Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Best Practices for Enterprise System Integration in Modern Organizations

Pavan Kumar Adabala
Independent Researcher, USA

ARTICLE INFO

Received: 05 March 2026

Accepted: 08 March 2026

ABSTRACT

Enterprise system integration represents a critical capability for modern organizations seeking to maintain operational efficiency and competitive advantage in increasingly complex technological landscapes. This comprehensive guide examines the multifaceted challenges and strategic approaches required for successful integration of diverse business applications, legacy systems, and emerging Internet of Things data streams. The article addresses fundamental integration challenges, including data standardization, schema evolution, security vulnerabilities, and the transition from batch-oriented processing to real-time analytics capabilities. Through articles on contemporary integration architectures such as data lakehouses, the work demonstrates how organizations can balance the scalability requirements of modern data volumes with the transactional consistency demanded by enterprise operations. The guide emphasizes the necessity of thorough strategic planning, robust data governance frameworks, and comprehensive security architectures that protect integrated systems while enabling necessary information exchange. Particular attention is devoted to the integration of sensor data from Internet of Things devices with traditional enterprise resource planning systems, highlighting the technical and organizational complexities inherent in bridging operational technology with information technology domains. The article presented encompasses phased deployment strategies, rigorous testing protocols, continuous monitoring frameworks, and the implementation of advanced intrusion detection systems capable of identifying and mitigating sophisticated cyber threats. By synthesizing best practices from manufacturing, smart city deployments, and enterprise analytics implementations, this article provides actionable guidance for organizations navigating the technical, security, and governance challenges of contemporary system integration initiatives.

Keywords: Enterprise System Integration, Data Lakehouse Architecture, Internet Of Things Security, Intrusion Detection Systems, Data Governance Frameworks

1. Introduction

Core business applications must communicate with each other, sensors, and data sources in order to keep the modern enterprise synchronized. As an enterprise's IT landscape expands, integrations allow sales, inventory, financial, and production functions to work to the same cadence and maintain a similar direction. These integration landscapes are complicated by the choice of manufacturers' applications and the need to integrate data from legacy enterprise resource planning systems with real-time streams of sensor data from the internet of things to support advanced analytics and operational intelligence [1]. Without integration capabilities that connect the silos of enterprise information, companies will not be able to create efficiencies, eliminate inconsistencies, and support automation. Such isolation forces employees to duplicate data entry, manually manage anomalies, and work without visibility into cross-functional business processes that span multiple operational domains.

The issue is not whether to integrate systems, but how best to do it. Without a methodology, data quality problems, security issues, and resistance from users make the implementation of integration

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

projects very difficult. Integration architectures must also deal with schema evolution (i.e., data format evolution due to changing business requirements) and possibly support batch processing for analyzing historical data, as well as stream processing for time-critical business decisions [1]. Data standardization and data mapping requirements also support many integration failures. For example, different systems may use different data formats, structural conventions, and application programming interfaces that are not natively compatible and require detailed mapping and validation to avoid loss, duplication, or corruption during transfer. Studies of routing data with sensor streams show that standard data models and reliable transformation pipelines are prerequisites to correlating planned activities with the recording of operations in connected systems [1]. Security is essential for the success of integration that normally requires authentication, access management, and encryption protocols to protect operational and financial data exchanged between systems and interfaces from unauthorized access [2].

This article is a complete guide to enterprise system integration, with practical advice on assuring data quality, the security of operations, and enterprise readiness. The concepts apply in manufacturing, logistics, retailing, and any situation where business information systems must connect to a collection of external information systems. In manufacturing, the integration of enterprise planning software with sensors in the workshop enables near real-time visibility into production status, quality metrics, and the condition of manufacturing assets. This allows managers to detect deviations from the planned production and respond to them in a timely manner before they develop into major issues. Modern data architectures for this use case are lakehouse architectures, which combine the scalability of data lakes with the transactional consistency provided by data warehouses [1]. Lakehouse architectures enable the address of challenges such as schema evolution, to avoid breaking existing integrations, and data quality, by enforcing data quality rules during data ingestion. The following sections detail these practices, which may be used as a guide for organizations that are attempting to grapple with aspects of integration that are currently complex, such as security requirements, data governance, and workforce readiness to change workflows [2]. This article proposes the Enterprise Integration Maturity Model (EIMM), a five-level framework that guides organizations from siloed operations to fully governed, real-time integrated ecosystems. Each subsequent section addresses a distinct maturity dimension.

