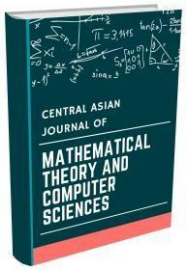

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.casjournal.org/index.php/CAJMTCS

Volume: 07 Issue: 02 | April 2026 ISSN: 2660-5309

Article

Re-engineering Enterprise Systems through Data-Centric Architectures

Ruaa Kadhim Jabir[1], Yasser Samir Hadi[2], Dunea Taleb Kazim[3]

1. Administrative Polytechnic College, Baghdad Middle Technical University
2. Administrative Polytechnic College, Baghdad Middle Technical University
3. Administrative Polytechnic College, Baghdad Middle Technical University

*Correspondence : ruaa-kadhim@mtu.edu.iq, yasser_s@mtu.edu.iq, dunea-taleb@mtu.edu.iq

Abstract: The increasing complexity of enterprise information environments has been increasing the pressure to radically re-engineer the way in which organizations design, govern and operate their data infrastructure. The conventional system design that only considers data as a product of the application logic is becoming less and less able to address the needs of scalability, interoperability, and security of the contemporary digital companies. This paper discusses the paradigm shift in data-centric architectures, including the underlying concepts of data mesh, data fabric, and federated data governance, as well as application in a business and government setting. The analysis is based on the latest research on the topic and official governmental editions to assess the architecture trends, security systems, and modernization policies. Special focus is placed on the concept of Zero Trust data security models, API-based interoperability, the concept of DevSecOps integration, and alignment of enterprise architecture. To help in the analysis, the paper has four comparative tables and six illustrative figures that are given at different points of the text. The results show that the organizations that embrace the principles of data centrism can attain quantifiable improvements in the quality of data, agility in operations, and cyber resiliency. A framework of phased enterprise re-engineering and future research directions are given at the end of the paper.

Keywords: Data-Centric Architecture, Data Mesh, Data Fabric, Zero Trust, Enterprise Systems, Federated Governance, API Interoperability, DevSecOps

Citation: Jabir, R. K. Hadi, Y. S & Kazim, D. T. Re-engineering Enterprise Systems through Data-Centric Architectures. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(2), 285-298

Received: 10th Jan 2026
Revised: 21th Feb 2026
Accepted: 14th Mar 2026
Published: 09th Apr 2026

1. Introduction

The historical design of enterprise information systems is that of application-based models, with data being present to fulfil a set of software functions. The effect of this method is creating siloed repositories, shared datasets, inconsistent semantics and fragile integration patterns that get more and more expensive and risky to maintain over time [1][2][3][4][5][6][7]. These legacy architectures are structural setbacks to digital transformation as organizations expand and increase in complexity. This inability to share, administer, and place trust in data across the organizational boundaries swiftly deteriorates the efficiency of operations and strategic decision-making [8][9][10][11][12]. Data-centric enterprise system re-engineering is an essential inversion of this model: instead of applications executing on data, data execute applications and services are built on well-managed and discoverable data assets and product-oriented data [13][14][15][16].

The driving force behind this change can be seen in the industries [17][18][19]. Companies dealing with big data analytics, machine learning pipelines, and multi-clouds have discovered that big data lakes and warehouses are bottlenecks hindering innovation

in the business world [20]. In the government sector, the government agencies such as the U.S. Department of Defense, NASA, the Intelligence Community, the Department of Homeland Security have all stated clear plans regarding the modernization of their information settings around data-centric principles [21][22]. These plans are an indicator of a common awareness that old IT architectures are prohibitively expensive, insecure, and restrictive to mission [23]. This is particularly a timely topic to be pursued systematically because of the intersection of scholarly study and government policy in the field of data-centric re-engineering [24][25].

The structure of this paper is as follows. Section 2 is a literature review of the theoretical basis of data-centric architectures such as data mesh and data fabrics. Section 3 reviews governance and security models, where the focus is placed on the Zero Trust and federated models. Section 4 examines the implementation patterns within enterprise and government circumstances. Section 5 has a comparative analysis of architectural strategies. Section 6 is on enablers to adoption and barriers to adoption. Section 7 suggests a step-by-step re- engineering model. Section 8 ends with implications to research and practice.

2. Materials and Methods

This investigatory paper follows a qualitative, analytic approach which blends literature review, comparative analysis, and practical framework development to examine the evolution of enterprise systems into data-centric designs. First, a broad review of recent academic studies, industry reports and government policy documents is done to obtain a theoretical basis for key concepts like data mesh, data fabric, federated governance and Zero Trust security models. This review facilitates the identification of existing architectural trends, traditional application-centric system pain points and best practices in modern data management. Next we apply a comparative analysis approach to the systematic comparison of different architectural paradigms comparing the paradigms across multiple dimensions of analysis including scalability, governance, interoperability, and security with organized comparisons and aggregated evidence. Furthermore, real-world deployment patterns from corporate and government sectors are analyzed to study practical approaches for adoption, factors for success, and boundaries. In addition, the study adopts a conceptual modeling perspective to design a progressive enterprise re-engineering plan that consists of key stages including evaluation, small-scale implementation, and full-scale deployment. The methodology focuses on combining the technological, organizational, and policy perspective for a more integrated assessment, and analysis throughout. The upshot is a qualitative synthesis and interpretation of the evidence (rather than empirics), which informs organizational recommendations for becoming more data-driven architectures and to create heightened data governance, system agility, and security resilience.

