INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND TECHNOLOGY (IJARET)

ISSN Print: 0976-6480 ISSN Online: 0976-6499

https://iaeme.com/Home/journal/IJARET

High Quality Peer Reviewed Referred Scientific, Engineering & Technology, Medicine and Management International Journals

PUBLISHED BY

IAEME Publication

Plot: 03, Flat- S 1, Poomalai Santosh Pearls Apartment,
Plot No. 10, Vaiko Salai 6th Street, Jai Shankar Nagar, Palavakkam,
Chennai - 600 041, Tamilnadu, India

Email : editor@iaeme.com, iaemedu@gmail.com

www.iaeme.com

International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 16, Issue 3, May-June 2025, pp. 149-164, Article ID: IJARET_16_03_009
Available online at https://iaeme.com/Home/issue/IJARET?Volume=16&Issue=3
ISSN Print: 0976-6480 and ISSN Online: 0976-6499; Journal ID: 1793-4637
Impact Factor (2025): 28.80 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJARET_16_03_009

ARCHITECTING SCALABLE DATA INTEGRATION FRAMEWORKS FOR HYBRID ENTERPRISE PLATFORMS WITH STRONG DATA GOVERNANCE

V Balamuralidhar Sarabu
Data Architect,
Rent A Center, Texas, USA.

ABSTRACT

Modern enterprises increasingly operate within hybrid technology environments that combine on-premises infrastructure, multiple public cloud platforms, Software-as-a-Service (SaaS) applications, and distributed data ecosystems. While this hybrid model provides flexibility and scalability, it also introduces significant challenges in integrating data across heterogeneous systems while maintaining consistent governance, security, and operational reliability. Traditional data integration approaches based on tightly coupled middleware architectures and centralized batch pipelines are often insufficient for handling the scale, velocity, and diversity of modern enterprise data flows.

This paper presents an architectural approach for designing scalable data integration frameworks tailored for hybrid enterprise platforms while embedding strong data governance mechanisms throughout the data lifecycle. The proposed framework emphasizes modular and layered integration architectures that combine API-driven connectivity, event-driven data streaming, distributed data processing

pipelines, and metadata-driven governance controls. These architectural components enable organizations to efficiently integrate data from diverse enterprise systems including transactional platforms, cloud services, analytics environments, and external partner systems.

The study further examines governance strategies such as metadata management, data lineage tracking, policy-based access control, and automated compliance monitoring that ensure transparency, security, and reliability in enterprise data flows. By integrating governance capabilities directly within the integration architecture, organizations can maintain consistent data quality and regulatory compliance while enabling scalable data exchange across distributed systems.

Through conceptual architecture models, integration workflow designs, and governance frameworks, this research outlines practical design principles for building resilient enterprise data integration ecosystems. The proposed approach supports modern enterprise requirements including real-time analytics, AI-driven applications, and cross-platform interoperability, providing a foundation for scalable and governed data integration in hybrid enterprise environments.

Keywords: Hybrid Enterprise Platforms, Data Integration Architecture, Enterprise Data Governance, API-Driven Integration, Event-Driven Architecture, Distributed Data Systems, Cloud Data Integration, Enterprise Data Management

Cite this Article: V Balamuralidhar Sarabu. (2025). Architecting Scalable Data Integration Frameworks for Hybrid Enterprise Platforms with Strong Data Governance. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 16(3), 149-164.

https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_16_ISSUE_3/IJARET_16_03_009.pdf

I. Introduction

The rapid growth of digital technologies has significantly transformed enterprise data ecosystems. Modern organizations operate within hybrid technology environments that combine on-premises infrastructure, cloud platforms, and Software-as-a-Service (SaaS) applications. While these hybrid environments provide flexibility and scalability, they also introduce challenges in integrating and managing data across distributed systems.

Enterprise platforms such as enterprise resource planning systems, customer relationship management platforms, analytics tools, and operational databases generate large volumes of

data that must be exchanged across multiple applications. Without effective data integration frameworks, organizations often face fragmented data environments, inconsistent information flows, and operational inefficiencies caused by isolated data silos.

Traditional integration architectures relied on centralized middleware and tightly coupled system connections. Although these approaches supported structured communication between systems, they often lacked the scalability and flexibility required for modern distributed enterprise platforms. With the expansion of cloud computing and real-time analytics, organizations increasingly require integration architectures that can handle high-volume and real-time data exchange across heterogeneous systems.

