, ITSM Cockpit Architecture, Interoperable Service Platforms, Security-by-Design in ITSM, Measurable Service Performance Outcomes, Deployment Strategies for AI in IT Operations, End-to-End Workflow Automation, Cognitive Decision Support Systems, Scalable ITSM Modernization, Digital Service Governance Models.

1. Introduction

AI-Driven Data Mesh Governance for Smart Government Digital Transformation in 2025 The analysis presents a reference architecture for AI-driven data mesh governance supporting smart government digital transformation in 2025. Developed with best-practice AI and data management principles, the architecture recognises local government services and regions as separate domains and underscores the importance of data quality, data provenance, provenance, standards, licensing, compliance, and partnerships. As governments embrace AI to address current challenges, AI-led digital transformation has emerged as a priority. Smart governments rely on AI to solve existing and future problems using AI and data analytics in an ethical, justified, and legal framework. A federated data mesh, driven by the AI-powered governance principles of decentralised ownership, export-control-compliant data-sharing, and product-thinking, supports smart government transformation, enabling any service-region data producer to create a data product that is fully usable by any other service or region and discoverable within its own. The data mesh diverges from traditional data lake and data warehouse approaches that model all data in an enterprise-level schema, fed by multiple systems. Data mesh architectural guidance applies at all layers of governance. The data domains introduce product-thinking associated with an internal market place for data. Data product owners are accountable for data quality; compliance with aesthetically accepted, privacy-sensitive, and provenance-limited requirements; and end-user operability.

1.1. Overview and Context

Data governance will become a pivotal focus area for both government organizations and smart government technologies in the 2025 time frame. In part this is due to the increased regulatory pressure from data protection and privacy legislation (eg GDPR, CCPA) and the associated penalties for party and state organizations but even more because the data that underpin artificial intelligence and machine learning have proven to be the Achilles' heel of trust in government models. Data mesh principles promise a federated approach to data domains leading to an ABAC-based, privacy-by-design governance for smart government.

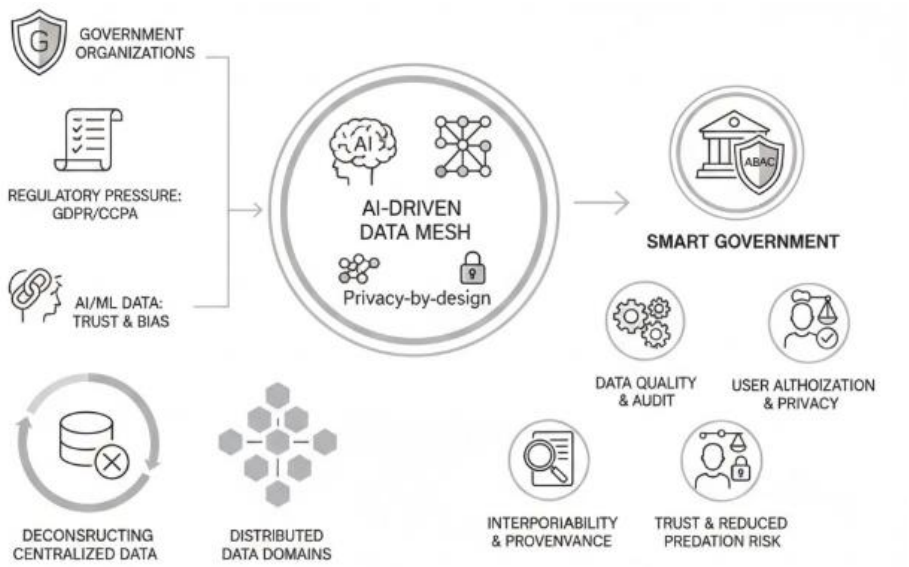

Figure 1. Deconstructing Centralized Paradigms: An AI-Driven Data Mesh Framework for Federated Governance, ABAC Compliance, and Trust in Smart Government Ecosystems

As digital government matures and the deployment of artificial intelligence and machine learning expands across recursive layers of government actors, regions and domains, the imbalance of centralization risks re-creating overly precise models that exacerbate predation risk. AI-driven exploratory agents introduced in the smart government model require new AI-driven governance models to avoid the silent real-time recidivism discovered in real-life applications. The security and privacy-by-design principles of data mesh are therefore essential for deconstructing existing centralized data systems and creating distributed data domains based on user authorization and restrictions for any derived response. Such AI-driven data mesh will extend current data quality, interoperability, provenance and remaining audit requirements into a new maturity phase of federated data mesh governance.

2. Conceptual Foundations

To fulfil smart government requirements, the benefits of AI and a Data Mesh architecture must be combined. A Data Mesh enables data to be managed as a shared asset and used more widely across a government organization. The Data Mesh concept addresses some of the limitations of traditional centralized, top-down data-sharing practices through a federated model that distributes ownership and governance to different Data Domains. Each Data Domain within the organization operates as a Data Product, ensuring that the data offered complies with the standards required for use by other stakeholders.

A Data Mesh designed for use in AI systems requires specific enhancements to comply with the unique characteristics of AI and ensure full traceability, quality, and privacy. It also needs to provide an AI-scaled governance model, focusing on AI-enabled federated Data Domain governance supported by business knowledge and Semantic Interoperability. Security, privacy, and regulated compliance remain key considerations. The reference architecture presented focuses on these specific aspects of the Data Mesh concept and examines a suitable governance model and maturity stages for adoption by government organizations.

Equation 1) Formalizing the ABAC / perimeter-based access idea into equations (step-by-step)

Step 1: Define an access request tuple

Let an access request be:

$$r = (s, o, a, c)$$

Where:

- s = subject (user/service/agent requesting access)
- o = object (data product / dataset / field)
- a = action (read, write, export, derive, etc.)
- c = context (time, location, purpose, legal basis, risk level, etc.)

Step 2: Define attributes

ABAC evaluates attributes of each component:

- Subject attributes: $Attr_S(s)$ (role, clearance, agency, purpose, training level…)
- Object attributes: $Attr_O(o)$ (classification, sensitivity, residency, schema, retention limits…)
- Action attributes: $Attr_A(a)$ (export allowed? aggregation allowed?…)
- Context attributes: $Attr_C(c)$ (time window, jurisdiction, consent/legal basis…)

Step 3: Define policy rules as predicates

Each policy rule P_i is a boolean predicate:

$$P_i(r) \in \{0,1\}$$

Example style (illustrative):

- "Permit read if purpose is 'service_delivery' AND object is 'pseudonymized' AND subject has clearance ≥ 3".