3. Results and Discussion

Theoretical Foundations of Data-Centric Architectures

From Application-Centric to Data-Centric Design

The technical change in the approach of application-centric to data-centric design is not only a technical whim, but a philosophical redefining of what enterprises think of value creation by information. Application-centric models base data schema, storage formats and access patterns on the needs of each individual software system. This gives rise to the spread of proprietary formats, vendor-locked repositories, and hand-written point-to-point integrations increasing maintenance complexity with each new system being added to the stack. This builds up over decades creating what practitioners refer to as technical debt at the data layer in the form of inconsistent master data and opaque lineage as well as brittle pipelines that fail when any upstream system evolves. The data-centric paradigm reverses these dependencies by considering data as a first-class enterprise resource that has its governance life cycle regardless of the applications that produce or consume data [1].

A data-centric architecture does not have an application module as its basic design unit but a data product. Data products are independent, versioned, discrete packages of data which not only encompass the data itself but also its schema, quality contracts, lineage metadata, access policies and documentation. Such product orientation makes domain teams possess and publish its data assets similarly to how software engineering teams publish reusable APIs and libraries. The data lifecycle and application lifecycle are separated dramatically, and systems are coupled with each other much less than they might be when exposed to ad-hoc extracts. The data mesh and data fabric paradigms both depend on this discipline of architecture that became the most dominant approaches to data re-engineering in an enterprise [3].

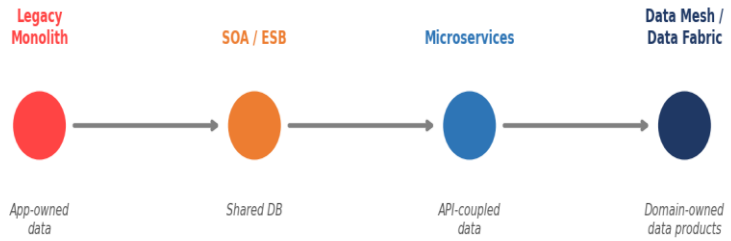

Figure 1. Architecture in the direction of data-centricity.

Data Mesh: Principles and Design Philosophy

The data mesh paradigm relies on four principles decentralization of data ownership by domains, data as a product, self-serve data infrastructure as a platform, and federated computational governance. These guidelines are all aimed at solving the organizational and technical causes of data quality and access failures in big business. Domain ownership realizes that it makes sense to have the teams that are closest to the data, namely those that know its semantics, quality aspects and business context, to govern and publish the same. The data mesh can avoid the organizational bottleneck of centralized data engineering teams that cannot achieve the scale required by an enterprise through the dissemination of ownership to domain teams [2].

The principle of data-as-a-product puts data governance on a par with data design, as a compliance box. Domain teams are not only required to create data but also make it discoverable, addressable, trustworthy, self-describing, interoperable, secure, and valuable. Self-serve infrastructure, such as data ingestion, storage, transformation, cataloging and access control, allows domain teams to achieve this accountability without needing to have extensive familiarity with platform engineering. The enterprise-wide policy enforcement policies, including privacy laws, security classifications, and interoperability standards are enforced using federated computational governance, which does not involve the establishment of a new bottleneck entity, rather than the elimination of the bottleneck that decentralization was meant to eradicate [4].

Table 1. The Fundamentals of Data Mesh and the Classical Data Architecture.

Dimension	Traditional Architecture	Data Mesh Architecture
Ownership Model	Centralized data team	Domain-owned data products
Data Unit	Table / dataset	Data product with SLA
Governance	Top-down, manual	Federated, computational
Infrastructure	Shared monolithic platform	Self-serve domain platform

Integration Pattern	ETL pipelines	API / event-driven interfaces
Scalability	Limited by central team	Scales with domain teams
Data Quality Accountability	Platform team	Domain data product owner
Discoverability	Manual catalog	Automated metadata registry

Data Fabric: Complementary and Contrasting Approaches

Data mesh is a solution to organizational structure and ownership whereas data fabric is a solution to the technology layer that provides a seamless and smart access to data in a heterogeneous environment. A data fabric is a type of architecture that applies metadata management, knowledge graphs and AI-driven automation to provide a unified logical view of information that is dispersed across on-premises systems, across cloud service providers, at the edge and in the partner environment. The data fabric, unlike the data mesh, can be implemented as an overlay of technology on infrastructure already in place, without necessarily changing ownership patterns or team designs. This is why data fabric is especially appealing to businesses that need to enhance their integration in the short term, but do not want to engage in the extensive organizational change that data mesh requires [5].

The connection between data mesh and data fabric is most appropriately seen as complemental and not competitive. The plumbing of data fabric offers the automated data discovery, semantic integration, policy enforcement, and intelligent orchestration to allow data mesh domain teams to meet their product responsibilities in an efficient manner. A business applying data mesh with data fabric no longer owned will see domain teams devote more than proportionate effort to plumbing integration, as opposed to creating data product value. On the other side a data fabric without the organizational discipline of data mesh will tend to recreate the governance failures of centralized architectures regardless of its technical complexity. Both commercial and government environments have the most mature enterprise data architectures, which are likely to incorporate both paradigms, with data fabric serving as the facilitating technology layer in a data mesh organizational model [1].

Governance and Security Frameworks

Federated Data Governance

The model of organizational structure that allows large enterprises to strike a balance between the enterprises benefits influenced by distributed domain ownership and the needs of uniformity of enterprise-wide policies is federated data governance. In a federated structure, the central governing institution defines the policies, standards and accountability structures, which govern all the areas. These policies are then implemented by domain teams into their local context and adjusted to meet domain-specific needs with respect to compliance with enterprise mandates. This form of organization is federated and is reflective of other fields of organizational governance, including financial controls in multinationals or regulatory compliance in federated government agencies [6].