Modern integration approaches therefore emphasize API-driven connectivity, event-based messaging architectures, and distributed data processing frameworks. These technologies enable loosely coupled systems that can exchange data efficiently while supporting scalable enterprise operations.

Alongside integration scalability, organizations must also ensure strong data governance. Governance frameworks help maintain data accuracy, security, and compliance by implementing mechanisms such as metadata management, data lineage tracking, access control policies, and regulatory monitoring. Integrating governance capabilities within the data integration architecture ensures that enterprise data remains reliable and compliant throughout its lifecycle.

This paper presents an architectural approach for designing scalable data integration frameworks for hybrid enterprise platforms while embedding strong governance mechanisms. The proposed framework focuses on modular integration layers, distributed processing pipelines, and governance-driven data management to enable reliable and secure data exchange across enterprise systems.

II. Data Integration Challenges in Hybrid Enterprise Environments

Hybrid enterprise platforms introduce multiple complexities in managing and integrating data across distributed systems. Organizations often operate a mix of legacy applications, modern cloud services, analytics platforms, and external partner systems. Each system may store and process data differently, making consistent and scalable integration difficult. As enterprises expand their digital ecosystems, these integration challenges become increasingly significant.

One of the most common issues is the presence of **data silos**. Many enterprise applications operate independently and maintain separate datasets with limited interoperability. When data remains isolated within individual systems, organizations struggle to obtain a unified view of business operations. This fragmentation reduces the effectiveness of analytics initiatives and limits the ability to make data-driven decisions.

Another major challenge is **schema diversity and data transformation**. Different applications often represent similar business entities using different data structures, formats, and naming conventions. For example, customer data stored in a customer relationship management system may use a different schema than data stored in financial systems or analytics platforms. Effective integration frameworks must therefore support flexible data transformation, schema mapping, and normalization processes.

Scalability and performance limitations also affect traditional integration architectures. Legacy integration systems were often designed for periodic batch processing, which may not meet the real-time requirements of modern enterprise applications. Organizations increasingly require integration systems capable of handling high-velocity data streams generated by cloud services, Internet of Things devices, and real-time analytics platforms.

Another important challenge involves **data governance and compliance requirements**. Enterprises must ensure that integrated data adheres to organizational policies and regulatory standards. This includes enforcing access control policies, maintaining data lineage records, and ensuring that sensitive data is properly protected throughout the integration pipeline. Without governance controls embedded in the integration framework, organizations face increased risks related to data misuse and compliance violations.

Additionally, **system interoperability** presents technical difficulties in hybrid environments. Enterprise systems may use different communication protocols, integration standards, and authentication mechanisms. Integration platforms must therefore support diverse connectivity models, including APIs, messaging systems, file transfers, and streaming protocols.

To address these challenges, enterprises require integration architectures that combine scalability, interoperability, and governance capabilities. Designing such frameworks requires a clear understanding of the technical and operational barriers that exist in hybrid enterprise ecosystems.

Table 1. Key Data Integration Challenges in Hybrid Enterprise Platforms

Challenge	Description	Enterprise Impact
Data Silos	Independent systems storing isolated datasets	Limited enterprise-wide insights
Schema Diversity	Different data structures across applications	Increased transformation complexity
Scalability Limitations	Legacy systems designed for batch processing	Difficulty supporting real-time data flows
Governance Gaps	Lack of lineage, policy enforcement, and auditing	Compliance and security risks
System Interoperability	Multiple protocols and data formats across platforms	Complex integration development

III. Layered Architecture for Scalable Data Integration Frameworks

Designing scalable data integration systems for hybrid enterprise environments requires a structured architectural approach that separates integration responsibilities into distinct functional layers. A layered architecture improves modularity, scalability, and maintainability by allowing each layer to address specific integration tasks such as connectivity, data transformation, orchestration, and governance. This approach also enables enterprises to evolve individual architectural components without disrupting the entire integration ecosystem.

The proposed architecture consists of multiple logical layers that collectively manage the flow of data from source systems to enterprise applications, analytics platforms, and storage environments. Each layer performs specialized functions while maintaining interoperability with adjacent layers. This modular design supports integration across heterogeneous platforms including legacy enterprise systems, cloud-based services, and external data providers.