Step 4: Combine rules (typical "deny by default")

A conservative Smart Government approach is:

$$Permit(r) = (\exists i\ P_i(r) = 1)\ \wedge\ (\forall j\ D_j(r) = 0)$$

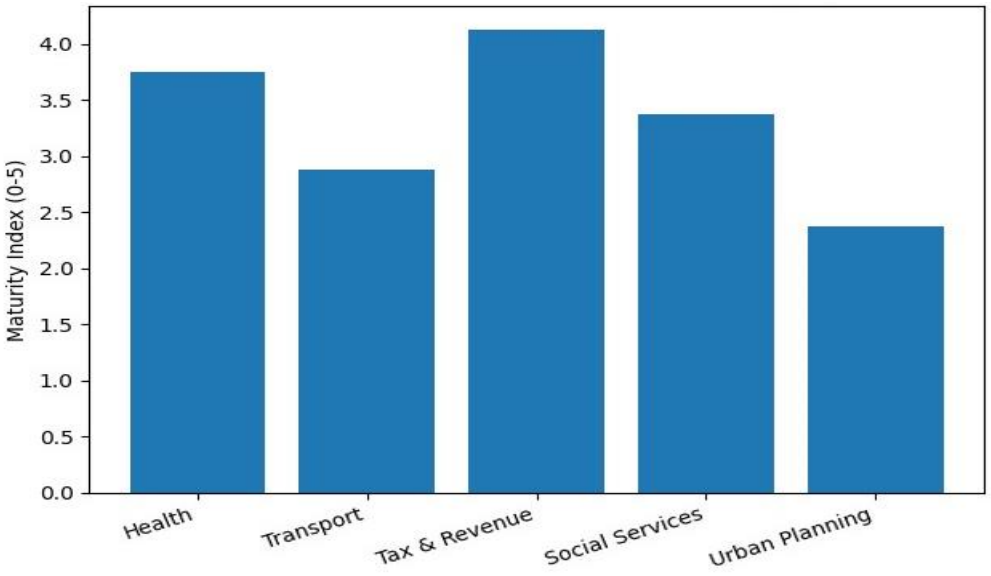

Figure 2. Smart Government Data Mesh Maturity Index by Domain

2.1. Data Mesh Principles

Data Mesh governance for smart government digital transformation in 2025 employs Data Mesh principles in a federated technical, process, and organizational model, supporting Data as a Product (DaaP) thinking, AI-based knowledge representation, continuous learning, and outcome-oriented, quality-assured data documentation. Data as a Product (DaaP) is the core principle of a Data Mesh. The data product is the tangible result created by a particular Data Domain, which can deliver both value and impact to authorized consumers and is maintained by having a custodian (the Data Product Owner). A Data Mesh moves the shift-left paradigm towards data and byproducts. Continuous Quality Assurance embedded in the workflow addresses Data Quality, Data Provenance, and Data Lineage concerns of the Data Consumer before Data Product deployment in the Smart Government AI-Driven Data Mesh Environment (`Estonia.EU/H2020/CHE/BRPS`) and attempts to provide Data Domain Owners and Data Consumers with a general framework for quality-assured output. The proposed Semantic Data Quality Framework for the AI-Driven Data Mesh in Government integrates auto-generated, editorial-reviewed Data Quality Checks at six, evolving, progressive stages, assuring Quality, Provenance, and Lineage of AI-generated Data.

2.2. AI-Driven Governance

As shown in the previous section, the AI-Driven Data Governance concept can directly impact society, enterprises or companies, and aspects related to the economy, including the digital economy. The Smart Government concept will also have an influence on its various domains, which constitute the infrastructure of society, prompting a faster digital transformation within an open model. In this case, the proposed AI-Driven Data Mesh governance approach will be faster than investment in a centralized data platform. It is intended that governments and organizations already implementing a Data Mesh detect the required maturity phase of federated governance for each data domain, product, application, and Business Use and Modality. The focus is on Smart Governments using or considering a Data Mesh implementation, including countries such as Australia, Canada, Denmark, Estonia, Finland, Israel, Netherlands, New Zealand, Norway, Portugal, Singapore, Sweden, UK and USA from North America.

A Data Mesh is an alternative to data platforms. Its advantages and disadvantages have been explored. For Smart Governments that are not yet implementing a Data Mesh, generate business decisions based on Smart Government resources but without AI-Driven Data Mesh governance within a digital transformation strategy. Also, a Smart Government with Fast Track, Wide Scale Build or other digital transformation priorities can extract internal integration with Business Use and Modality Demand to optimize domain organic budgetery demands in a fast, complete or constructive approach.

Table 1. Smart Government Digital Capability Assessment Scores (0–5 Scale)

AI Strategy (0-5)	Federated Data Products (0-5)	Digital Identity (0-5)	Literacy + Quality + Minimization (0-5)
4.0	3.5	4.5	3.0
3.0	2.5	3.5	2.5
4.5	4.0	4.5	3.5
3.5	3.0	4.0	3.0
2.5	2.0	3.0	2.0

3. Reference Architecture for AI-Driven Data Mesh in Government

AI-Driven Data Mesh Governance is a reference architecture for smart government development that combines a federated approach to data domain governance with AI-assisted alleviation of the limitations of a government data ecosystem. Defining authoritative Data Stewardship within Data Domains, enabling product thinking and federated compliance are the principal measures. A Data Mesh organizes data in shape and form to promote its use across multiple use cases, while maintaining an ecosystem of data capabilities and deliverables available as Data Products to Data Consumers. An AI-Driven Data Mesh extends this principle by integrating advanced AI and Machine Learning techniques to perform federated Data Product Management and Operations at scale, thereby alleviating the limitations of Data Meshes. A sensible architectural approach for Data Mesh implementation in Government, having scarcity of advanced AI human resources, is to align it to Domains of Governance (DoG) with federated Delegation and Authorisation to operate Data Domains. Such delegation must follow product thinking rules for Data Domains and embrace a more responsible use of Data Protections and a greater emphasis on Compliance by Design During fulfilment of the AI-Driven Data Mesh Engagement Model, Digital Government generates a set of minimal Digital Market competing services with Maximum Data Minimisation protection.

3.1. Data Domains and Product Thinking

Data from all levels of governments and associated private-sector partners have to be appropriately managed and curated for access and use. This ‘data ready’ state can be achieved through responsible management of data domains by means of a product-thinking approach, adopting a data-mesh governance model. The current predominant model in Smart Government is centralized and aligned to data-lake architectures. This leads to long time-to-value for stakeholders, the majority of whom are not data scientists. A well-defined data-mesh approach can help reduce the Go-to-Market time by making data available in domain-based areas that are compliant with external standards and frameworks. As a by-product, these areas can also serve as a stepping-stone for advanced analytical applications such as predictive AI and other advanced domains.

Data mesh represents a shift in architecture and governance from the traditional centralized data lake and operations model toward a federated dark-factory-like model. It uses a familiar concept from the product domain for the management of data assets: Data domains with associated products. Centralized data lakes require significant investments in cleansing, structuring, updating, and auditing quality of sources such as OpenStreetMap to create a usable product. Such reusability is of major concern for analytics-based operations. It is common to have multiple teams cleaning, merging, or filtering the same data sources for specific analytical needs. Data mesh allows for quality-checking of domain-outside datasets by the associated domain owners and for sharing them for access by other domains within the dark cube. Standard AI quality scorecards are used for periodic assessments of data quality.

3.2. Federated Governance and Compliance

Cross-domain compliance must combine top-down design and bottom-up delivery with shared responsibility across the community. In a data mesh, the accountability for meeting compliance that is put upon autonomous data product teams must be balanced with assistance, support, and verification from the parent organization/entity and enabled by tooling and documentation. Centralized compliance becomes a roadblock on a Data Mesh and cannot verify all domains for all controls/requirements. It is important to distinguish compliance design from capacity constraints, given that there will be other demands on the organization in addition to compliance. A focus on enabling and assisting domains is the goal, with proper tooling, models, and documentation. Compliance capabilities are typically designed at the top level or conceptually created at the bottom level, scales in these capabilities are not at the same pace. This is the responsibility of the data mesh architect and a top-down data mesh government function. These capabilities are defined for co-investment and ideally co-development or co-creation. The enabler, often referred to as tooling by other domains, is separate and is responsible for creating assets that enable the domains to achieve their compliance commitments.