Technical federated governance implementation is based on policy-as-code frameworks, which represent the rules of governance in machine-executable form, where compliance can be verified automatically rather than by manual audit. One important way of operationalizing federated governance at the level of data products is through data contracts, formal arrangements between data producers and consumers of what to include in the schema, what to exclude, what to specify as fresh, and what to specify as out of band. Automated monitoring, alerting and enforcement are possible based on these contracts, thus lessening the burden on governance of domain teams and central oversight bodies. The federated enterprise architecture framework of DoD is one of the notable national-scale instances of this model in the public sector [20].

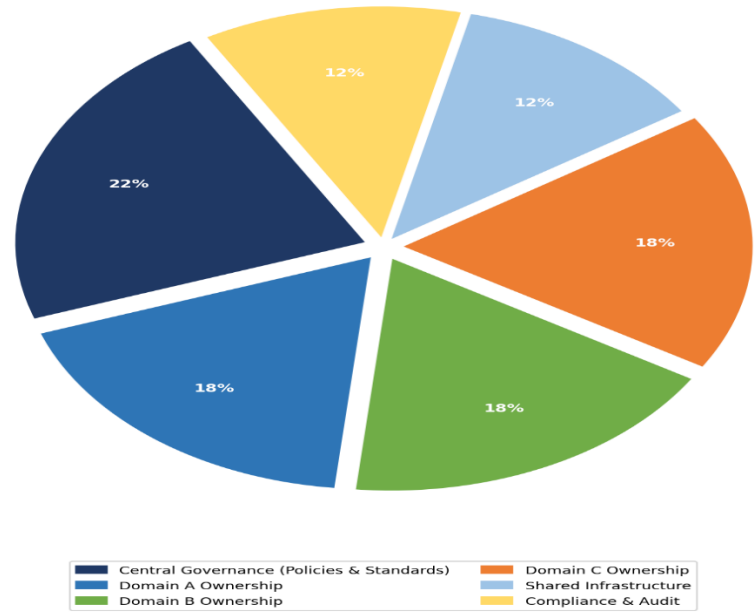

Figure 2. Sharing of the governance roles within enterprise areas.

Zero Trust Data Security

Zero Trust is a security design model that is based on the premise that none of the parties, both external and internal to the network perimeter, want to be trusted by default. Zero Trust in the data-centric architecture context mandates that, all data access requests must be continuously authenticated, authorized, and audited irrespective of the location in the network or network-based identity credential of the requestor. This is a radical change to the perimeter-based security frameworks that provide widespread access to authenticated users in an environment of trust. Zero Trust in the data environment transition implies the use of attribute-based access control, data-level encryption, constant monitoring, and automated responding to threats functionality that, in combination, will ensure that data access is never arbitrary or overly generous [7].

U.S. Department of Defense has defined an elaborate Zero Trust maturity model that is structured into seven pillars having the data pillar at the center of the model. The data pillar consists of data cataloging and classification, data access management, data encryption, data loss prevention, as well as data monitoring and analytics. Further maturity development based on these abilities demands connectivity to identity and access management solutions, security information and event management solutions, and policy enforcement engines. In the case of enterprise systems that are being re-engineered by adopting a data-centric approach, the implementation of Zero Trust principles in the initial architecture design phase is a crucial element of the process in terms of fulfilling the security purpose and operational effectiveness [9].

Table 2. Zero trust maturity levels of the data pillar.

Maturity Level	Characteristics	Key Capabilities
Traditional	Perimeter-based, static controls	Basic access control, manual audit
Initial	Identity-aware access, partial encryption	MFA, data classification initiated
Advanced	ABAC enforced, automated monitoring	Dynamic policy, DLP deployed
Optimal	Continuous adaptive authorization	AI-driven anomaly detection, full encryption

API-Driven Interoperability and Security

The main tool of data-centric architecture is Application Programming Interface where data products reveal their content to authorized consumers. Compared to using a direct database connection or file transfer, APIs offer a versioned, audited, and controlled interface that fulfills access control policies, input validation, and monitoring consumption patterns. Standardized API frameworks such as (RESTful) APIs, GraphQL, and event-driven messaging interfaces allow domain teams to product data products in a discoverable and consumable format by a wide variety of downstream applications without the need to do consumer-specific integration work [11].

The API Reference Architecture of the U.S Department of the Air Force offers a comprehensive roadmap to API-based enterprise integration; one that meets security and interoperability needs. The architecture requires the API gateway to enforce authentication, rate limit, and threat detection as well as allow automated catalog maintenance and lifecycle control on API. In the case of enterprises in the process of data-centric re-engineering, the adoption of a reference architecture of this nature offers a systematic avenue of substituting the conventional point-to-point integrations with controlled and API-mediated data product interfaces. The overall outcome of such a shift is a decrease in the complexity of integration, data freshness, and increased capacity to track and audit data flows throughout the enterprise [11].

Implementation Patterns in Enterprise and Government Contexts

Commercial Enterprise Implementations

The application and use of the concepts of data mesh and data fabric in real-world business settings has been reported by accumulating a mass of case studies and gray literature showing the successes and difficulties of applying these concepts in practice. Financial services, retail, telecommunication, and technology organizations have sought data-centric re-engineering to solve particular pain points such as slowness in the delivery of analytics, low data quality, high integration prices and failure to scale machine learning. In such implementations, the citation of success factors has focused on a powerful executive sponsorship, a definition of domain boundaries, investment in self-serve platform capabilities, and the creation of data product ownership accountability structures consistent with the current organizational hierarchies [4].

The challenges faced in commercial implementations fall in three categories: organization resistance to the distributed ownership model, technical complexity of platform standardization across the current existing systems, and short-term measures and demonstration of the return on investment. The gray literature review by Goedegebuure et al. shows that a number of organizations use hybrid solutions and apply the principles of data mesh only in high-value areas but have centralized architectures in other areas. This practical, staged methodology minimizes the risk of transformation but necessitates close management to ensure new silos do not occur in addition to the already existing ones [3].