At the foundation of the architecture lies the **source systems layer**, which includes operational databases, enterprise applications, external APIs, and IoT devices that generate enterprise data. These systems often operate independently and produce data in different formats, requiring standardized integration mechanisms to ensure consistent data exchange.

Above the source systems layer is the **data ingestion and integration layer**, responsible for collecting data from diverse sources using mechanisms such as APIs, message queues, file-based transfers, and streaming pipelines. This layer enables both batch and real-time data ingestion while ensuring reliable connectivity across distributed systems.

The **data processing layer** performs critical transformation and validation tasks that prepare data for downstream consumption. Functions such as schema mapping, data

normalization, enrichment, and quality validation are implemented within this layer. Modern integration frameworks often utilize distributed processing engines and stream processing platforms to handle high-volume workloads efficiently.

The **data storage and management layer** provides scalable storage environments for integrated data. These environments may include operational databases, enterprise data warehouses, and data lakes used for analytics and reporting. This layer ensures that integrated data is stored in optimized formats that support efficient retrieval and analysis.

Finally, the **governance and security layer** spans across the entire architecture and ensures that data flows comply with enterprise policies and regulatory requirements. Governance services manage metadata repositories, data lineage tracking, access control policies, and data quality monitoring. Embedding governance controls within the integration architecture improves transparency and ensures accountability across enterprise data pipelines.

By organizing integration capabilities into distinct architectural layers, enterprises can achieve greater scalability and flexibility in managing hybrid data ecosystems. The layered framework also simplifies system upgrades, technology transitions, and platform expansions by isolating changes within specific architectural components.