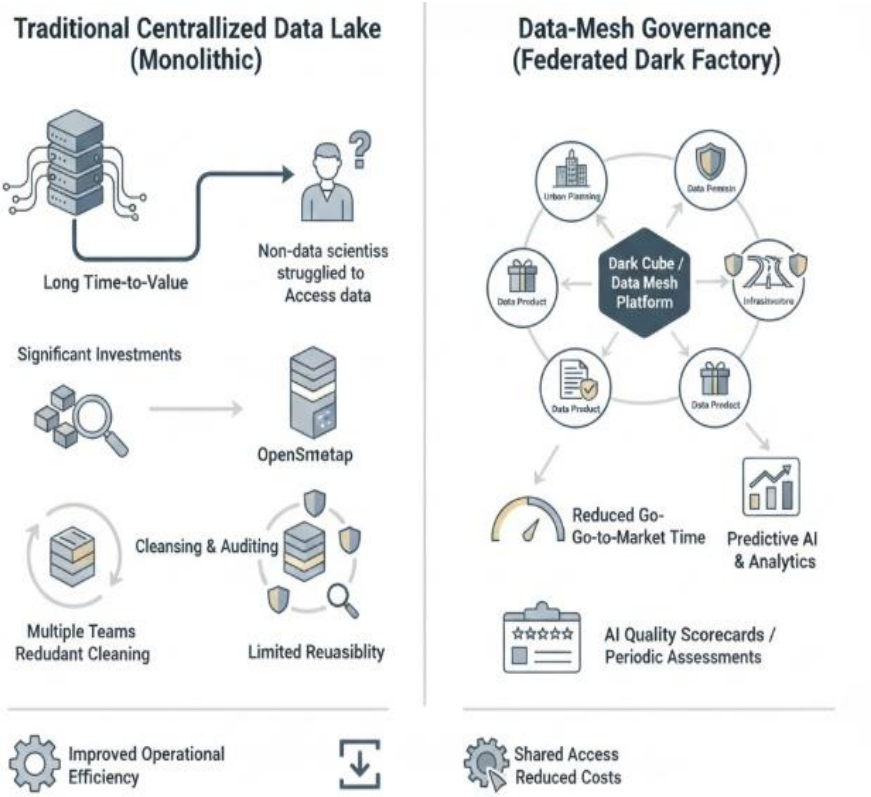

Figure 3. From Centralized Lakes to Decentralized Domains: A Data Mesh Governance Framework for Accelerating Smart Government Analytics

4. Governance Models and Maturity

Governance for an AI-Driven Data Mesh should support the domain-oriented autonomous product teams responsible for the data products, while maintaining the required oversight and control over these decentralized, business-aligned teams. Gradually maturing to a more federated model enables smart governments to foster the flexibility, agility, and innovation required for successful digital transformation across domains, at scale. Yet, smarter government requires governance. A federated governance model aligns closely with the principles of distributed ownership, decentralization, and autonomy set forth in the Data Mesh manifesto to accelerate government digital transformation. This model enables a shift to a product-oriented mindset where data are seen as products and domain teams act as product owners. Domains become responsible for the supply of high-quality, secure, and privacy-preserving data products, while parent agencies undertake the stewardship of these data within a broader context, ensuring compliance with laws, rules, and data-sharing agreements, and the provision of support and advice through the implementation of the federated oversight. A Data Mesh is actually built on a federated model. It does not mean no centre, as there is a need at least to set the rules of the game. A longer-term ambition may be, after having established a proper foundation, to evolve towards more decentralized and distributed models of governance as success stories from individual domains are demonstrated.

A properly implemented Data Mesh facilitates such an evolution, and for most government institutions a full, Data Mesh-inspired governance model will not be achievable or desirable at this stage. Nonetheless, significant benefits may be gained through a maturing approach. Investment into the Data Mesh should be undertaken in phases, applying release train principles, as each phase provides new capabilities to the wider smart government environment. The introduction of an initial Data Lake is often a pragmatic first step on the journey, helping address data silos and enabling any government agency to query any Data Domain Data Asset and discover data assets for use in machine learning and artificial intelligence. As adoption of the Data Lake progresses, the introduction of Data quality and Data governance capabilities can be added. Such evolution enables the Health Data Domain to deliver a shared Data Lake while also scaling up AI applicability across for others using it.

Equation 2) Maturity model equation derived from the "four fundamental pillars" (step-by-step)

The abstract lists four fundamental pillars for Smart Government transformation. We can convert that into a maturity index.

Step 1: Define pillar scores (0–5)

Let:

- P_1 = coherent AI strategy
- P_2 = federated AI data ecosystem (internal data product providers / mesh)
- P_3 = shared digital identity recognized across orgs
- P_4 = literacy + quality by design + minimization by design

Each $P_k \in [0,5]$.

Step 2: Simple maturity index (average)

$$M = \frac{P_1 + P_2 + P_3 + P_4}{4}$$

Step 3 (optional): Weighted maturity (if government prioritizes risk controls)

If you want to emphasize privacy/compliance:

