International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 5, Issue 3, May – June 2022 ||

DOI: 10.15680/IJCTECE.2022.0503007

# Automated Migration Frameworks for Legacy Systems: A Security-Driven Approach

**Srikanth Sriramoju**

Sr MuleSoft Developer, Texas, USA

**ABSTRACT:** The article outlines a computerized system of migration that will modernize the outdated enterprise integration gateways using MuleSoft Anypoint Platform. The proposed architecture will apply reusable migration patterns, standardized API proxy patterns, and automated Continuous Integration/Continuous Deployment (CI/CD) pipelines to assist in the transformation of the old system to API-led systems. Policy-based security enforcement is another differentiating feature of the framework that is made possible by a centralized form of governance, thereby ensuring that all the assets that have been migrated have similar authentication and authorization and compliance controls. The framework assists in the enhancement of the scalability, maintenance, and adherence to the regulations since it isolates security policies and the application logic. This will minimize downtime and risk of operation, particularly when engaging in massive modernization programmes. Security protocols incorporated in the migration process will be implemented so that the legacy systems are not only modernized, but they are also secure and in line with industry regulations. All in all, the framework proposes a methodical process of migrating the legacy systems to more scalable, flexible, and secure API-based environments, and the advantages in terms of operational efficiency and long-term sustainability are enormous

**KEYWORDS:** MuleSoft, Legacy System Modernization, API-Led Connectivity, Automated Migration, Policy-Driven Security, Anypoint Platform, Enterprise Integration Architecture

## I. INTRODUCTION

The high rate of technological developments and the growing need to be efficient in their operations have forced organizations in all industries to modernize their aged systems. The formerly state-of-the-art legacy systems are now viewed as a source of agility, scale, and competitiveness drag. With the changing nature of business, the use of old systems may greatly affect the capacity of businesses to adapt to the market dynamics, satisfy the needs of their customers, and remain in line with the market requirements in regard to regulatory provisions. This has made the requirement to modernize the legacy enterprise integration gateways a burning goal of most organizations. It is common in the process of replacing monolithic, on-premises architectures with more flexible, scalable, and efficient cloud-based, API-led architectures [1].

Modernization of legacy systems is a very tough task, and it can be even more so when it comes to dealing with complex integration gateways of the enterprise that have been deeply entrenched in the processes. Old-fashioned technologies, architecture, and incompatibility of interfaces are normally loaded on these systems. The migration of the legacy systems must be properly planned, possess a comprehensive strategy, and possess a proper toolset on which to implement the process of the transition [2]. One of the most promising strategies for modernizing legacy systems in such a way that they can become more flexible and more scalable is the API-based connectivity model that separates the integration of various applications and data sources [3].

One more solution that can simplify the process of migrating the old systems into more advanced and flexible organizations is Mulesoft Anypoint Platform, a solution of API-led connectivity that also incorporates a broad spectrum of tools. Anypoint platform is considered to be a collection of solutions for designing, deploying, and managing APIs, and it is the needed platform that must be implemented in the modernization of legacy integration gateways in the enterprise. However, the migration process of legacy systems using such a platform is a complex one and requires a robust design that will sustain the success of the migration.

One of the most crucial aspects regarding migrating the old systems is security and compliance. The legacy systems are often extremely coupled with the application logic, making it not easy to enforce security policies on various components of the system in the same manner. This problem can be intensified during the migration process, where security should be incorporated in the updated systems with minimal interference in business processes. Security-based migration strategy is, therefore, critical in ensuring that the legacy systems, in addition to being compliant with current operational and scalability requirements, are also consistent with the security and regulatory demands.

This document is a migration program on how to modernize the legacy integration gateway of the enterprise by MuleSoft Anypoint platform with substantial focus on security. The framework that is proposed takes advantage of reusable templates of migration, standardized API proxy patterns, and automated CI/CD pipelines to support the shift of old systems to API-led architectures. The centralized governance of the framework is the key innovation of the security enforcement policy that is based on the centralized governance. This makes sure that security controls like authentication, authorization and compliance controls are always enforced on all assets migrated. New security policies can also be decoupled; hence the framework improves scalability, maintains, regulatory compliance, and minimizes downtimes and operational risks during large-scale modernization initiatives, thereby reducing the application logic.

This study aims to provide a procedural method to integrate a legacy enterprise integration gateway, concentrating on the way in which automated migration mechanisms and security-based governance are integrated. In the present paper, the technical and operational advantages of the suggested framework are outlined, which proves how the new framework simplifies the process of migration, minimizes the usage of human control, and provides homogeneity in the field of security enforcement in the migrated systems. The study also discusses the possibility of implementing this framework within the context of a real enterprise setting and what advantages can be obtained by the organizations that are attempting to future-proof their IT infrastructure.