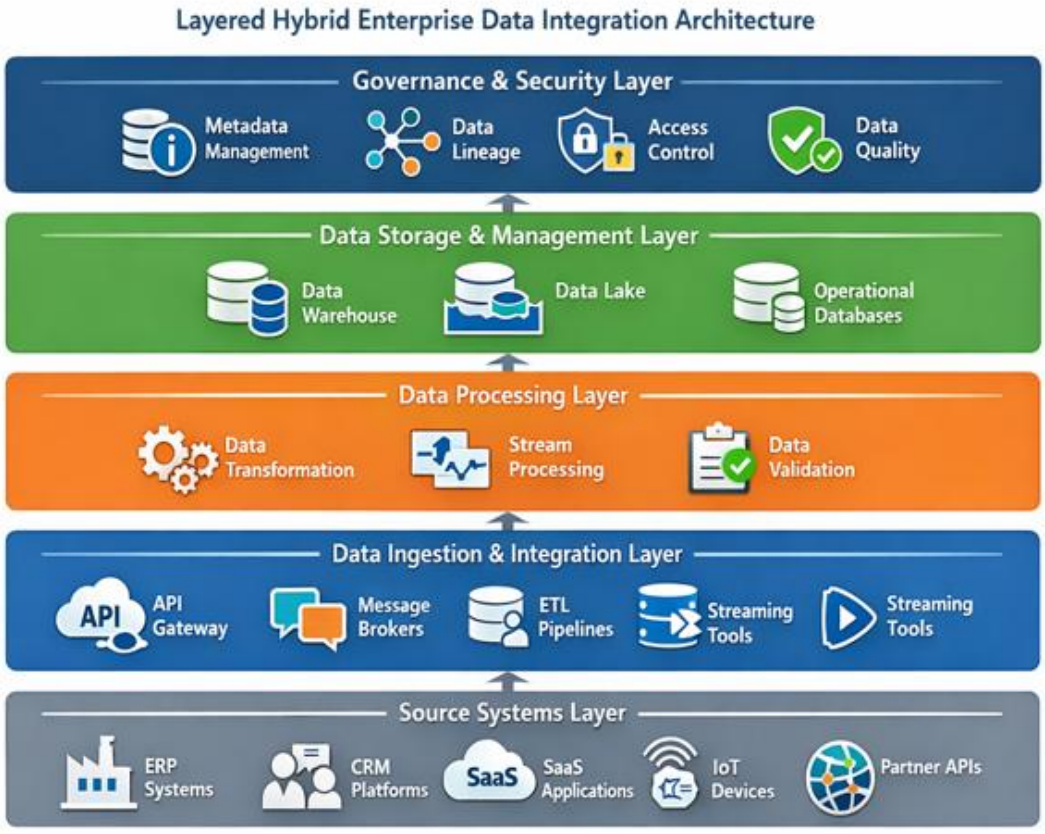

Figure 1. Layered Hybrid Enterprise Data Integration Architecture

Key Architectural Benefits

- Scalability: Independent layers allow horizontal scaling of ingestion and processing components.
- Interoperability: Standardized integration interfaces enable communication across heterogeneous enterprise systems.
- Flexibility: New applications and data sources can be integrated without redesigning the entire architecture.
- Governance Integration: Built-in governance mechanisms ensure consistent policy enforcement and compliance monitoring.
- Operational Resilience: Layer separation reduces system dependencies and improves fault tolerance.

IV. Modern Integration Patterns for Hybrid Enterprise Platforms

As enterprise systems evolve toward distributed and cloud-based infrastructures, traditional integration methods are gradually being replaced by more flexible and scalable integration patterns. Modern data integration frameworks leverage architectural patterns that support real-time communication, loose coupling between services, and scalable data exchange across heterogeneous platforms. These integration patterns allow organizations to efficiently connect enterprise applications, cloud services, analytics platforms, and external partner systems.

One of the most widely adopted approaches is **API-driven integration**. Application Programming Interfaces (APIs) provide standardized interfaces through which systems can securely exchange data and services. API gateways manage authentication, routing, rate limiting, and service orchestration, enabling organizations to create reusable integration services that can be accessed across enterprise platforms. This approach promotes interoperability and simplifies integration development by exposing data services through well-defined interfaces.

Another important pattern is **event-driven architecture**, which enables systems to communicate through asynchronous messaging mechanisms. In event-driven integration, applications generate events whenever specific actions occur, such as a new transaction, system update, or data modification. These events are transmitted through messaging platforms or event brokers where downstream applications can subscribe and respond to relevant events. This model supports real-time processing and reduces tight dependencies between systems.

Data streaming architectures also play a critical role in modern integration frameworks. Streaming technologies allow continuous data flows from operational systems to analytics platforms and data warehouses. Unlike traditional batch processing pipelines, streaming integration enables near real-time data availability, which is essential for applications such as fraud detection, predictive analytics, and operational monitoring.

Another emerging approach is **data virtualization**, which enables unified access to distributed data sources without physically moving or replicating the data. Data virtualization platforms create logical data layers that provide a consolidated view of enterprise data across multiple systems. This approach reduces data duplication while enabling faster access to integrated datasets.

Selecting appropriate integration patterns often depends on enterprise requirements such as latency tolerance, system complexity, data volume, and governance policies. In many cases, hybrid integration models combine multiple patterns including API integration, event streaming, and batch pipelines to support diverse enterprise workloads.