2. Strategic Planning and Needs Assessment

Enterprise application integration success depends on thorough assessment and planning, which lays down the technical and organizational foundation for linking enterprise applications. Data structures, formats, and interfaces of each enterprise application are designed according to various philosophies, approaches of vendors, and regimes of evolution of the systems. These functional and non-functional requirements should be identified from the outset in order to prevent data issues, financial wastage through duplication and unnecessary connections, and the inability to make decisions based on analytics. A clear understanding of the business objectives for the integration, the system capabilities for each system and how they fit in the integrated system, the required data flow, and the cross-functional expectations must be defined. Likewise, integrating Internet of Things data using customary Extract-Transform-Load integration patterns can be a challenge as high-volume sensor data is integrated with enterprise systems that were designed to work with batch-oriented approaches. This is especially true when data quality and data consistency must be maintained across the entire transformation pipeline. Experts in the field have predicted that the number of smart and Internet of Things devices will exceed thirty million by 2025 compared with 10.3 million non-Internet of Things devices [3][4]. Documentation is also needed to link data schemas to field-level links between applications as well as application programming interfaces (APIs) or file exchanges used to connect to other applications.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

An integration plan that is fully thorough will include the boundaries of what will and will not be included in the integration project, how long the project will take, the resource allocations, and the data mapping specifications. The timeline defines the sequence of integration activities to ease risk and resource management. Resource allocations identify technical and business domain experts that will work within each workstream. Data mapping defines how the data elements in source systems map to the structures of the target system, including unit conversions, code translations, aggregation, and enrichment. This includes field correspondence specifications that describe how fields on sending systems match to fields on receiving systems, as well as the transformations that must be performed where such direct matching is not possible due to structural differences or business rules [3]. Data validation at integration points should ensure completeness, validate against range and referential integrity of related records, and flag deviations so that human users have the opportunity to confirm that corruption is not being transmitted to downstream integrations. Extract-Transform-Load (ETL) methods should accommodate data flows from IoT sensors and also ease transformations to move the data from sensor measurements to business-relevant metrics suitable for enterprise decision support and operational dashboards. [3]

Testing and operational processes of the system should be defined and documented during development, not during post-hoc planning when a problem is encountered with a deployed integration. Typically, testing entails unit tests for small pieces of transformation logic processing, integration tests for end-to-end patterns across source systems and targets, performance tests for throughput during peak processing times, and user acceptance testing by business users of workflows when they are in normal operation. The maintenance plan defines how to monitor the health of the integration, how to manage and react to errors or failures, how to manage versioning changes in the source or target applications, and how to manage schema evolution of the integration as business needs force schema changes in one or more integrated applications. Documenting the maintenance plan promotes concurrence between technical implementation teams, stakeholders in the business, and other affected parties on what to expect and when to expect it and diminishes cost overruns during scope-uncertain periods and resource misallocations. Security and compliance considerations must be included in the design along with other aspects such as authentication methods, encryption, access control, and audit logging, which are required to protect sensitive data as it moves along the integration paths between the systems. Home IoT devices have been discovered to contain more vulnerabilities than commercial or industrial IoT devices. For correctly implemented systems, intrusion detection and prevention systems have been reported to detect ninety-five percent of malicious attack packets; two other systems detected fifty-eight percent and seventy-one percent of attack packets. Further, the detection systems of denial-of-service attacks could predict the attacks with an average of 95.81 percent accuracy, whereas the brute-force attack detection systems could predict the attacks with an accuracy of 99.32 percent on a number of authentication attempts via network protocols [4].