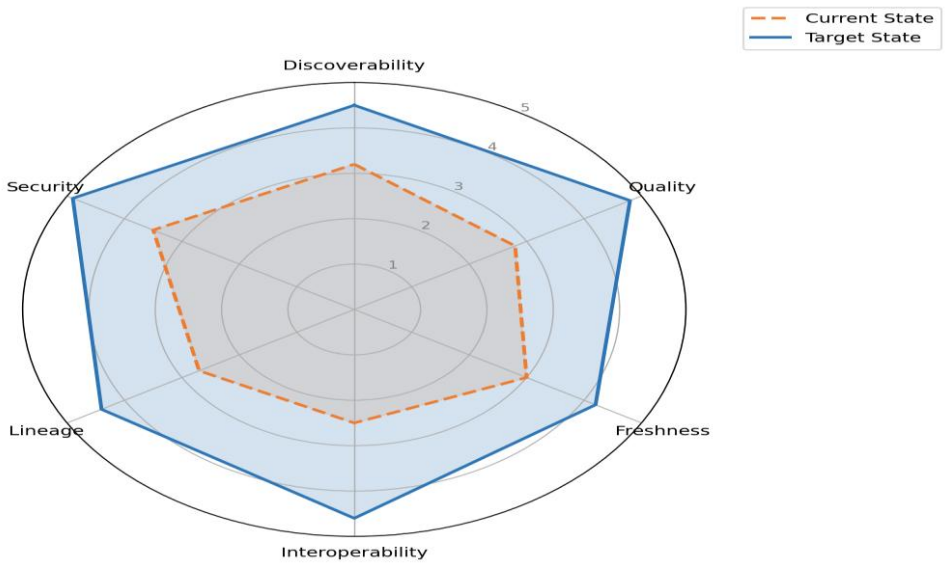

Figure 3. Data product maturity measured on six dimensions.

U.S. Department of Defense Implementation

U.S. Department of Defense is the largest and most complicated public sector enterprise data re-engineering endeavor, constituting hundreds of age-old systems, classified and unclassified information settings, multi-domain functioning necessities, and a need to obtain data excellence in the face of advanced adversaries. The data-centric re-engineering approach of the DoD is expressed in a set of inter-related strategic and architectural documents defining both the vision and the implementation course. The cybersecurity reference architecture serves as the body of the overall security, as the Software modernization implementation plan and the Federated Business Enterprise Architecture framework deal with technology and organizational aspects of change at their respective levels [8].

In the DoD Software Modernization Implementation Plan of FY25-26, the shift to modular, API-first architecture that adheres to the principles of the data mesh is among the priorities. In this plan, a software factory model is built where the data-product-enabled applications developed through DevSecOps pipelines consume and add to a controlled data fabric instead of using privately held data repositories. This is supplemented by the Unified Network Plan 2.0 of the Army, which provides network-layer requirements of data-centric operations which include assured data transport, low-latency edge processing, and resilient connectivity requirements of joint operations [12].

Table 3. Data-Centric Re-engineering Initiatives and Objectives DoD.

Initiative	Lead Organization	Primary Objective	Architecture Pillar
Zero Trust Data Pillar	DoD CIO	Continuous data authorization	Security
Software Mod Plan FY25-26	DoD CIO	Modernize legacy systems	Software
Army Unified Network 2.0	U.S. Army	Resilient data transport	Network
DAF API Reference Architecture	Dept. of Air Force	API-driven interoperability	Integration
Federated BEA Framework	DLA / DoD	Enterprise architecture alignment	Governance
DevSecOps Fundamentals v2.5	DoD CIO	Secure software delivery	Development

Intelligence Community and Other Federal Agencies

The Intelligence Community offers special specifications to data-centric architecture due to the sensitivity of its information resources, the necessity to share data across domains with controlled admission as well as the necessity to integrate information on the resources of different collection capabilities within machine speed. ODNI Vision of the IC Information Environment describes a future whereby data can be discovered, accessed, and utilized between the elements of IC using a common fabric of interoperable services without compromising the compartmentalization and access controls required by mission security. The vision specifically addresses the use of the data product concepts that require the publication of authoritative data sources as discoverable services accessible to authorized analysts across the boundary of components [13].

The IT Strategic Plan 2022-2026 of NASA also shows a data-centric focus, emphasizing the modernization of the scientific data management systems, the introduction of the cloud-native architecture, and the introduction of open data standards that will improve the discoverability and reuse of the data created by the mission. Similar issues in the operational domain are covered by the modernization program of the Department of Homeland Security, which is reported in its 2026 update that is aimed at substituting fragmented case management and intelligence platforms with built-in data-product-focused ones [17].