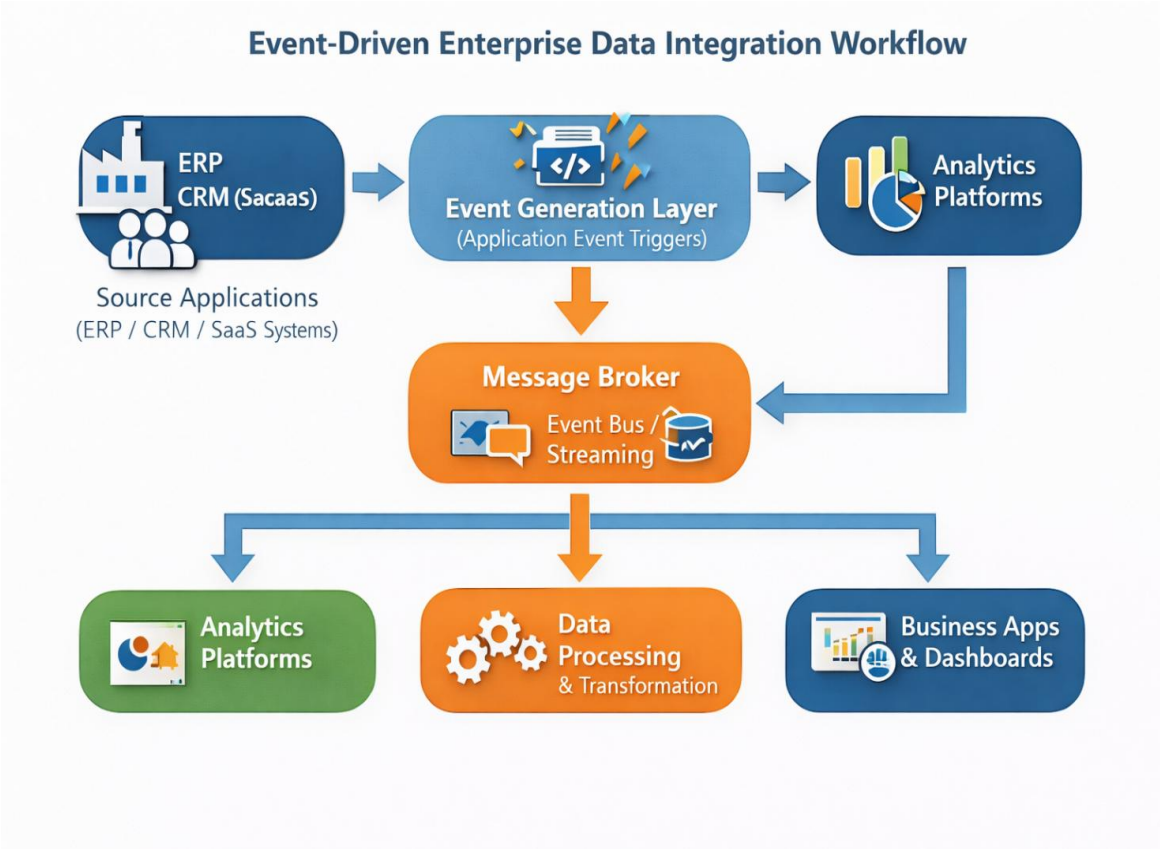

Figure 2. Event-Driven Enterprise Data Integration Workflow

Table 2. Comparison of Modern Enterprise Integration Patterns

Integration Pattern	Key Characteristics	Suitable Use Cases
API-Based Integration	Standardized service interfaces	Application interoperability
Event-Driven Integration	Asynchronous event messaging	Real-time system updates
Data Streaming	Continuous high-volume data flow	Real-time analytics
Data Virtualization	Logical access to distributed data	Unified enterprise data access
Batch ETL Pipelines	Periodic data transformation and loading	Large-scale historical data processing

Modern integration patterns provide the foundation for building scalable enterprise data ecosystems capable of supporting digital transformation initiatives. By combining API-based communication, event-driven messaging, and streaming pipelines, organizations can create flexible integration frameworks that support both real-time and batch data processing across hybrid enterprise environments.

V. Data Governance Framework for Enterprise Data Integration

As enterprise data ecosystems expand across hybrid platforms, implementing strong data governance becomes essential to ensure data reliability, security, and regulatory compliance. Data integration frameworks must not only facilitate efficient data exchange across systems but also maintain strict control over how data is accessed, transformed, and distributed. Without robust governance mechanisms, organizations risk inconsistencies in data quality, unauthorized data access, and compliance violations.

A comprehensive governance framework provides policies, processes, and technological controls that manage enterprise data throughout its lifecycle. Within modern integration architectures, governance capabilities are often embedded directly into integration pipelines to ensure continuous monitoring and enforcement of enterprise policies. This approach enables organizations to maintain visibility into how data moves across systems while ensuring that governance requirements are consistently applied.

One of the fundamental components of enterprise data governance is **metadata management**. Metadata repositories store information about data structures, definitions, ownership, and usage policies. Maintaining centralized metadata catalogs helps organizations

standardize data definitions across applications and simplifies integration development by providing a consistent data reference framework.

Another critical capability is **data lineage tracking**, which records the flow of data as it moves through integration pipelines and enterprise systems. Lineage tracking provides transparency into how data is transformed, aggregated, and consumed across different platforms. This capability is particularly important for auditing, regulatory compliance, and troubleshooting data quality issues.

Data quality management is also a core governance function. Integration frameworks must incorporate validation mechanisms that verify data accuracy, completeness, and consistency before data is delivered to downstream systems. Automated validation rules, anomaly detection mechanisms, and data profiling tools help maintain reliable datasets across enterprise platforms.