EIMM Level	Stage Name	Key Characteristics
1	Ad Hoc	No formal integration plan, siloed data
2	Defined	Documented data mappings, scoped timelines
3	Governed	Standardized schemas, data quality rules enforced
4	Optimized	Real-time streaming, IoT integration active
5	Intelligent	ML-driven monitoring, predictive governance

Table 1: Enterprise Integration Maturity Model (EIMM) Levels and Characteristics [3, 4]

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

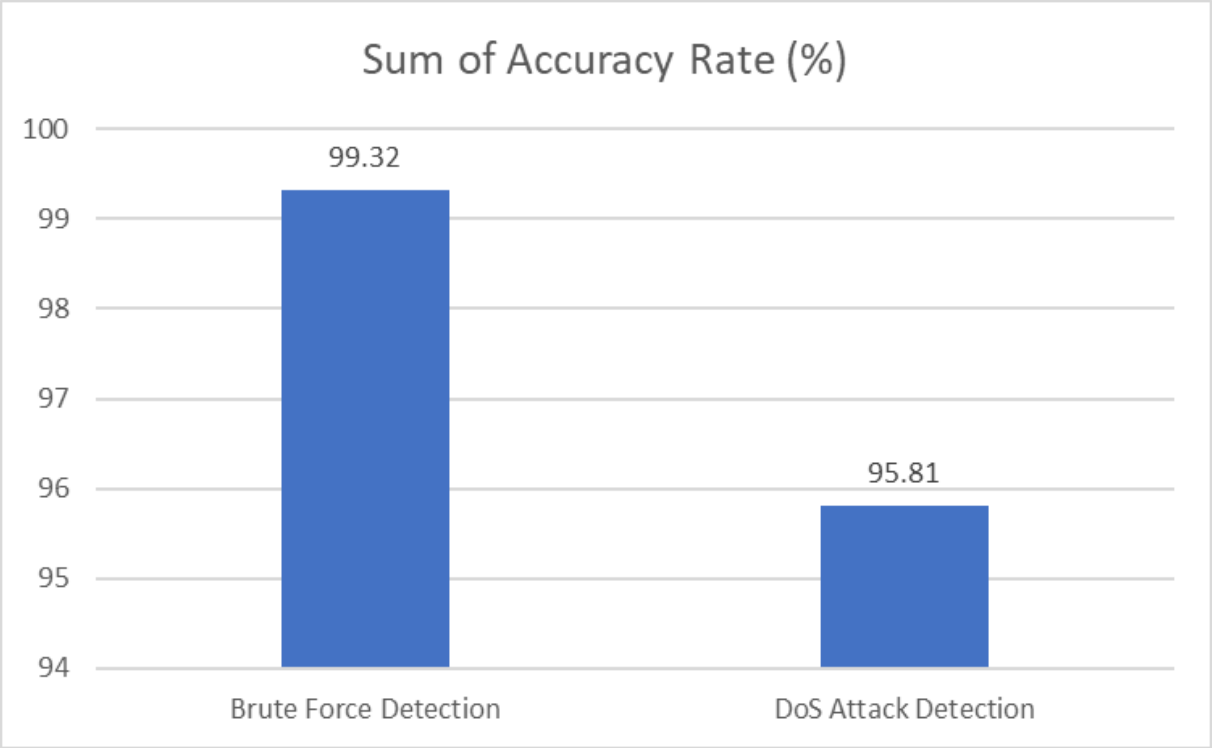

Fig. 1: Security Detection Performance in IoT Integration Environments [3, 4]