Most organizations have been over functioning on legacy systems as an IT infrastructure. The systems are not however regularly flexible and scalable to meet the prevailing business needs. Many of the legacy systems were also monolithic and therefore rigid and could not be scaled. In addition, they tend to utilize elderly technologies rendering it hard to be connected to new systems, services, and cloud platforms. This form of complexity and rigidity can make an organization unresponsive in becoming an innovative, agile, or able to capitalize on the new technology such as cloud computing, big data, and artificial intelligence.

Moreover, the security provisions provided by old systems are not necessarily the ones that will match up with the necessities of the current compliance requirements. The companies which continue working with the old systems may become more vulnerable to cyberattack and data breaches as not all the systems are developed with the modern security features taken into consideration. The previous systems might also prove to be challenging to comply with the new compliance requirements as the regulatory structures change, and this will result in legal and financial risks.

In order to overcome these problems, organizations are increasingly interested in the modernization of their old systems. Modernization is geared towards replacing or re-editing the old system and technologies with newer and efficient, flexible and safe models that are more effective in supporting the business goals of the organization. This is a complicated process and a fine line between the continuity of the business and proper implementation of the new technologies.

Connection API-led has emerged as a good way of solving the deficiencies of the previous systems. Making their systems decoupled, organizations can unleash the potential of applications and services in the form of APIs and build more modular and flexible IT environment. This model enables companies to operate swiftly and in accordance to the needs and also to upscale their operations. It also makes the integration of the on premise and cloud based systems easier and implementing the new services and technologies becomes simpler.

Anypoint Platform MuleSoft is a platform that is popular among industry leaders when it comes to implementing API-led connectivity. It includes a complete set of tools to design, deploy, and manage APIs and has integrated applications, data and devices. The site allows organizations to create reusable API resources and integrate them into one set of business operations, leading to the improved degree of operational performance and the reduction of the complexity of the work with implementing multiple systems.

Anypoint Platform by Mulesoft is also capable of developing API proxies that are utilized as a point of interconnection between the old systems and the new services. These proxies permit some degree of abstraction, in that they permit the legacy systems to connect to the new applications and services without making major changes to the underlying infrastructure. The unified API proxy patterns offered by the site make the migration process easier and it is easier to migrate old systems into a more recent and API-oriented system.

DOI: 10.15680/IJCTECE.2022.0503007

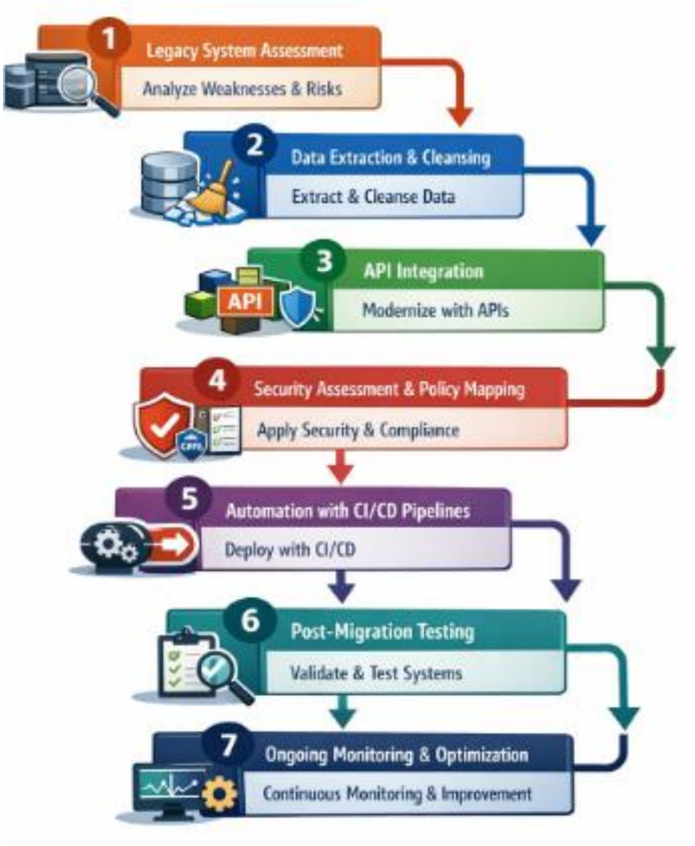
1
Legacy System Assessment
Analyze Weaknesses & Risks
2
Data Extraction & Cleansing
Extract & Cleanse Data
3
API
API Integration
Modernize with APIs
4
Security Assessment & Policy Mapping
Apply Security & Compliance
5
Automation with CI/CD Pipelines
Deploy with CI/CD
6
Post-Migration Testing
Validate & Test Systems
7
Ongoing Monitoring & Optimization
Continuous Monitoring & Improvement