Access control and security governance ensure that sensitive data is protected from unauthorized access. Identity and access management mechanisms enforce role-based or attribute-based access policies, ensuring that only authorized users and applications can access specific datasets. Encryption technologies and secure communication protocols further protect data during transmission across distributed systems.

Finally, **policy enforcement and compliance monitoring** ensure that enterprise data practices align with regulatory requirements and internal governance standards. Governance platforms often implement automated compliance monitoring tools that continuously evaluate data usage patterns and flag potential violations.

Embedding these governance capabilities within the data integration architecture enables organizations to create transparent, secure, and well-managed data ecosystems. Such frameworks not only support regulatory compliance but also improve trust in enterprise data assets used for analytics and strategic decision-making.

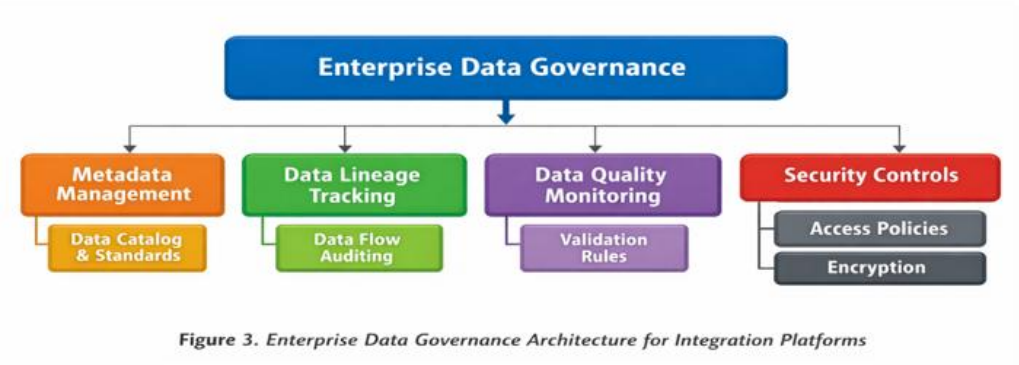

Figure 3. *Enterprise Data Governance Architecture for Integration Platforms*

Figure 3. Enterprise Data Governance Architecture for Integration Platforms

Table 3. Core Components of Enterprise Data Governance

Governance Component	Description	Role in Integration
Metadata Management	Centralized catalog of data definitions	Ensures standardized data interpretation
Data Lineage Tracking	Records data movement and transformations	Supports auditing and transparency
Data Quality Monitoring	Validates accuracy and completeness	Maintains reliable enterprise datasets
Access Control Policies	Restricts data access based on roles	Protects sensitive enterprise data
Compliance Monitoring	Ensures adherence to regulatory policies	Reduces governance and legal risks

Effective governance frameworks play a crucial role in enabling scalable and trustworthy enterprise data integration systems. By combining metadata management, lineage visibility, data quality validation, and security controls, organizations can maintain strong oversight of data flows while supporting complex hybrid enterprise environments.

VI. Operational Considerations for Scalable Integration Platforms

Beyond architectural design and governance frameworks, the operational performance of data integration systems plays a critical role in ensuring reliability and scalability within hybrid enterprise environments. As organizations process increasing volumes of enterprise data, integration platforms must support high availability, fault tolerance, monitoring capabilities, and performance optimization mechanisms. Operational efficiency ensures that integration workflows remain stable and responsive even under heavy workloads and dynamic system conditions.

One of the key operational requirements for enterprise integration platforms is **performance scalability**. Modern enterprises often process large datasets generated from transactional systems, IoT devices, digital platforms, and analytics applications. Integration platforms must therefore support distributed processing models that allow horizontal scaling of ingestion pipelines, transformation engines, and streaming frameworks. Cloud-based integration platforms often implement containerized microservices and distributed computing clusters to handle large-scale workloads efficiently.

Another important operational capability is **system monitoring and observability**. Integration architectures involve multiple distributed components such as APIs, message

brokers, processing engines, and storage platforms. Without proper monitoring mechanisms, identifying failures or performance bottlenecks becomes difficult. Observability platforms collect metrics, logs, and traces from integration components to provide centralized visibility into system behavior. Monitoring dashboards allow administrators to track data flow status, processing latency, error rates, and system resource utilization.