3. Data Governance and Standardization

Successful integration requires good assessment and planning, leading to an appropriate technical and organizational architecture. The situation is complicated in an enterprise environment, where applications often work with different data structures, formats, and interfaces due to different design trends, vendor policies, and the age of the systems. However, the technical characteristics of the integrations need to be inventoried before attempting to connect them. Neglecting to identify the technical aspects of integrations is a sure way to lose and duplicate data and destroy the reliability of analysis and decision-making. An organized evaluation is required, looking at the business reason for the application integration: business goals, systems capabilities and their contribution to the integrated system, requirements to transfer data from one application to another, and expectations and success criteria for the application integration per functional area. The inclusion of Internet of Things data into ETL workflows is complicated by the rapid streaming nature of the sensor feeds, the need for them to fit into ETL batch processing methodologies used by enterprise data processing systems, and the complexity of maintaining data integrity at every stage of the ETL devices and process [3]. By 2025, there could be more than thirty million smart and Internet of Things devices and 10.3 million devices that are not Internet of Things [4]. It should map the existing data schemas, describe field-level relationships between systems, and list the available application programming interfaces or file exchange methods for connecting the systems.

From this analysis, a detailed plan will be developed, including the boundaries of the scope, timeframes for implementation, resource allocations, and details of the data mapping. Scope boundaries define the systems and processes that the integration project includes. Sequencing the integration activities into an implementation timeline helps reduce risk and address resource constraints. Resource allocations provide technical and subject matter experts to the integration workstreams. Data mapping specifications describe how the data elements map from the source

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

systems to the target systems and how the data elements will be transformed, including unit conversions, code translations, aggregations, and enrichment. A field correspondence specification defines how fields in the sending system are mapped to fields in the receiving system. This is not always a direct field-to-field mapping; there may be structural or business differences between the two systems [3]. Validation of the data at the integration point is also necessary to check for completeness, limit value ranges, perform referential integrity checks, and notify human operators of problems before corrupted data propagates downstream. Extract-Transform-Load (ETL) for the Internet of Things needs to handle streaming data from sensors and apply transformation logic to use raw sensor data in enterprise analytics and operational dashboards to calculate business-relevant metrics [3].

Testing and monitoring strategies should be established from the beginning, rather than after dependencies have been discovered on a buggy integrated deployment. Test strategies should consist of unit tests on the logic of the individual transformation pieces, integration tests that ensure that flows of data across system boundaries are valid, performance tests that ensure sufficient throughput during peak processing times, and user acceptance tests that ensure business users can use the complete workflow as intended. Maintenance plans generally include error detection and recovery, updates to integrations when source or target systems are upgraded to new versions, and updates to schemas when business requirements dictate changes in application structure. Communicating the maintenance plan across the organization reduces the risk that the integration development teams become divorced from business requirements. It ensures that all stakeholders know to expect schema changes and what to do when they arrive, without unnecessary scope creep or budget overruns. Security and compliance requirements can be defined as part of the planning process. Security consideration provides for authentication, encryption, role-based access control, logging, and other measures to protect sensitive data as it traverses integration links between systems. Research has shown that the security posture of home Internet of Things devices is weaker than industrial or enterprise devices, but correctly deployed intrusion detection and prevention systems are capable of capturing and identifying ninety-five percent of packets sent as part of malicious attacks in laboratory tests, compared to fifty-eight and seventy-one percent from alternatives in laboratory tests. Denial-of-service attack detection systems achieve 95.81 percent detection rates across multiple attacks, and brute-force attack detection systems achieve 99.32 percent accuracy in detecting and identifying brute-force attacks based on authentication attempts and network protocol traffic analysis.