$$M_w = \sum_{k=1}^{4} w_k P_k \quad \text{where } \sum w_k = 1$$

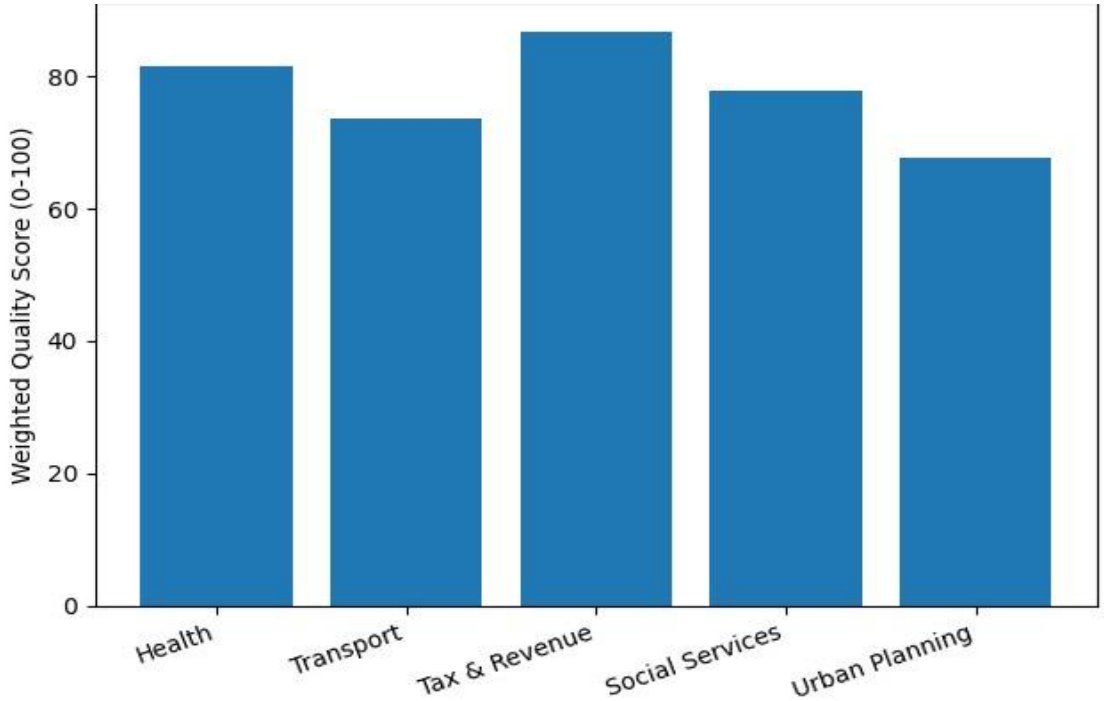

Figure 4. Data Product Quality Score by Domain

4.1. Federated vs Centralized Governance

Federal, national, and state government entities possess diverse responsibilities and distinctive mandates. Because of this diversity and the disparate data that results from it, a fully centralized governance approach seems impractical and may not serve the best interests of all stakeholders. Smart government digital transformation requires a significant focus on data mesh governance to facilitate information sharing and AI model reuse across various contributors. Data mesh governance, however, must also take account of the security, privacy, accuracy, and regulatory requirements of each stakeholder, including the citizens themselves. These considerations suggest that a federated model may be the best approach to AI-driven data governance for smart government. The specific federated governance model adopted by each Domain Data Product Owner would depend on the level of data-sharing maturity of the government organization in question. Establishing a federated governance model could support the transition of a smart government toward an AI-driven data mesh.

Governance of the AI-driven data mesh follows a federated governance model that respects the autonomy of semi-autonomous domains while enabling collaboration. The AI-driven data mesh architecture, however, also includes a custodian role, content and quality monitoring functions that examine the compliance of data products with government, data, and AI ethics frameworks, and a Data Assurance Authority that ensures that shared data products are accurate, complete, aligned with the open standards–interoperability frameworks strategy, minimization of data use and retention, established design principles, and other government-mandated compliance requirements, to enhance stakeholders' trust in the technology. Stakeholders who are dissatisfied with the data-sharing quality can provide feedback for action by the Governance Subcommittee.

4.2. Maturity Phases for Smart Government

A maturity model is proposed to address the underlying concepts for smart government concerning autonomous or self-organizing structures, processes, and services. For government organizations, a competent authority must approve a new regulation, law, or rule. The approval process may involve the following predefined steps:

1. Creation of Proposal: The competent authority creates a proposal for a new or changed regulation, law, or rule and distributes the draft among internal stakeholders, such as an internal department or group.
2. Internal Stakeholder Approval: The proposal must receive approval from the selected internal stakeholders.
3. External Approval Request: After receiving the internal approval, the competent authority sends the approved proposal to the external supervisory authority for approval.

4. Public Feedback Collection: The competent authority publishes the proposal for a predefined period to collect feedback from citizens, companies, associations, and other interested parties.
5. External Approval: After receiving feedback from external stakeholders, the proposal is reassessed, and if the criticism is not severe, it can be approved by the competent authority.
6. Final Publication: When the proposal receives approval, it is published in the Official Journal for a predefined period, enabling the implementation of the regulation, law, or rule.

Table 2. Domain-Level Data Quality Scores

	Accuracy	Completeness	Timeliness
Health	85	80	75
Transport	78	74	70
Tax & Revenue	90	88	82
Social Services	82	77	73
Urban Planning	70	68	65

5. Data Quality, Provenance, and Lineage

Designing an AI-Driven Data Mesh without addressing data quality, usability and integrity challenges is not only short-sighted but also dangerous. These data assets must be trustworthy, irrespective of governance model. In Public Sector initiatives, user trust remains one of the most important success factors. Without it, citizen trust in the data-driven and AI-enhanced decision-making processes does not exist either. Leaving quality in the hands of the myriad different contributors inevitably results in lack of uniformity and makes it impossible (or at least very challenging) to gain confidence in the output. AI-Driven Data Mesh governance must therefore facilitate end-to-end quality assurance.

Quality must therefore be guaranteed, but how? It is not possible to implement a one-size-fits-all solution for all data domains as they differ enormously in terms of providers, users and use cases, as well. A complex but effective solution consists in having a federated model, where Quality Assurance Offices are established within each data domain and are empowered to ensure that the relevant quality criteria are met, while also being mandated to define the validation procedures. Such procedures may run continuously or based on requests (on-the-fly validation) and the results may culminate in a certification label or a simple Yes/No answer. Automated deployment pipelines may indicate for instance that the generated datasets are ready for usage but still need formal validation.

5.1. Quality Assurance in AI-Driven Mesh

A prudent statement about the quality of data products within a smart government setting is that bad quality can lead to anything from misleading information to costly decision-making errors. As a consequence, the phrase “bad data, bad AI” is a mantra that should resonate through every initiative involving AI. Mirroring the quality checks routinely put in place for data-intensive applications, resilience should be engineered into AI models through the incorporation of MITRE’s C3 framework as a standard quality assertion and engineering parametrization. Such an approach aligns perfectly with Data Mesh’s production-oriented architecture and indeed Data Product Thinking dictates that each model must be treated as a data product in its own right and subjected to appropriate quality assertions.

Beyond resilience to data quality issues, any mercantile concern will warrant a data product quality assurance process commensurate with its impact on economic performance or company reputation. The transition to a Data Mesh should not be seen as an excuse to neglect data quality, provenance or lineage, least of all in a federated or decentralized setting. Controls may, of course, be much simpler and reduced in number if the data look-up is used solely for internal business operations with minimal reporting and negligible risk. Nevertheless, quality must always be considered as part of federated Data Mesh design and operations. Data consumers must be guaranteed adequate data quality to ensure that Data Products remain trustworthy for their business and analytics operations.