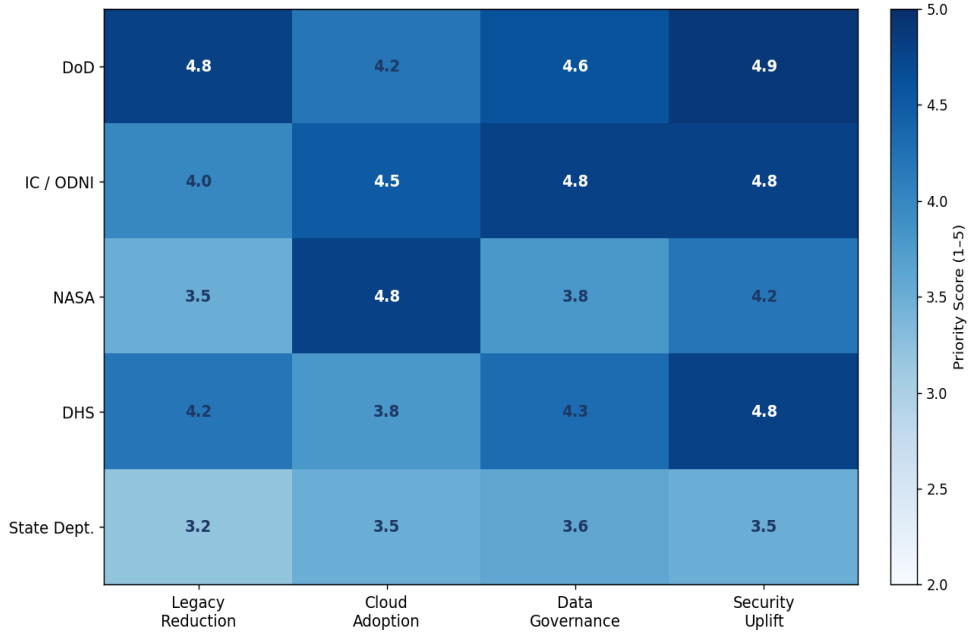

Figure 4. 20242026 data modernization investment priorities, Federal agencies.

Comparative Evaluation of Architectural Approaches

Data Mesh vs. Data Fabric: Dimensions of Comparison

The relative assessment of data mesh and data fabric designs should take into consideration the multi-dimensionality of the enterprise architecture decision-making, including transactional, technical, financial and time aspects. At the organizational dimension, mesh models of data require more radical redesign of organization team duties and accountability designs, whereas data fabrics can be implemented with more relatively small organizational redesign. In the technical aspect, the data fabric needs advanced metadata management, AI-assisted cataloging, and automatic policy enforcement facilities, whereas the technical requirements of data mesh are humbler and can be satisfied with a broader selection of platform options. The financial aspect deals with dissimilar risk profiles: data mesh will be associated with greater initial organizational change expenses but potentially greater long-term scalability advantages whereas data fabric investments in advanced platform technology could provide quicker short-term integration advantages [5].

Both methods have unique advantages when compared to the unique needs of massive government enterprises. Data mesh can fit the federated organizational design of multi-component agencies, in which the domain ownership is directly proportional to the component boundaries. The capability of data fabric to generate logical consolidation of physically dispersed data stores is a solution to the defenses and intelligence environments multi-classification and multi-enclave requirements. Recent literature indicates that the best solution is a conglomeration of the organizational philosophy of data mesh and the technical capabilities of data fabric, which is a hybrid model that can be seen in a number of the government architecture documents examined to conduct this study [6].

Evaluating Re-engineering ROI

The difficulty on quantifying the investment of data-centric re-engineering is a long-standing issue that has gained more and more coverage in scholarly and practitioner publications. The annual IT systems assessment prepared by the GAO gives information on the costs to maintain legacy federal IT systems, with examples being given of legacy system maintenance taking 70-80 percent of the IT budgets and showing decreasing mission value. This establishes a strong economic rationale of change, yet the advantages of data-centric re-engineering are spread over many value dimensions comprising of faster analytics delivery, lower integration expenses, improved data quality, better security posture, and more productive workforce, which are hard to combine into one ROI measure [18].

Commercial data mesh implementations have been studied to provide certain performance improvements such as reduction in time-to-insight in analytics use cases, reduction in data pipeline maintenance effort, and increase in data quality scores as determined by automated data contract verification. These advantages accrue with time as the data products and consuming applications increase because each additional data product can be consumed by all the applications already in force without additional integration cost. The overall cost of ownership of a data-centric architecture therefore has a disparate curve than the application-centric alternatives: greater initial investment in platform and governance infrastructure, and decreasing marginal costs of the addition of new data capabilities as the platform matures [2].

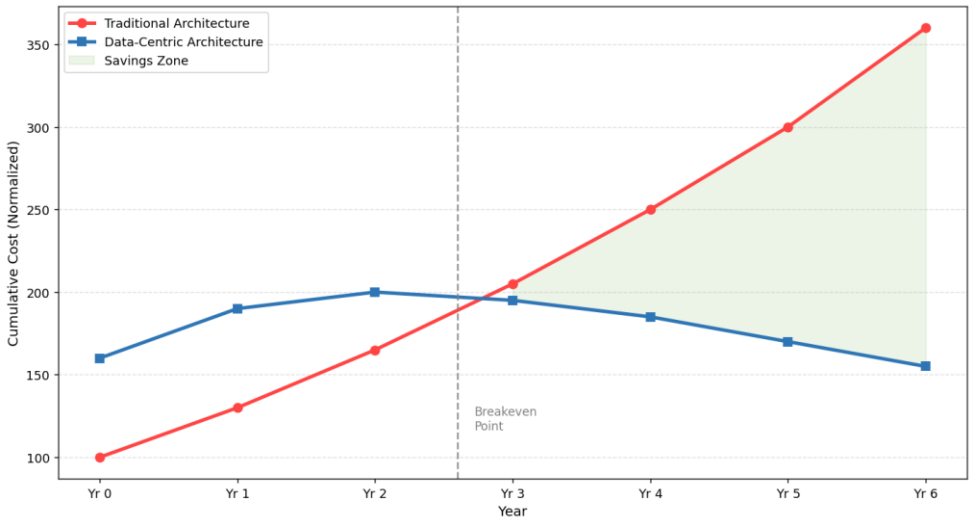

Figure 5. A comparison of total cost of ownership between traditional and data-centric architecture.