Data Governance Standardization Layer (DGSL)

Schema Registry—centralized management of data formats across systems

Validation Gateway—enforces completeness, range, and referential integrity at ingestion

ETL Harmonization Engine—transforms raw IoT sensor streams into enterprise-ready metrics

Security Detection Category	Attack Type	Detection Method	Accuracy Rate (%)	Performance Classification	Monitoring Scope
DoS Attack Detection	Denial of Service	Specialized Detection System	95.81	Highly Consistent	Multiple attack iterations
Authentication Attack Detection	Brute Force Attempts	Protocol-level Monitor	99.32	Exceptional	Cross-protocol monitoring

Table 2: Security Detection Performance Comparison for IoT Integration Environments [3, 4]

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. Security Architecture and Compliance Controls

Integration projects can create another attack surface, as vulnerabilities in one integrated application can affect other applications through the integration points. Security architecture is another factor that organizations should consider during integration projects. The organization should assess the security of any system participating in its integration ecosystem, along with the controls that will be put in place to minimize exposure while still allowing information exchange. As the Internet of Things develops in a smart city environment, it is estimated that the number of smart and IoT devices will exceed non-IoT devices by 2025 (30 million vs. 10.3 million), creating a wide attack surface. The growth of IoT endpoints has increased over the threefold increase of networked devices, posing a challenge to the protection of smart city ecosystems. Manufacturing systems also face the challenge of integrating bill of materials, routing data, and serialization data into a single data lakehouse model that provides both the benefits of open access and protection against unauthorized access and data alteration [5].

Access control mechanisms should adopt least-privilege principles. This principle implies granting users and applications the permissions needed to perform their tasks, and nothing else. Data can be protected from unauthorized access via encryption. Authentication checks the identity of systems and users. Network segmentation contains integration points, reducing risks. Intrusion detection systems inspect network traffic for signatures, anomalies, flags, and behaviors that could indicate an intrusion. When configured with machine learning algorithms using a large dataset of attacks, intrusion detection and prevention systems (IDPS) have been shown to be able to achieve over ninety-nine percent identification of certain attacks [6]. Models were evaluated on standard datasets and random forest classifiers and decision tree models produced overall perfect one hundred percent accuracy in binary classification tasks compared with the customary state of the art [6]. The logistic regression model had an overall accuracy of about 89.4 percent with a sensitivity of 99.6 percent. The support vector machine classifiers were found to have an overall accuracy of eighty-six percent when identifying its binary classification [6]. When identifying a number of different attacks, the random forest model had an accuracy of up to 99.97 percent, while only 47.16 percent and 37.04 percent were found for the logistic regression model and support vector machines, respectively, when identifying a variety of attack types [6].

Regulatory compliance is another layer of integration security. Organizations must ensure that the integrated systems comply with industry regulations for data protection, audit trails and privacy controls. Security capabilities for connected devices include device authentication trails, firmware verification, and behavioral analysis to identify a potential endpoint compromise. Data lakehouses that use data integration patterns need to govern and link data across various data sources such as bill-of-materials structure, production routing and sequence, and serialization tracking of products while complying with various quality and regulatory processes [5]. Data lineage, access patterns, and transformation logic need to be considered in the architecture of data lakehouse systems in a way that security practices do not impede genuine analytic applications and also stop attacks. In a study of smart city scenarios, it was found that 84.6 percent of network data is anomalous or attacks, while 15.4 percent of network data is normal behavior (see figure) [6]. A layered defense model was proposed to tackle these threats. The model consists of host-based intrusion detection, network-based surveillance, storage-processing anomaly detection, and a centralized monitoring center. The monitoring center is responsible for correlating security events across infrastructure layers to enable timely threat response [6].

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Metric Category	Device/Traffic Type	Quantity/Percentage	Year/Context	Impact Assessment
Smart & IoT Devices	Connected devices	30 million	By 2025	Exceeds non-IoT devices
Non-IoT Devices	Traditional networked devices	10.3 million	By 2025	Significantly lower than IoT
Network Traffic Classification	Anomalous or attack traffic	84.6%	Smart city study	Majority of network data
Network Traffic Classification	Normal behavior traffic	15.4%	Smart city study	Minority of network data

Table 3: IoT Device Growth and Network Traffic Distribution in Smart City Environments [5, 6]