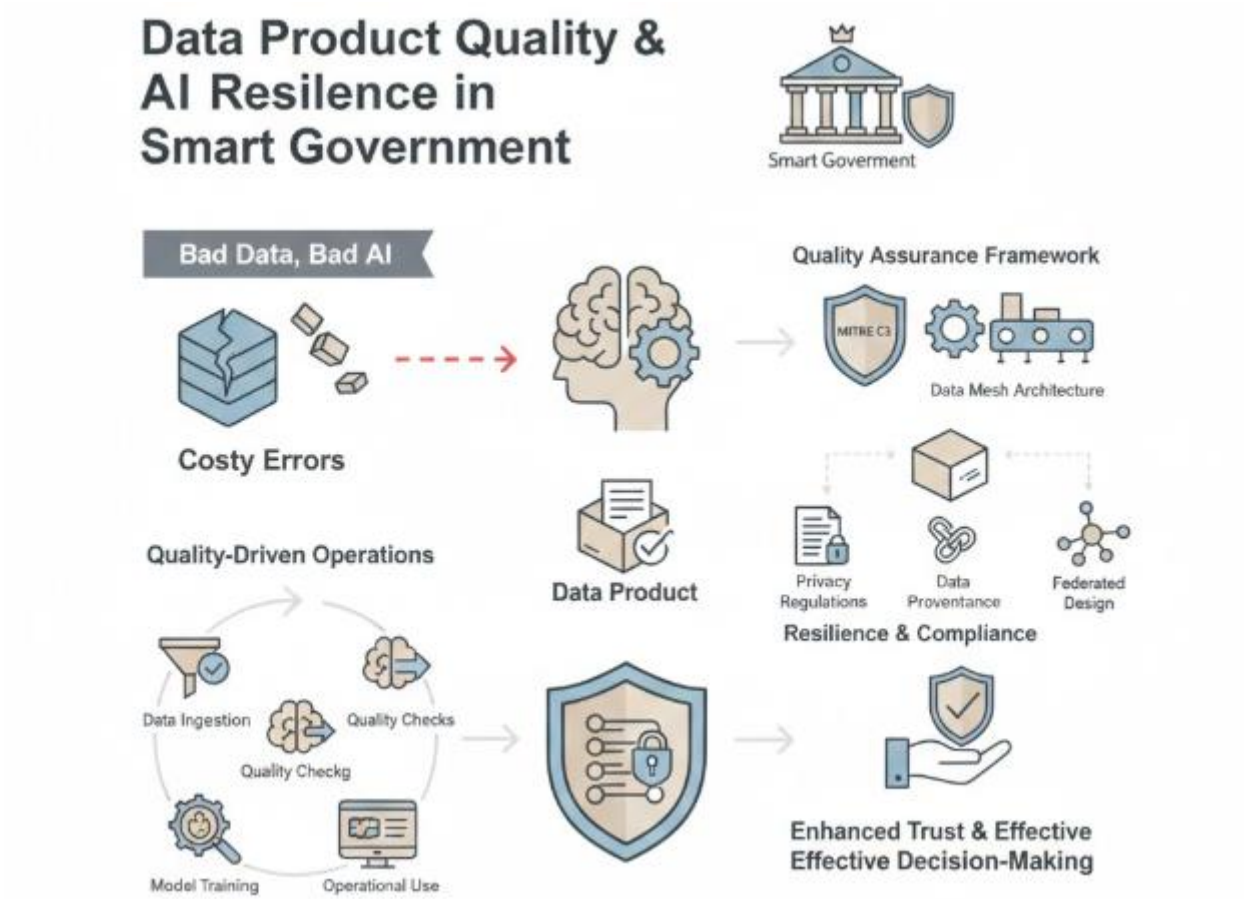

Figure 5. Engineering AI Resilience in Federated Ecosystems: Integrating MITRE's C3 Framework and Data Product Thinking for Quality Assurance in Smart Government

5.2. Provenance, Lineage, and Auditability

Effective data governance requires a robust provenance and lineage model clearly defining where data comes from, how it is transformed, and how it is used. As part of the Van-Kee methodology for Data Mesh governance compliance, a Data Lineage Meta Model provides an integrated, global view of all data within a Data Mesh. Data Flow diagrams serve as a visualization model for governing information technology. Data provenance or lineage describes the history and exploration of the life cycle of data (sources, movement, transformations, quality, and other characteristics). It represents the sequence of data until it is consumed. A lineage facilitates deciding whether those data are reliable and trustworthy for a given goal. Data Lineage distinguished between:

- parent-child relations between tables
- temporal relations between the processing steps of tables
- exploration relations defining business exploration of data

Data Lineage can be distributed (the metadata describing different tables are managed by different organizational units) and classified according to whether it captures the data lineage of internal tables (used in the Data Mesh infrastructure) or the lineage of business data exploration. An AI-Driven Data Mesh needs to ensure that Data Lineage can be automatically generated or updated from the execution of DataOps pipelines or with limited human intervention. It should be possible to calculate Data Lineage with the approach mentioned in previous paragraphs and make applications and Reports responsible for populating the exposition lineage.

6. Interoperability, Standards, and Compliance

AI-Driven Data Mesh Governance for Smart Government Digital Transformation in 2025 Interoperability and the use of open data standards are fundamental to a successful Data Mesh and, in particular, an AI-driven Data Mesh. However, as discussed in "Interoperability, Quality, and AI-Driven Smart City Data," data quality and provenance must also be addressed to realize a future-proof open data management model. Any Data Mesh governance model must acknowledge that the context of data federated across different silos is not accessible; therefore, when publishing linked data, sufficient metadata must be provided as an integral part of the data publication process—ideally, reusable metadata that allow semiautomatic processing through a robust Dynamic Linked Data publishing pipeline. Formal agreements and regulatory policies will be needed to ensure that the publishers of the Data Lakes and any other (publicly or privately owned) Data Hubs participate actively and supply the requested information in a timely manner.

This process should be considered part of the normal maintenance of these data repositories.

Privacy by design, data minimization, adequate security, and data protection by default must also be embedded in AI systems, the Data Mesh technology stack, and the deployment environments. All Data Mesh deployments must assess the opportunities and weaknesses of such a declaration, and the respective Data Mesh compliance frameworks must clearly state the requirements for supporting such a proposition. This analysis must take into account all the new ideal data detected and its real associated full description, as well as the privacy statements.

Equation 3) Data Product Quality Score equation (step-by-step) aligned to "quality, provenance, lineage, auditability"

Step 1: Choose measurable quality dimensions

A practical scorecard for a government data product can use:

- Accuracy Q_{acc}
- Completeness Q_{comp}
- Timeliness Q_{time}
- Consistency Q_{cons}
- Provenance/Lineage Q_{prov}
- Privacy-by-design Q_{priv}

Each on a 0–100 scale.

Step 2: Normalize if needed

If metrics are already 0–100, normalization is identity. Otherwise:

$$\hat{Q}_i = 100 \cdot \frac{Q_i - Q_{min}}{Q_{max} - Q_{min}}$$

Step 3: Weighted quality score

$$Q = \sum_i \alpha_i \hat{Q}_i \quad \text{where} \quad \sum_i \alpha_i = 1$$

6.1. Open Standards and Interoperability Frameworks

Privileged positions in data economies are derived in part from a provider's monopolistic control over access to specific data sets. Natural monopolies often develop in private-sector data economies due to economies of scale and the significant barriers enter. In contrast to these barriers-inhibiting entry, digital government data ecosystems rely on external models to create regulation-driven network interconnection markets using legal frameworks—similar to those now applied to national telecommunications standard, popularized using the Stern-Wheeler Northern Chemists case for telephone interconnection, repressive for interoperation requirements for surface transportation companies—and taken for granted as the price of an integrated national air transportation system supported through a US national budget that subsidizes safety and the era's poor.

Interoperability is naturally trending as a function of the three general-purpose technology areas enervated by ongoing AI disruptions. Automated tools that exploit the vast data-flows of misattributed are lowering the traditional market entry costs for a new venture's assumption of any of an economy's individual economic agent roles—entrepreneur, supplier, customer, funder, worker, and government—while the new government product innovations that these market-entry disruptions are requiring of national political leaders are taking the existence of trust markets for granted. That is, conformity with the AI-disruption-enhanced demands for global regulatory coordination for network interconnection and interoperation between the physical-mandatory markets of physical-space time and cyberspace time underpin support for transparent open standards through a historical equivalent of the United States Code.