Enablers and Barriers to Adoption

Technical Enablers

The infrastructure, platform, and tooling dimensions of technical requirements of successful data-centric re-engineering. Cloud-native environments at the infrastructure tier offer the elasticity, managed services, and worldwide dispersion qualities that allow domain teams to execute autonomously handled information products without having to encumbrance themselves with the physical infrastructure provisioning. Containerization

and orchestration environments, in particular, Kubernetes-based environments, give the stable runtime environment that allows the data product deployment to be cross-portable between cloud providers and on-premises environments, minimizing the risk of vendor lock-in. The enterprise DevSecOps model of the DoD requires the implementation of software factories and hardened container registries, which is a tangible roadmap of the data-centric re-engineering infrastructure layer in government settings [14].

In the platform layer, the presence of fully open-source data management frameworks, such as Apache Kafka to event streaming, apache Iceberg to open tabular formats, dbt to data transformation, and OpenMetadata to data cataloging, has significantly lowered the technical cost of applying the principles of data mesh. Such frameworks offer building blocks of self-serve data infrastructure and do not necessitate enterprises to create their own platforms. The development of AI-based data cataloguing and metadata management software has also increased the viability of data fabric deployments and made the automated identification and categorization of data assets in scales that are otherwise unfeasible through manual curation possible [24].

Organizational and Cultural Barriers

Although enabling technologies are available, organizational and cultural barriers to the adoption of data-centric re-engineering are still the greatest challenges. Switching to the domain-owned data product necessitates a fundamental change in the way the technical teams understand their roles and quantify their achievements. Data engineers that are used to developing centralized pipeline are forced to change their positions as provider of platforms and data product quality assurance. Teams in business domain areas who traditionally relied on centralized data teams need to be held to responsibility in terms of data quality and governance results that they were historically not much in charge of. Such a reallocation of responsibility often is often opposed especially in companies where a tradition of bureaucracy and stringent differentiation of roles is established [4].

In both scholarly and practical literature, leadership alignment and executive sponsorship are continuously being mentioned as the most significant success factors of data-centric transformation. It is unlikely that institutional inertia can be overcome without the visible and sustained effort of the top management to effect the organizational change demanded to realize distributed data ownership models. The Federal Zero Trust Data Security Guide does not ignore this issue, mentioning that policy directives are not enough to bring change and must be supplemented by resource allocation, training, and incentive alignment. The Oregon CTO Biennial Outlook also enumerates organizational culture as the main limitation to modernizing technology in the public sector [15].

Table 4. Enablers and barriers to Data-Centric Re-engineering.

Category	Enablers	Barriers
Technical	Cloud-native infrastructure, open-source platforms, AI-assisted cataloging	Legacy system complexity, data format heterogeneity, security integration gaps
Organizational	Executive sponsorship, domain team empowerment, cross-functional governance	Resistance to distributed ownership, unclear accountability, siloed budgets
Cultural	Data literacy programs, data product mindset, continuous improvement culture	Risk aversion, compliance-over-innovation orientation, limited data skills
Financial	Declining platform costs, measurable ROI frameworks, modernization funding	High upfront investment, uncertain benefits realization timeline, budget cycles

Policy / Regulatory	Zero Trust mandates, open data policies, federal modernization initiatives	Compliance complexity, classification constraints, procurement limitations

A Framework for Phased Enterprise Re-engineering

Phase 1: Foundation and Assessment

Enterprise re-engineering in its initial data-centric phase sets up the organizational/architectural/technical basis on which further transformation operations rely. This stage commences with a detailed data estate analysis that enumerates the available data resources, records their origin, quality and business importance and identifies the business units that produce and consume the data. At the same time, an architectural analysis examines the existing integration environment, determining the most expensive and fragile integration patterns as being the most high-priority targets of re-engineering. The deliverable of this stage is a data estate baseline that gives the empirical basis of transformation planning comprising domain boundary definition, data product candidate identification and platform gap analysis [20].

Another part of the foundation phase involves the creation of the federated system of governance that will guide the transformation. It includes the definition of the mandate of the central governance body, data product ownership accountability model, and policy-as-code framework that will further automatize the compliance enforcement. More importantly, this step has to gain the organizational buy-in to ensure that the change is implemented: the executive support, the multi-year investment authorization in the organizational funds, and the investments in the workforce development to be more data- and platform-engineering-skilled. The success stories of federal agencies that have already implemented successful data-centric changes highlight the fact that governance and organizational preparation are the keys to success as technical planning [13].

Phase 2: Pilot Domain Implementation

The second stage is the translation of architectural vision into operation reality by introducing data-centric principles into few high workload, high visibility pilot areas. The pilot phase should consider the domains of selection based on the areas where the data product ownership advantages are the most apparent, and the domain teams should have the adequate level of technical skills and organizational incentive to effectively work. Banking A combination of high data demand, distinct areas of ownership analysis, and quantifiable outcome measures tends to influence financial reporting, customer analytics, operational logistics, and security operations as the most likely pilot areas in both business and government contexts. The pilot project is a test of concept of the technical platform and as an organizational change management process of showing to the skeptical business stakeholders the worth of the new model [21].

In the pilot stage, self-serve platform infrastructure is launched and developed in reaction to domain group comments. Data product specifications are developed and published based on the data product specification developed during the foundation phase, and the federated governance mechanisms, such as data contracts, quality monitoring and automated policy enforcement, are tested in operational conditions. The experience during the pilot stage drives the design of the scale out plan of the latter stages, what platforms are missing, which governance policies need to be clarified, what the organization is able to do before large-scale adoption, etc. Software factories as a method of DoD usage iterative, capable, validated ability model furnishes a prototype of this pilot-based model [10].

Phase 3: Scale-Out and Continuous Improvement

The third phase applies data-centric architecture concepts to the entire enterprise portfolio, based on the experience of the pilot phase, and a broader range of data products is created that includes all data assets of high value. Scale-out demands the technical maturation of a platform such as automated data product onboarding, self-service metadata management, and AI-assisted data discovery, as well as capacity building of the organization structure among the larger group of domain teams. One of the most problematic aspects at this stage is the consistency and quality of governance because

more data products and areas contribute, and it is necessary to invest in the automated governance tooling and review the federated governance periodically [22].