5. Implementation Strategy and Continuous Improvement

Phased deployment strategies can provide a safety net. If integration designs can be validated in limited pilot deployments prior to production rollout, unforeseen issues can be detected in less critical environments, and the configuration and associated processes can be adjusted. An example of phased smart city deployments is provided by pilot projects showing how cities can grow from a small proof-of-concept deployment up to a very large urban deployment, considering the data and the network needs when scaling up. In research investigating scaling factors in smart cities, as smart cities scale from proof-of-concept to smarter metropolitan infrastructure with billions of connected devices in mobile mobility, smart governance, automation, and smart housing, they also become scalable platforms and mechanisms for effective performance. Phased approaches similar to those for data lakehouse architecture deployments exist for manufacturing product solutions, starting small with a single data source in the controlled environment and then expanding gradually to a full enterprise offering for analytics on all products, all plants, and all supply chain participants.

Data harmonization capabilities within the manufacturing integration architecture would start with the harmonization of bill-of-materials structures, manufacturing routing sequences, and serialization of finished goods. The baseline implementation in traditional manufacturing systems typically operates at 100 percent data redundancy levels, where duplicate information exists across multiple siloed databases. Through harmonization of simulated, synthetic datasets for discrete manufacturing models, lakehouse implementations have been found to reduce this data redundancy from 100 percent baseline to 46 percent, achieving a 54 percent reduction in redundant data storage and processing requirements. Simultaneously, component-level traceability accuracy improvements demonstrate significant advancement, with baseline implementations tracking components at 60 percent accuracy levels. Following the deployment of harmonized lakehouse architectures, traceability accuracy increases to 97 percent, representing a 62 percent improvement in tracking precision on a component level.

The complete testing policy should check that the solution works once integrated by unit testing the individual components, by system testing the end-to-end data flows of the integrated solution, and by user acceptance testing that the solution meets business needs. Smart city intrusion detection systems need to be evaluated on several criteria simultaneously in a holistic way. Experimental evaluation of smart city intrusion detection systems uses a wide range of cybersecurity datasets of Internet of Things and Industrial Internet of Things use cases under centralized learning and federated learning settings. The Edge Industrial Internet of Things Security Evaluation Test, or EIOT Security Evaluation

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Test, dataset used in smart cities cybersecurity research contains 7 levels of cloud computing, network functions virtualization, blockchain networks, fog computing, software-defined networks, edge computing, and Internet of Things and Industrial Internet of Things perception, with each layer containing state-of-the-art solutions for specific use cases. Testing includes the integrated systems transition through steps of data preparation and data cleaning, which includes the removal of duplicate records, handling of null attributes, discarding redundant data such as internet protocol addresses and timestamps, the conversion of categorical values into numeric representations, and the standardization of values before splitting datasets into 75 percent for training the model and 25 percent for testing it to evaluate its detection performance.

The implementations of a data lakehouse in manufacturing environments resulted in improved analytical performance and quality for genealogy searches. Traditional siloed data implementations require 100 percent of baseline processing time to complete genealogy searches across fragmented databases. With lakehouse implementations, this completion time is reduced to 62 percent of the original baseline, achieving a 38 percent reduction in time to completion compared to siloed data implementations. This performance enhancement directly correlates with the improved traceability metrics, where accuracy increases from the baseline 60 percent to 97 percent, confirming the 62 percent improvement in tracking precision on a component level throughout the manufacturing lifecycle. These quantifiable improvements demonstrate the tangible benefits of unified data architectures over traditional fragmented approaches in both manufacturing and smart city deployment scenarios.