Fault tolerance and reliability mechanisms are also essential for maintaining continuous data flows across enterprise systems. Integration pipelines must implement error handling strategies such as message retries, checkpointing, dead-letter queues, and automatic recovery processes. These mechanisms prevent data loss and ensure that temporary failures do not disrupt critical enterprise workflows.

Another operational aspect is **workflow orchestration and scheduling**. Enterprise integration pipelines often involve complex sequences of tasks including data extraction, transformation, validation, and loading operations. Workflow orchestration platforms coordinate these tasks and manage dependencies between integration jobs. Automated scheduling ensures that batch processes and periodic data synchronization tasks are executed at the appropriate times.

Additionally, **security monitoring and operational governance** must be integrated into operational management practices. Security monitoring tools track unusual data access patterns, unauthorized integration requests, and potential security breaches within integration pipelines. These mechanisms strengthen overall enterprise data protection and support regulatory compliance initiatives.

By implementing strong operational management practices, organizations can ensure that their data integration platforms remain reliable, scalable, and secure. Operational observability, automated recovery mechanisms, and performance monitoring collectively enable enterprises to maintain consistent data flows across complex hybrid infrastructure environments.

Table 4. Operational Capabilities for Scalable Integration Platforms

Operational Capability	Description	Enterprise Benefit
Distributed Processing	Scalable computing resources for data processing	Handles high-volume workloads
Monitoring and Observability	Real-time tracking of integration performance	Faster issue detection
Fault Tolerance	Automatic recovery and retry mechanisms	Prevents data loss
Workflow Orchestration	Automated coordination of integration tasks	Improves operational efficiency
Security Monitoring	Detection of abnormal data access patterns	Strengthens data protection

VII. Security and Risk Management in Hybrid Data Integration

As enterprise data flows expand across hybrid platforms, ensuring strong security and risk management becomes a fundamental requirement for integration architectures. Data integration frameworks often process sensitive information originating from enterprise applications, financial systems, customer platforms, and external partner networks. Without adequate security mechanisms, organizations face risks such as data breaches, unauthorized access, and regulatory violations.

One of the most important security requirements in hybrid integration environments is **data protection during transmission and storage**. Data exchanged between distributed systems must be secured using encryption protocols to prevent interception or unauthorized modification. Transport-layer encryption ensures secure communication between integration components such as APIs, message brokers, and data processing services. Similarly, data stored within enterprise repositories must be protected using encryption mechanisms that safeguard sensitive information.

Another key aspect of integration security involves **identity and access management**. Enterprise integration platforms often connect numerous systems, services, and user applications. Access control frameworks enforce authentication and authorization policies that ensure only authorized users and systems can access specific datasets or integration services. Role-based access control and policy-driven authorization models help maintain strict security boundaries across enterprise platforms.

API security also plays a critical role in modern integration architectures. APIs serve as primary interfaces for data exchange across distributed applications, making them potential targets for cyber threats. Secure API gateways enforce authentication mechanisms, rate limiting policies, and traffic monitoring capabilities to protect integration endpoints from unauthorized requests and malicious attacks.

Another important consideration is **risk monitoring and incident response**. Security monitoring tools analyze integration logs, system events, and network traffic patterns to detect unusual activity that may indicate security threats. Automated alerting systems notify administrators when suspicious behaviors occur, enabling rapid response and mitigation actions.

Organizations must also address **compliance and regulatory requirements** when designing integration security strategies. Many industries require strict control over how data is stored, accessed, and shared. Compliance frameworks require organizations to maintain audit

trails, enforce data access policies, and implement governance mechanisms that ensure transparency in data handling practices.

By integrating these security mechanisms into enterprise integration architectures, organizations can build resilient systems capable of protecting sensitive data while supporting scalable hybrid data flows. Security-driven integration design not only protects enterprise assets but also strengthens trust in enterprise data ecosystems.