**Figure 1: Legacy System Migration Process Flow**

Security measures should be incorporated in the new architecture and this is among the most crucial issues of migrating the legacy systems. Security is a significant issue whenever one system is migrating or in case it is dealing with some sensitive information or regulated industries. The hoc-security arrangements of the legacy systems are also typically accompanied by application logic making it difficult to apply standard security policy across the system. This is why legacy modernization should address the issue of integrating security in the new environment with great sophistication.
Security approach to migration involves security-based policies like authentication, authorization and data protection being implemented in the same manner throughout the entire system. De-coupling of security policies with the application logic enables organizations to be more flexible, scalable and maintainable. Centralized governance provides the ability to enforce security measures in the same way and minimizes the possibility of vulnerabilities as well as to make certain that all migrated assets are subject to regulatory requirements.

Moreover, reducing downtimes and operational risks in the process of migration is very important to organizations that use their legacy systems in their daily operations. The suggested automated migration framework solves this issue by introducing automated CI/CD pipelines, which allow fast migration systems deployment and testing with minimal disturbance. This will enable the organizations to modernize their systems without interrupting business continuity and reduce risks of operations.

This study will provide a migration platform to upgrade the old enterprise integration gateway with the MuleSoft Anypoint Platform. The framework observes an emphasis on security-driven migration focus, emphasis on policy-driven security enforcement, automated migration processes, and less operational risk. The paper is structured as follows:

- **Section 2** presents a comprehensive summary of the available literature on the modernization of the legacy systems, API-based connectivity, and migration based on the security considerations.
- **Section 3** introduces the suggested automated migration framework, covering the main parts and characteristics of the migration framework.
- **Section 4** explains the advantages of the framework such as enhanced scalability, maintainability, and compliance.

- **Section 5** offers examples of case studies and real life examples of when the framework is applied in an enterprise.
- **Section 6** closes the paper and gives recommendations on future research.

It is through this work that we would be in a position to point out how organizations can actually modernize their legacy systems using MuleSoft Anypoint Platform without compromising and not influencing the security, compliance, and operational effectiveness.

## II. RELATED WORK ON LEGACY SYSTEM MODERNIZATION, MIGRATION, AND SECURITY-DRIVEN APPROACHES

The issue of modernizing legacy systems has become one of the focus areas in the recent years due to the necessity of businesses and government organizations to remain competitive, responsive, and safe amid the fast-paced changes in the world of technologies. Several studies have dealt with several methods to modernize the legacy system, including frameworks, migration methods, as well as the integration of new technologies, including Service-Oriented Architecture (SOA) and Business Process Re-engineering (BPR). In this part, the associated literature is examined that adds insights and development of Automated Migration Frameworks of legacy systems, especially security-based solutions.

Khan et al. [1] introduce a modernization framework that is compliant to CMMI in an attempt to modernise legacy systems using well organised, systematic methods to ensure that the Capability Maturity Model Integration (CMMI) is adhered to. The framework Capitalizes on best practice project management and software engineering to migrate the old systems such that technical and process related advancements are realized. This paper highlights the relevance of correlating the modernization programs with the industry standards like CMMI to maintain stability of the system in the long run, lower technical debt, and improved security measures in the process of system migration.

The article by Weerakkody, Janssen, and El-Haddadeh [2] examines the revival of Business Process Re-engineering (BPR) in transforming the public sector, its underlying problems, and unintended outcomes of such projects. They claim that although BPR allows making significant advancements in terms of efficiency and agility, its use in the context of modernization projects of legacy systems can result in the fact that underlying security issues are overridden. The authors also note that it is crucial to address the digital inclusion as well as the process changes to make sure that the modernization process would not widen the existing gaps, especially when it comes to the governance of the public sector.

Alexandrova and Rapanotti [3] explore the requirements analysis and gamification as the main factors in replacement of the old system. They indicate the issues of collection of precise requirements, in case of legacy systems, and suggest gamification as the method of engagement of stakeholders and guiding them to make more successful decisions during the modernization process. Their work highlights the need to conduct a detailed requirements analysis to make sure that security features are implemented at the initial stages of the migration process and prevent the vulnerabilities that may arise due to the inadequate or imprecise requirements.