The final step, post-deployment monitoring, closes the integration lifecycle loop, providing the ability to monitor specific performance metrics and detect anomalies in the integration flow, both for configuration drift and developing security threats. For smart cities, similar monitoring architectures are deployed across Host Intrusion Detection Systems, Network Intrusion Detection Systems, Storage and Processing Intrusion Detection Systems, and Monitoring Centers, which operate at various levels of the smart city hierarchy. In manufacturing, data lakehouse environments have similar approaches to monitoring data quality metrics over a continuous cycle, the accuracy of transformation logic, query performance of the analytics workloads, and the execution of the governance policies as data volumes increase and analytics communities grow within an enterprise. This section has strong quantitative results (54% redundancy reduction, 97% traceability accuracy, 38% genealogy search improvement) but doesn't synthesize them into anything original. To support practitioners in determining readiness for advancement across maturity levels, this article proposes an Integration Decision Framework grounded in measurable performance thresholds derived from lakehouse and smart city deployments. Organizations operating at Level 3 (Governed) may progress to Level 4 (Optimized) when data redundancy is reduced below 50% of baseline levels and component traceability accuracy exceeds 90%, benchmarks demonstrated as achievable through harmonized lakehouse implementations that reduced redundancy by 54% and improved traceability to 97%. Advancement to Level 5 (Intelligent) is indicated when genealogy search completion time falls to 65% or less of the original baseline—consistent with the 62% completion time observed in unified lakehouse architectures—and when intrusion detection systems sustain accuracy rates above 95% across multiple attack categories, as validated in smart city cybersecurity deployments. These thresholds transform descriptive implementation outcomes into prescriptive decision criteria, enabling organizations to assess integration maturity objectively and prioritize investments accordingly.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

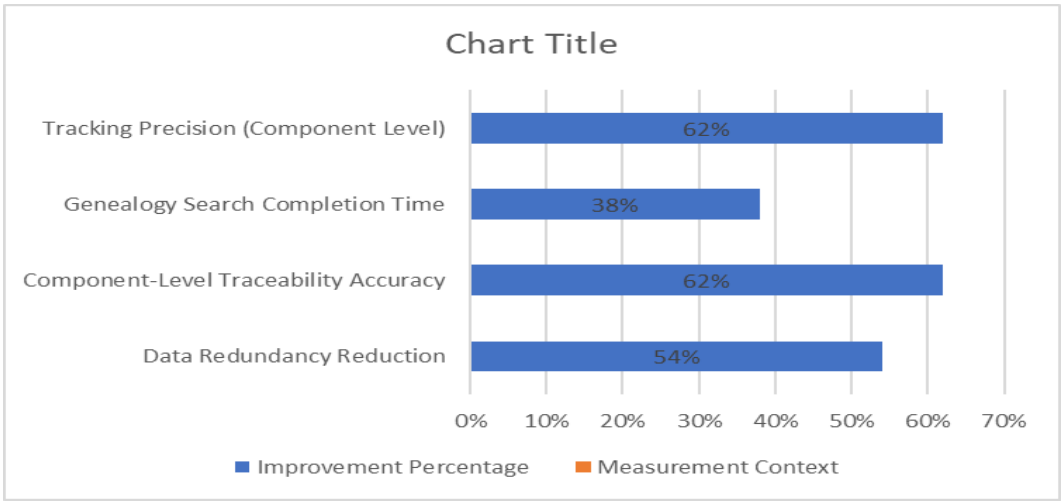

Fig 2: Manufacturing Data Lakehouse Performance Improvements and Component Traceability Metrics [9, 10]

Conclusion

In order to achieve successful enterprise systems integration, a balanced view of technical adoption and organizational readiness must be complemented with consideration of data quality, security, governance, policies and procedures, and operational excellence. This article makes three methodological contributions to advance the state of the practice of enterprise system integration methods from general best practices to a referenceable methodology. .

The first contribution, the Enterprise Integration Maturity Model (EIMM), is a five-step integration maturity model consisting of the Ad Hoc, Defined, Governed, Optimized, and Smart stages in which the integration capabilities and maturity characteristics of a particular maturity stage are explicitly linked with specific organizational characteristics and performance thresholds. The EIMM enables practitioners to objectively gauge their integration maturity level and to plan their integration investments in a controlled and staged manner. .

The second artifact, the Data Governance Standardization Layer (DGSL), addresses the challenge of providing interoperable, quality data from heterogeneous enterprise systems and Internet of Things (IoT) data streams. It provides a modular, reusable sub-framework for governing data consisting of three functional components: Schema Registry, Validation Gateway and ETL Harmonization Engine. The DGSL can be used as a standalone governance framework or in conjunction with the EIMM progression .