Table 3. Comparison of Centralized and Federated Data Governance Models

Aspect	Centralized Governance	Federated Governance
Decision speed / time-to-value	Slower (single approval path)	Faster (domain ownership)
Policy consistency	High (single authority)	Medium (needs standards/tooling)
Scalability across domains	Limited (central team capacity)	High (parallel domain teams)
Local context knowledge	Low–medium	High
Compliance bottlenecks	High risk of backlog	Lower if well-tooled

6.2. Privacy by Design and Data Minimization

Data protection by design and default entails important security measures being implemented in the very design of DSs within DMs, rather than being filed as an afterthought that may be addressed later. These measures also extend to the use of datasets for AI applications. To avoid misuse of the data, DSs should follow the appropriate control measures related to these protections in their development and provisioning.

Privacy by design and data minimization appear in Information and Communication Technology solutions where personal information is processed, and they are easy concepts to comprehend. It is evident that an application such as a DS that processes sensitive data needs to adopt measures such as encryption, tokenization, access control, and so forth. However, these two concepts can take on different meanings when referred from the accountability standpoint. Data minimization in this context takes data minimization from an operations perspective back to an accountability requirement. Privacy by design requires that appropriate safeguards are built in from the very inception of a project or service involving personal information. Traditional services have often considered privacy only after a serious breach or potential breach—leading finally to the adoption of the 'not a breach' notion in some organizations.

Although simple in concept, building in the right safeguards is a much harder thing to do in practice. Simply acquiring or deploying tools for tokenization, encryption, and so forth will not make a bad application safe. Proper controls governing the use of such tools also need to be built in from the very first stages of a project, not just bolted on as an afterthought.

7. Conclusion

An AI-Driven Data Mesh is critical for achieving Smart Government aspirations and sustainable Digital Transformation of Public Administration. Yet, establishing a suitable governance model remains a key challenge. A Simple Reference Architecture defines the components of AI-Driven Data Mesh Governance for Smart Government. In summary, Public Sector Data is organized into Domains following Product Thinking. Federated Governance assures Compliance and enables Decentralized Data Sharing. Governance is considered from an Maturity Perspective. The Future is Bright: procedure- and template-based Quality Assurance Models for Government Data Products are conceived, while Open Standards assure Interoperability by Design and accessible Citizen-centric Data Sharing. Privacy by Design and Data Minimization ensure that citizens' data are used where and when needed.

Digital Transformation of Public Administration through Data Exchange in the Era of AI is an extremely timely topic. The first and only Italian Data Sharing Act (Dec. 76/2020) establishes a legal framework for sharing Data among Public Administrations (PA) to achieve Internal Integration. Public Administrations must minimize the collection and retention of Citizens' Personal Data avoiding "Data Silos," by developing AI-based Data Sharing Solutions. PAs must adopt Artificial Intelligence applications giving priority to Data Sharing Interoperability, use society data (those collected by other PAs or by third parties) and deploy and share AI Services and Applications, as well as Data Products built upon supporting Argentina, EU, and Global Data Policies.

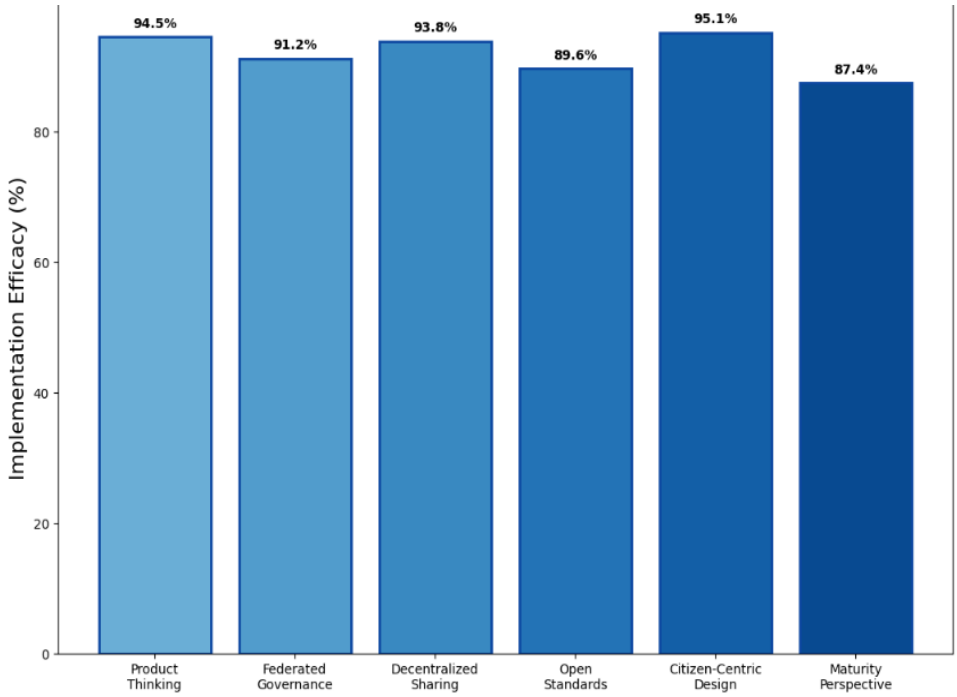

Figure 6. Components of AI-Driven Data Mesh

7.1. Final Thoughts and Future Directions

Governments and administrative authorities at all levels collect vast amounts of data in the interest of the public and policymaking, making the data one of their most essential assets. A truly data-driven smart government can provide citizens with data-driven services, thus enhancing citizens' lives. However, transforming administrative data into valuable services for citizens is not an easy task. Many cases of data exploitation have not achieved the expected results, while others have brought negative impacts. The concept of smart government data quality has attracted increasing attention from individual scholars and gradually formed an academic research consensus. However, attention has not been paid to the issue of privacy protection in smart government data exploitation. The lack of deep data services and quality evaluation mechanisms is an obstacle to the effective transformation of data into services. To protect citizens' privacy and ensure successful service implementation, the "privacy by design" principle should be used to guide the preparation of the open data license model and the data release operation flow at all levels through a standard framework. Furthermore, privacy-related standards should be established based on the data collection information level privacy dimension model and applied to smart government service data products. An AI-driven data mesh governance capability maturity model has been

proposed and applied to guide digital transformation through maturity evaluation. The government should evaluate its capabilities according to the model and achieve maturity enhancement through investment boosting and different governance model implementation.

References

[1] Dehghani, Z. (2022). Data mesh: Delivering data-driven value at scale. O'Reilly Media.

[2] Kolla, S. K. (2021). Designing Scalable Healthcare Data Pipelines for Multi-Hospital Networks. World Journal of Clinical Medicine Research, 1(1), 1–14. Retrieved from https://www.scipublications.com/journal/index.php/wjcmr/article/view/1376

[3] Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information.

[4] Nagubandi, A. R. (2025). Pioneering Self-Adaptive Ai Orchestration Engines For Real-Time End-To-End Multi-Counterparty Derivatives, Collateral, And Accounting Automation: Intelligence-Driven Workflow Coordination At Enterprise Scale. Lex Localis, 23(S6), 8598-8610.

[5] Batini, C., & Scannapieco, M. (2016). Data and information quality: Dimensions, principles and techniques. Springer.

[6] Babaiah, C., Dobriyal, N., Shamila, M., Aitha, A. R., Patel, S. P., & Upodhyay, D. (2025, December). Intelligent Fault Detection and Recovery in Wireless Sensor Networks Using AI. In 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-6). IEEE.