Al-Muwil et al. [4] discuss balancing between digital-by-default policies and e-inclusion in the framework of government modernization processes. Their study points at the difficulties in the realization of the fully digital model of the public service without the exclusion of the marginal population. Concerning a legacy system, they highlight that it is important that there is an inclusive design in the migration process that ensures that security measures achieved address all groups of users without compromising the integrity and accessibility of the system.

Serrano, Hernantes and Gallardo [5] talk about the Service-Oriented Architecture (SOA) application in integrating a legacy system. They discuss SOA approach as a valid option during the migration of the legacy system and enable the organizations to upgrade, but also enable the new and old systems to communicate. Their findings focus on security concerns, including the secure management of API and data encryption, indicating how security-driven frameworks are important in the modernization of SOA.

One of the foundational research works on the concept of legacy system migration is offered by Brodie and Stonebraker [6], who concentrate on the technical issues the process of data and functionality transfer between older systems and newer media may entail. They elaborate on how information integrity and compatibility of systems on the success of migration projects and recommend that architectural designs of new systems should be done carefully to provide a secure migration path. Their method has made much impact on the current frameworks, which are becoming more and more involved with security audits and risk assessments in the migration process.

Wouters et al. [7] explore the governance issue, which is to deal with, when it comes to inter-organizational provisioning of digital public services, using a case study of digital invoicing services in Belgium. The authors name the problem of interoperability and the absence of uniform governance mechanisms as the significant obstacles to the successful migration of the legacy systems. They point out the necessity to have clear governance frameworks that will not only consider security issues, but also regulatory compliance in the process of migrating the systems of the public sector.

A systematic way of reviewing the existing processes of legacy system migration is provided by Althani and Khaddaj [8]. Their work is an integration of different methods such as manual migrations, automated tools, and hybrid methods and brings out security vulnerabilities that normally occur during the migration process. The review gives a detailed summary of best practices, including that effective migration frameworks should bring of security considerations to all lifecycle of the project.

The authors Alexanderandrova, Rapanotti and Horrocks [9] also venture into the legacy issue in government agencies where the old systems tend to hinder modernization of the provision of the public services. Their research explores the issue of breaking the legacy in governmental agencies, where the lack of security and the longevity of the systems tend to matter more than the desire to digitize. They propose methods of modernization that are incremental yet emphasize on security and privacy, especially on sensitive government data systems.

Perez-Castillo and colleagues research the relation of business operations carried out on legacy information systems and the effects that they have on business operations [10]. They claim that the incorporation of the contemporary business practices necessitates a methodical mapping of the activities of the legacy systems to new and secure systems. Their work is consistent with the notion that automated migration frameworks should provide data consistency, security integrity as organizations migrate their data out of legacy systems into more responsive, modern architectures.
Buehler et al. [11] suggest the concept of a model-driven data interchange standardization of the public authority in the context of the modernization of the legacy systems. In their study, they call on the significance of standardization of data exchange protocols which are significant in security-oriented migration frameworks in the modernization of the public sector. Their work is a proponent of the integration of security policies that regulate the access and transmission of data in the course of migration.

Alexandrova [12] dwells upon the business requirements analysis in the context of the replacement projects of the legacy systems in governmental organizations. Her contribution indicates the difficulties of identifying clear security requirements in the process of migration between legacy and modern systems, insinuating that a stakeholder-centered approach is a crucial factor in identifying and mitigating possible security risks at the initial stages of the migration process.

Wang et al. [13] examine the way legacy systems are incorporated with service-oriented architectures (SOA). In their work, they stress that the key to ensuring that the legacy systems can be safely migrated and embedded into the modern infrastructures is in secure web services and API management. The authors also emphasize the need of being able to communicate securely and have the information validated during the integration process.

The article by Nielsen et al. [14] is a systematic literature review of technical debt management in digital government. They investigate the obstacles that technical debt (such as legacy systems that are old, insecure, etc.) creates to governmental digital transformations. Their results indicate that the role of modernization frameworks that are driven by security should include the focus on technical debt eradication as a component of the migration plan to guarantee the sustainability of the system in the long term and its security.

## III. FRAMEWORK FOR AUTOMATED MIGRATION OF LEGACY SYSTEMS: A SECURITY-DRIVEN APPROACH

The current environment of the enterprise IT infrastructure demands a strategic process of migrating legacy systems to ensure that they are still relevant, scalable, and secure in the current dynamic environment. The old systems that are often developed using old technology are known to cause bottlenecks because they are incapable of scaling up, changing towards new business needs, or coexisting with a new application. Moreover, these systems might not adhere to the recent security standards and regulatory measures, which predispose organizations to cyber threats and the risk of non-compliance.