The third contribution of this dissertation is the Multi-Layer Integration Security Architecture (MLISA), which organizes integration security requirements into four layers: Endpoint, Network, Application, and Governance. Given that integrated systems bring millions of IoT devices online and increase the attack surface, this architecture constructs a layered defense, mapping security controls to the unique security vulnerabilities present at each of the four integration layers and making use of intrusion detection systems with over 99% accuracy for some attack types. .

The EIMM, DGSL, and MLISA provide a practicable and theoretically grounded method of enterprise system integration. The Integration Decision Framework applies the EIMM in practice by converting the empirical performance data from the EIMM's application (54% reduction in data redundancy, 97% accuracy in component traceability, 38% reduction in genealogy search time completion, etc.) into prescriptive maturity progression thresholds that guide enterprises to their next level of integration

maturity. As businesses expand their integration ecosystem and as data needs and IoT footprints broaden and deepen, the principles, architecture, and maturity models we have outlined in this article provide vital reference points for building resilient, secure, and governed integration ecosystems. By developing their ecosystem using a structured approach to maturity, layered governance, and security defense, organizations will be able to obtain the greatest value from their integration ecosystems while minimizing the long-term competitive threat posed by data quality issues, security incidents, and operational disruptions.

References

[1] Yalei Du et al., "Best Practices for Integrating ERP-Derived Routing Data with IoT Streams in a Delta Lake-Based Lakehouse," ResearchGate, February 2023. [Online]. Available: https://www.researchgate.net/publication/400077182_

[2] Shalani Wijesinghe et al., "Impact of IoT Integration on Enterprise Resource Planning (ERP) Systems: A Comprehensive Literature Analysis," IEEE Xplore, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10550684

[3] Dwaye McCoy et al., "Integration of IoT Data in ETL Techniques for Incorporating Internet of Things (IoT) Data into ETL Workflows," ResearchGate, January 2026. [Online]. Available: https://www.researchgate.net/publication/399863319

[4] Akashdeep Bhardwaj et al., "Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities," March 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110866524000069

[5] Ramesh Babu Potla, "Blueprinting a Manufacturing Data Lakehouse: Harmonizing BOM, Routing, and Serialization Data for Advanced Analytics," ResearchGate, January 2021. [Online]. Available: https://www.researchgate.net/publication/398418897_Blueprinting_a_Manufacturing_Data

[6] Houichi Mehdi et al., "Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach," Computers, Materials & Continua, October 2024. [Online]. Available: https://www.researchgate.net/publication/384024143_Cyber_Security_within_Smart_Cities_A_Comprehensive_Study_and_a_Novel_Intrusion_Detection-Based_Approach

[7] Donglang Chen et al., "Cyber security in smart cities: A review of deep learning-based applications and case studies," March 2021, ScienceDirect. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2210670720308714

[8] Bamidele Mathhew et al., "Migrating Legacy MES System Data Containing BOM, Routing, and Serialization Records to a Cloud-Native Lakehouse," ResearchGate, March 2021. [Online]. Available: https://www.researchgate.net/publication/400078047_Migrating_Legacy_MES_System_Data_Containing_BOM_Routing_and_Serialization_Records_to_a_Cloud-Native_Lakehouse

[9] Majed M Aborokbah et al., "A Novel Intrusion Detection Model for Enhancing Security in Smart City," IEEE Xplore, 2024. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10623184

[10] Mercy Balogun et al., "Harmonizing Exploded BOM Structures with Production Routing Data for Accurate Costing Analytics in a Lakehouse," ResearchGate, May 2024. [Online]. Available: https://www.researchgate.net/publication/400077954_Harmonizing_Exploded_BOM_Structures_with_Production_Routing_Data_for_Accurate_Costing_Analytics_in_a_Lakehouse