The data-centric architecture is continually improved through continuous improvement mechanisms integrated into the governance structure to make sure that it allows adjustment to the requirements of the changing missions, emerging threats, and the development of new technology capabilities. Such mechanisms are routinely reviewing the health of data products, automatic quality trend, community of practice forums, which facilitate cross-domain learning, and architecture review boards, which do review the proposed change to platform standards. The appendices of the Federal Zero Trust Data Security Guide give specific implementation advice on the use of some of these mechanisms to the government setting, such as audit frameworks, incident response processes, and ongoing authorization processes [19].

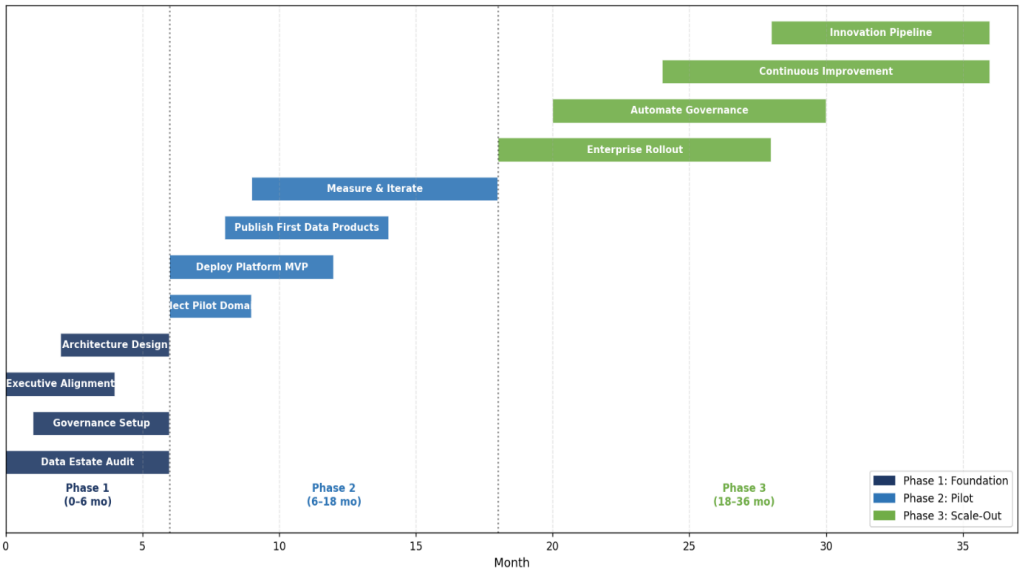

Figure 6. Three steps enterprise re-engineering plan.

Discussion

The review of academic research synthesis and government policy documents in this paper presents a strong and ever-increasing belief that data-centric architecture is the correct basis behind large-scale enterprise system re-engineering. The alignment of the organizational principles of data mesh, the technical features of data fabric and the security model provided by Zero Trust makes a consistent philosophy of architecture that responds to the same governance, interoperability, scalability, and security aspects of data management in an enterprise. This intersection is especially noticeable in the most developed systems of government architecture that more and more mention these concepts in a comprehensive way and not as isolated issues [23].

The data-centric re-engineering is maturing at a very fast pace. Empirical studies have been conducted to report the successes as well as the difficulties in actual implementations of data mesh, following early practitioner assertions of the transformative potential of data mesh. What comes out is a image of such pure though conditional value: data-centric architectures are highly beneficial under conditions such as appropriate implementation and demand organizational and governance investment which most businesses underrate. Although important, the requirements of the technical platform are becoming solvable by increasingly mature commercial and open-source tooling. The more enduring challenge is the organizational change requirements - especially the transition to the distributed data products ownership - especially in bureaucratically structured government enterprises [3].

The growing application of policy requirements by the federal government such as Zero Trust implementation requirements, open data standards, and software modernization requirements, as tools to speed up data-centric transformation, is an

important trend. These requirements generate institutional pressure which complements and at times replaces organic organizational change, and may speed up the adoption process in agencies that would otherwise be more sluggish. Nevertheless, mandate-driven change has its own dangers of compliance theater superficial adoption of terminology and documentation without architectural change that governance structures need to be developed to spot and eliminate [15].

4. Conclusion

The paper has discussed the theoretical, implementation pattern, security structure, and organizational enablement of data-centric enterprise architecture re-engineering. The analysis has shown that the shift towards the data-centric design is both a technological necessity and an organizational problem to be addressed through simultaneous coordinated investments on multiple dimensions. Despite their conceptual difference, data mesh and data fabric are practically complementary structures the use of which meets the entire range of data re-engineering needs of an enterprise. The technical enablers that need to be integrated into the data-centric architecture are zero trust data security, API-based interoperability, and DevSecOps integration; they should be designed into the data-centric architecture, and these features cannot be added post-implementation.

The phased re-engineering model, as suggested in Section 7, offers a systematic framework that enables organizations to journey the process through change and still manage the risk, develop organizational capacity in stages, and bring quantifiable benefits in every phase. The accumulated mass of federal architecture advice can be utilized by government enterprises to guide the transformation strategies thereupon, and in the same vein, the commercial enterprises can tap into the stringent standards of security and governance systems that have been established within the defense and the intelligence community set ups. Future directions in the research involve longitudinal research of the quality of data products in operational settings, empirical research into the usefulness of federated governance, and exploration of AI-enhanced data mesh capabilities that are now emerging both in the scholarly and practitioner communities.