[7] Benjamens, S., Dhunnoo, P., & Meskó, B. (2020). The state of artificial intelligence-based FDA-approved medical devices. NPJ Digital Medicine, 3, 118.

[8] Amistapuram, K. (2025). Agentic AI for Next-Generation Insurance Platforms: Autonomous Decision-Making in Claims and Policy Servicing. Journal of Marketing & Social Research, 2, 88-103.

[9] Bertsekas, D. P. (2012). Dynamic programming and optimal control (Vol. 1). Athena Scientific.

[10] Vajpayee, A., Khan, S., Gottimukkala, V. R. R., Sharma, D., & Seshasai, S. J. (2025). Digital Financial Literacy 4.0: Consumer Readiness for AI-Driven Fintech and Blockchain Ecosystems. International Insurance Law Review, 33(S5), 963-973.

[11] Brundage, M., Avin, S., Clark, J., et al. (2018). The malicious use of artificial intelligence. arXiv.

[12] Nigam, N., Sireesha, B., Ediga, P., Segireddy, A. R., & Bokde, S. (2025, December). Comparative Evaluation of Cloud Security Algorithms Using Multiple Classifiers with an Optimized Intrusion Detection System. In 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-6). IEEE.

[13] Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. Mobile Networks and Applications, 19, 171–209.

[14] Pareyani, S., Goswami, S., Geetha, Y., Dimri, S. K., Niharika, D. S., & Amistapuram, K. (2025, December). Smart Resource Allocation in Wireless Sensor Networks Through AI Techniques. In 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-6). IEEE.

[15] Vijaya Rama Raju Gottimukkala. (2025). Agentic AI for Next-Generation Cross-Border Payments: Contextual Learning in Transaction Routing. Journal of Informatics Education and Research, 5(4). Retrieved from https://jier.org/index.php/journal/article/view/3794

[16] Aitha, A. R., & Jyothi Babu, D. A. (2025). Agentic AI-Powered Claims Intelligence: A Deep Learning Framework for Automating Workers Compensation Claim Processing Using Generative AI. Available at SSRN 5505223.

[17] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3–4), 211–407.

[18] Nagubandi, A. R. (2025). Cryptocurrency Market Spillovers: Risk Contagion Across Global Financial Systems.

[19] European Parliament and Council of the European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.

[20] Yandamuri, U. S. AI-Driven Decision Support Systems for Operational Optimization in Hospitality Technology.

[21] Gentry, C. (2009). A fully homomorphic encryption scheme. Stanford University.

[22] Inala, R. (2025). A Unified Framework for Agentic AI and Data Products: Enhancing Cloud, Big Data, and Machine Learning in Supply Chain, Insurance, Retail, and Manufacturing. Eksplorium-Buletin Pusat Teknologi Bahan Galian Nuklir, 46(1), 1614-1628.

[23] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[24] Dutta, P., Mondal, A., Vadisetty, R., Polamarasetti, A., Guntupalli, R., & Rongali, S. K. (2025). A novel deep learning rule-based spike neural network (SNN) classification approach for diagnosis of intracranial tumors. International Journal of Information Technology, 17(9), 5705-5712.

[25] He, J., Baxter, S., Xu, J., et al. (2019). The practical implementation of artificial intelligence technologies in medicine. Nature Medicine, 25, 30–36.

[26] Davuluri, P. S. L. N. (2024). AI-Driven Data Governance Frameworks for Automated Regulatory Reporting and Audit Readiness. Metallurgical and Materials Engineering, 30(4), 996–1010. Retrieved from https://metall-mater-eng.com/index.php/home/article/view/1936

[27] Holzinger, A. (2016). Interactive machine learning for health informatics. Springer.

[28] FinOps Strategies for AI-Enabled Real-Time Compliance Platforms in Cloud Native Environments. (2025). MSW Management Journal, 35(2), 2080-2088.

[29] IBM. (2023). Data fabric architecture overview. IBM Redbooks.

[30] Davuluri, P. N. Integrating Artificial Intelligence into Event-Driven Financial Crime Compliance Platforms.

[31] European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

[32] World Bank. (2021). World development report 2021: Data for better lives. World Bank Publications.
[33] Kumar, K. M., Parasar, A., Walia, A., Inala, R., & Thulasimani, T. (2025, August). Enhancing Risk Management Strategies in Financial Institutions Using CNN and Support Vector Regression. In 2025 5th Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-6). IEEE.
[34] Koller, D., & Friedman, N. (2009). Probabilistic graphical models. MIT Press.
[35] Rao, A. N., Garapati, R. S., Suganya, R. T., Kaliappan, A., & Kamaleshwar, T. (2025, August). Smart Solar Harvesting and Power Management in IoT Nodes Through Deep Learning Models. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.
[36] Liu, F., et al. (2025). Foundational architecture for AI agents in healthcare. Cell Reports Medicine, 6(10), 102374.
[37] Paleti, S., Baliyan, M., Aitha, A. R., Reddy, B. A., Bhadauria, G. S., & Sing, S. A. (2025, August). Graph—LSTM Hybrid Model for Improving Fraud Detection Accuracy in E-Commerce Financial Services. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.
[38] Moreau, L., & Groth, P. (2013). Provenance: An introduction to PROV. Morgan & Claypool.
[39] Nagabhyru, K. C., Rani, M., Reddy, D. S., & Krishnaraj, V. (2025, August). Machine Learning-Driven Fault Detection in Electric Vehicles via Hybrid Reinforcement Learning Model. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.
[40] Obermeyer, Z., & Emanuel, E. (2016). Predicting the future—Big data and clinical medicine. Nejm, 375, 1216–1219.
[41] Amistapuram, K. (2025). Generative Ai For Claims Exceptions And Investigations: Enhancing Resolution Efficiency In Complex Insurance Processes. Available At Ssrn 5785482.
[42] Pearl, J. (2009). Causality (2nd ed.). Cambridge University Press.
[43] Srikanth, T., Segireddy, A. R., & Elavarasi, S. A. (2025, October). STaSFormer-SGAD: Semantic Triplet-Aware Spatial Flow-Guided Spatio-Temporal Graph for Anomaly Detection in Surveillance Videos. In 2025 International Conference on Communication, Computer, and Information Technology (IC3IT) (pp. 1-7). IEEE.
[44] Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. NEJM, 380, 1347–1358.
[45] Kolla, S. K. (2021). Architectural Frameworks for Large-Scale Electronic Health Record Data Platforms. Current Research in Public Health, 1(1), 1–19. Retrieved from https://www.scipublications.com/journal/index.php/crph/article/view/1372
[46] Varri, D. B. S. (2024). Adaptive and Autonomous Security Frameworks Using Generative AI for Cloud Ecosystems. Available at SSRN 5774785.
[47] Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
[48] Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30–39.
[49] Yandamuri, U. S. (2023). An Intelligent Analytics Framework Combining Big Data and Machine Learning for Business Forecasting. International Journal Of Finance, 36(6), 682-706.
[50] Sheller, M. J., Reina, G. A., Edwards, B., et al. (2020). Multi-institutional deep learning without sharing patient data. Brainlesion Workshop.
[51] guntupalli, r. (2025). explainable ai in clinical decision support: interpretable neural models for trustworthy healthcare automationexplainable ai in clinical decision support: interpretable neural models for trustworthy healthcare automation. tpm–Testing, Psychometrics, Methodology in Applied Psychology, 32(S9 (2025): Posted 15 December), 462-471.
[52] Shortliffe, E. H., & Sepúlveda, M. J. (2018). Clinical decision support in the era of AI. JAMA, 320(21), 2199–2200.
[53] Rongali, S. K. (2025, August). Deep Learning for Cybersecurity in Healthcare: A Mulesoft-Enabled Approach. In 2025 International Conference on Artificial Intelligence and Machine Vision (AIMV) (pp. 1-6). IEEE.
[54] Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning (2nd ed.). MIT Press.
[55] Siva Hemanth Kolla. (2023). Deep Learning–Driven Retrieval-Augmented Generation for Enterprise ITSM Automation: A Governance-Aligned Large Language Model Architecture. Journal of Computational Analysis and Applications (JoCAAA), 31(4), 2489–2502. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/4774
[56] Tsamados, A., Aggarwal, N., Cowls, J., et al. (2022). The ethics of algorithms. AI & Society, 37, 215–230.
[57] Sasi Kumar Kolla. (2023). Big Data–Driven Machine Learning Frameworks for Clinical Risk Prediction. International Journal of Medical Toxicology and Legal Medicine, 26(3 and 4), 44–59. Retrieved from https://ijmtlm.org/index.php/journal/article/view/1456
[58] Wooldridge, M. (2009). An introduction to multiagent systems (2nd ed.). Wiley.
[59] Bandi, V. D. V. K. (2023). Production-Grade Machine Learning Pipelines For Healthcare Predictive Analytics. South Eastern European Journal of Public Health, 189–205. Retrieved from https://www.seejph.com/index.php/seejph/article/view/7057
[60] Zhang, A., Xing, L., Zou, J., & Wu, J. C. (2022). Shifting ML for healthcare to deployment. Nature Biomedical Engineering, 6, 1330–1345.
[61] Velangani Divya Vardhan Kumar Bandi. (2024). Intelligent Data Platforms For Personalized Retail Analytics At Scale. Metallurgical and Materials