Table 5. Security Controls in Enterprise Integration Frameworks

Security Mechanism	Description	Risk Mitigated
Data Encryption	Protects data in transit and at rest	Prevents data interception
Identity and Access Management	Authenticates users and systems	Unauthorized access
API Security	Protects integration endpoints	API abuse and attacks
Security Monitoring	Detects suspicious activity	Early threat detection
Compliance Enforcement	Ensures regulatory adherence	Legal and compliance risks

VIII. Conclusion

The increasing adoption of hybrid enterprise platforms has significantly expanded the complexity of enterprise data ecosystems. Organizations now operate across distributed infrastructures that combine on-premises systems, cloud platforms, and SaaS applications. Within such environments, scalable and reliable data integration frameworks are essential for enabling seamless data exchange across heterogeneous systems while maintaining governance, security, and operational reliability.

This paper presented a comprehensive architectural approach for designing scalable data integration frameworks tailored for hybrid enterprise platforms. The study explored layered integration architectures that separate ingestion, processing, storage, and governance functions to improve scalability and system maintainability. Modern integration patterns such as API-driven connectivity, event-driven messaging, streaming data pipelines, and data virtualization were examined as key mechanisms for enabling flexible enterprise data exchange.

The research also emphasized the critical role of data governance in maintaining data reliability and compliance within distributed integration ecosystems. Governance capabilities including metadata management, data lineage tracking, data quality monitoring, and policy-based access control were identified as essential components of enterprise data management frameworks.

Operational considerations such as monitoring, observability, fault tolerance, and workflow orchestration were further discussed to ensure that integration platforms remain resilient under large-scale workloads. In addition, the paper highlighted the importance of security mechanisms including encryption, identity management, API protection, and compliance monitoring to safeguard enterprise data assets.

As organizations continue to expand digital transformation initiatives and adopt advanced analytics and artificial intelligence technologies, enterprise data integration architectures must evolve to support increasingly dynamic data ecosystems. Future integration platforms are expected to incorporate intelligent automation, AI-driven governance systems, and adaptive integration pipelines capable of responding to changing enterprise data requirements.

By combining scalable integration architectures with strong governance and security controls, enterprises can build resilient data ecosystems that support innovation, operational efficiency, and data-driven decision-making across hybrid technology environments.

References

[1] S. VimalRaj, "Redesigning Modern Data Architecture for Autonomous Data Pipelines and Multi-Model Governance in Enterprise Environments," International Journal of Information Technology Research and Development, vol. 6, no. 3, pp. 37-41, 2025.

[2] J. W. Sajja, G. B. Komarina, and N. K. R. Choppa, "Enterprise Data Transformation in the Era of S/4HANA: Cloud Migration Architecture and Governance Strategies," World Journal of Advanced Research and Reviews, 2025.

[3] S. Chilakala, "Enterprise Data Architectures: A Comprehensive Analysis of Modern Solutions and Implementation Frameworks," International Journal of Research in Computer Applications and Information Technology, 2025.

[4] N. Vasipally, "Enterprise Integration in the Digital Age: A Framework for Oracle SOA Suite and Microservices Convergence," International Journal of Computer Engineering and Technology, 2025.

[5] N. Edulakanti, "From Data Silos to Smart Integrations: A Framework for Enterprise-Wide Interoperability Using APIs, HL7, and JSON," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, 2024.

[6] W. Liu et al., "Research Trends in Security Governance of Data-Entity Integration in the Digital Economy," IFAC-PapersOnLine, vol. 59, no. 35, pp. 637-642, 2025.

[7] A. Ettinger, "Enterprise Architecture as a Dynamic Capability for Scalable and Sustainable Generative AI Adoption," arXiv preprint, 2025.

[8] E. Kandogan et al., "Orchestrating Agents and Data for Enterprise: A Blueprint Architecture for Compound AI Systems," arXiv preprint, 2025.

[9] A. M. Kirubakaran et al., "Governing Cloud Data Pipelines with Agentic AI," arXiv preprint, 2025.

[10] S. B. V. Vedat et al., "RAG-Driven Data Quality Governance for Enterprise ERP Systems," arXiv preprint, 2025.

Citation: V Balamuralidhar Sarabu. (2025). Architecting Scalable Data Integration Frameworks for Hybrid Enterprise Platforms with Strong Data Governance. International Journal of Advanced Research in Engineering and Technology (IJARET), 16(3), 149-164.

Abstract Link: https://iaeme.com/Home/article_id/IJARET_16_03_009

Article Link: https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_16_ISSUE_3/IJARET_16_03_009.pdf

✉ **editor@iaeme.com**