REFERENCES

[1] I. Blohm, C. Lehrer, and T. Bartels, “Data products, data mesh, and data fabric,” Bus. Inf. Syst. Eng., vol. 66, no. 5, pp. 643–652, Oct. 2024, doi: 10.1007/s12599-024-00876-5. https://link.springer.com/article/10.1007/s12599-024-00876-5

[2] I. Kumara et al., “Data Mesh Architecture: From Theory to Practice,” in Proc. IEEE Int. Conf. Serv. Comput. (SCC), 2024, pp. 1–10, doi: 10.1109/SCC62621.2024.00012. https://ieeexplore.ieee.org/document/10628210

[3] A. Goedegebuure, S. Jansen, and S. Brinkkemper, “Data Mesh: A Systematic Gray Literature Review,” ACM Comput. Surv., vol. 57, no. 3, pp. 1–36, Mar. 2024, doi: 10.1145/3687301. https://dl.acm.org/doi/full/10.1145/3687301

[4] J. Bode, M. Henkel, and J. Stirna, “Industry Insights From Data Mesh Implementations,” in Proc. IEEE Int. Conf. Big Data, 2024, pp. 1–8, doi: 10.1109/BigData59044.2024.10565876. https://ieeexplore.ieee.org/document/10565876

[5] S. Parimi, “Data Mesh vs. Data Fabric: The Future of Data Management,” Int. J. Sci. Adv. Inf. Technol., vol. 1, no. 1, pp. 1–23, 2025. https://www.ijsat.org/papers/2025/1/2657.pdf

[6] D. van der Werf, “Towards a Data Mesh Reference Architecture,” in Proc. BI Week Conf., 2024, pp. 1–15. https://conferences.big.tuwien.ac.at/biweek2024/pdfs/biweek2024_paper_164.pdf

[7] NetApp, “Data-Centric Zero Trust,” White Paper WP-7366, Apr. 2025. https://www.netapp.com/media/107740-wp-7366-data-centric-zero-trust.pdf

[8] U.S. Department of Defense, “DoD Cybersecurity Reference Architecture,” Jan. 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

[9] U.S. Department of Defense, “Advancing Zero Trust Maturity Throughout the Data Pillar,” Apr. 2024. https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI_DATA_PILLAR_ZT.PDF

[10] U.S. Department of Defense, “Software Modernization Implementation Plan, FY25-26,” Apr. 2025. https://dodcio.defense.gov/Portals/0/Documents/Library/SW-Mod-I-Plan25-26.pdf

[11] U.S. Department of the Air Force, “DAF API Reference Architecture,” Jul. 2024. https://www.dafcio.af.mil/Portals/64/Documents/Strategy/DAF%20API%20Reference%20Architecture%202.0.pdf

[12] U.S. Department of the Army, "Army Unified Network Plan 2.0," Mar. 2025. https://api.army.mil/e2/c/downloads/2025/03/04/0b7f95c5/army-unified-network-plan-2-0.pdf
[13] U.S. Office of the Director of National Intelligence, "Vision for the IC Information Environment," May 2024. https://www.odni.gov/files/documents/CIO/IC-IT-Roadmap-Vision-For-the-IC-Info-Environment-May2024.pdf
[14] U.S. Department of Defense, "DoD Enterprise DevSecOps Fundamentals v2.5," Oct. 2024. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Fundamentals%20v2.5.pdf
[15] Federal Chief Information Officers Council, "Federal Zero Trust Data Security Guide," Oct. 2024. https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisedMay2025_CIO.govVersion.pdf
[16] U.S. Department of Defense, "DoD Strategic Management Plan FY 2022-2026," Mar. 2023 (updated). https://media.defense.gov/2023/Mar/13/2003178168/-1/-1/1/DOD-STRATEGIC-MGMT-PLAN-2023.PDF
[17] NASA, "NASA IT Strategic Plan FY 2022-2026," 2024. https://www.nasa.gov/wp-content/uploads/2024/01/516011-nasa-it-strategic-plan.pdf?emrc=cd673c
[18] U.S. Government Accountability Office, "IT Systems Annual Assessment," GAO-25-107649, Jun. 2025. https://www.gao.gov/assets/gao-25-107649.pdf
[19] Office of Management and Budget / CISO Council, "Federal Zero Trust Data Security Guide: Appendices," Oct. 2024. https://www.cio.gov/assets/files/Zero-Trust-DataSecurityGuide_Oct24-Appendices-Final.pdf
[20] U.S. Department of Defense, "Federated DoD BEA Framework," Jan. 2024. https://www.dla.mil/Portals/104/Documents/DLMS/Summit/Resources/Federated_BEA_Framework_2024.pdf
[21] U.S. Department of Defense, "Logistics Information Technology Strategy," Feb. 2024. https://www.dla.mil/Portals/104/Documents/DLMS/Summit/Resources/OSD_Logistics_IT_Strategy_2024.pdf
[22] U.S. Department of Defense, "Enterprise SATCOM Management and Control (ESC-MC) Implementation Plan," Jan. 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/ESC-MC-ImplementationPlan.pdf
[23] U.S. Department of State, "Department of State, Foreign Operations, and Related Programs," FY23 Budget Justification, 2022. https://www.cgsnet.org/wp-content/uploads/2022/03/FY23-Budget-Justification.pdf
[24] Oregon Enterprise Information Services, "Chief Technology Officer 2025-2027 Biennial Outlook," Apr. 2025. https://www.oregon.gov/eis/strategy-and-design/Documents/CTO%20Trends%20Outlook%202025-27.pdf
[25] U.S. Department of Homeland Security, "DHS Modernization Update," Mar. 2026. https://www.house.mn.gov/comm/docs/eC69ygMf6EOd1OZF8Jt0Lw.pdf