Engineering, 30(4), 1011–1027. Retrieved from https://metall-mater-eng.com/index.php/home/article/view/1011-1027

[62] Benford, S., et al. (2009). Emergent multi-agent architectures. Autonomous Agents and Multi-Agent Systems, 18, 15–45.

[63] Enterprise-Scale Gen AI Orchestration Using Small LMs and LLM Agents for Intelligent ITSM and HRSD Automation in Enterprise Ecosystems. (2025). MSW Management Journal, 35(2), 1889-1897.

[64] Ferber, J. (1999). Multi-agent systems: An introduction. Addison-Wesley.

[65] Garapati, R. S., & Daram, D. S. B. (2025). AI-Enabled Predictive Maintenance Framework For Connected Vehicles Using Cloud-Based Web Interfaces. Available at SSRN 5524261.

[66] Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. Computer, 36(1), 41–50.

[67] Guntupalli, R. (2025). Federated Deep Learning for Predictive Healthcare: A Privacy-Preserving AI Framework on Cloud-Native Infrastructure. Vascular and Endovascular Review, 8(16s), 200-210.

[68] Huhns, M. N., & Singh, M. P. (1998). Readings in agents. Morgan Kaufmann.

[69] Nagabhyru, K. C., & Babu, A. J. Human In The Loop Generative AI: Redefining Collaborative Data Engineering For High Stakes Industries.

[70] Erl, T. (2016). Microservices design patterns. Prentice Hall.

[71] Gottimukkala, V. R. R. (2025). Generative AI for Exceptions and Investigations: Streamlining Resolution Across Global Payment Systems. Journal of International Commercial Law and Technology, 6(1), 969-972.

[72] Fowler, M. (2018). Refactoring (2nd ed.). Addison-Wesley.

[73] Segireddy, A. R. (2025). Generative Ai For Secure Release Engineering In Global Payment Network. Lex Localis: Journal of Local Self-Government, 23.

[74] Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1994). Design patterns. Addison-Wesley.

[75] Varri, D. B. S. V. (2025). Human-AI collaboration in healthcare security.

[76] Rieke, N., Hancox, J., Li, W., et al. (2020). Federated learning for digital health. NPJ Digital Medicine, 3, 119.

[77] Zaharia, M., et al. (2010). Spark: Cluster computing with working sets. HotCloud.

[78] Rongali, S. K., & Varri, D. B. S. (2025). AI in health care threat detection. World Journal of Advanced Research and Reviews, 25(3), 1784-1789.

[79] Lakshman, A., & Malik, P. (2010). Cassandra. ACM SIGOPS Operating Systems Review, 44(2), 35–40.

[80] Nagabhyru, K. C. (2025). Beyond Automation: The 2025 Role of Agentic AI in Autonomous Data Engineering and Adaptive Enterprise Systems.

[81] Stonebraker, M., & Çetintemel, U. (2005). One size fits all? ICDE Proceedings, 2–11.

[82] Yandamuri, U. S. (2022). Big Data Pipelines for Cross-Domain Decision Support: A Cloud-Centric Approach. International Journal of Scientific Research and Modern Technology, 227.

[83] Moreira, M. W. L., et al. (2018). IoT-based smart healthcare systems. Sensors, 18(4), 1155.

[84] Guntupalli, R. (2025). Multi-Cloud vs. Hybrid Cloud Security: Key Challenges and Best Practices. Hybrid Cloud Security: Key Challenges and Best Practices (November 21, 2025).

[85] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. NIST.

[86] Garapati, R. S. (2025). An Intelligent IoT Security System: Cloud-Native Architecture with Real-Time AI Threat Detection and Web Visualization. Journal homepage: https://jmsronline. com, 2(06).

[87] World Health Organization. (2021). Ethics and governance of artificial intelligence for health. WHO Press.

[88] Kolla, S. H. (2024). Retrieval-Augmented Generation With Small Llms For Knowledge-Driven Decision Automation In Enterprise Service Platforms. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 15(3), 476–486. https://doi.org/10.61841/turcomat.v15i3.15497

[89] Moreau, L., et al. (2015). The W3C PROV family of specifications. Future Generation Computer Systems, 29(7), 161–165.

[90] Rongali, S. K. (2025, August). AI-Powered Threat Detection in Healthcare Data. In 2025 International Conference on Artificial Intelligence and Machine Vision (AIMV) (pp. 1-7). IEEE.

[91] Jennings, N. R., & Wooldridge, M. (1998). Applications of intelligent agents. Springer.

[92] Van Roy, P. (2009). Self-management in distributed systems. IEEE Computer, 42(12), 40–47.

[93] Vardhan Kumar Bandi, V. D. (2024). Automated Feature Engineering Systems in Large-Scale Healthcare Data Environments. Journal of Neonatal Surgery, 13(1), 2127–2141. Retrieved from https://www.jneonatalsurg.com/index.php/jns/article/view/10004

[94] Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data. Information Systems Management, 29(4), 258–268.

[95] Pamisetty, A., Paleti, S., Adusupalli, B., Singireddy, J., Inala, R., & Nagabhyru, K. C. (2025, September). Explainable AI Systems for Credit Scoring and Loan Risk Assessment in Digital Banking Platforms. In 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (pp. 1478-1483). IEEE.