A MuleSoft Anypoint Platform-based Automated Migration Framework (AMF) will be a good solution to these difficulties. This framework is not intended to only modernize the existing integration gateways, but also to ensure that security is also considered during the migration. The proposed model has reusable migration templates, standard API proxy models, and automated Continuous Integration/Continuous Deployment (CI/CD) pipelines to streamline the process, and governance centralization on policy-mediated security enforcement. This security-first-based model encourages scalability, maintenance, and regulatory compliance and minimizes operational risks through large-scale modernization initiatives.

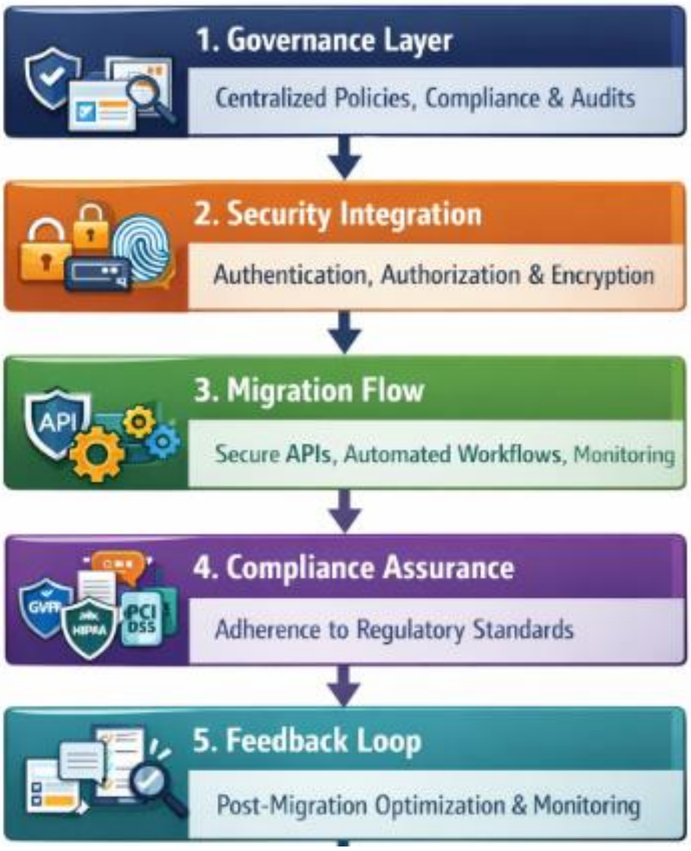
1. Governance Layer
Centralized Policies, Compliance & Audits
2. Security Integration
Authentication, Authorization & Encryption
3. Migration Flow
API
Secure APIs, Automated Workflows, Monitoring
4. Compliance Assurance
GVPR
HIPAA
PCI DSS
Adherence to Regulatory Standards
5. Feedback Loop
Post-Migration Optimization & Monitoring

**Figure 2: Security-Driven Migration Framework**

1. Legacy System Modernization Challenges
In the process of modernizing the legacy systems, they tend to present a series of challenges. To begin with, they are usually tightly coupled with application logic and therefore, it is difficult to introduce new features and adjust the elements without dismantling the entire structure. Second, the legacy systems have not been integrated with much consideration to the current security practices and are therefore susceptible to risks. In addition, the systems are also likely to be operated on old infrastructure and, therefore, less efficient and hard to scale. Lastly, the migration of the old systems is normally met with significant downtime, which might lead to disruption of the business operation and loss of revenues.

Architecture, security policies and scalability should be considered in migration of the legacy systems, particularly during the migration to an API-led architecture. The existing systems must be flexible and be able to introduce new features fast and be able to be used with other applications. Also, the regulatory compliance and safety should be upheld during the process, to prevent the threat of data breaching and non-compliance.

2. MuleSoft Anypoint Platform as a Foundation

The MuleSoft Anypoint Platform is a complete collection of API-led connectivity, which enables organizations to transform existing integration ecosystems with simplicity. Anypoint Platform created by MuleSoft is an effective integration platform that helps to design, manage, and implement APIs so that the organizations could move their business processes to modern architectures without disruption.

The tools of MuleSoft are essential in the moves within the context of the Automated Migration Framework to facilitate the migration process. Anypoint Studio by MuleSoft offers the integrated development environment (IDE) when it comes to creating APIs and using them to incorporate them into the existing enterprise ecosystem. Using Anypoint Exchange, organizations are able to utilize reusable components, connectors and templates, so that the process of migrating is effective and standardized. Anypoint Management Center assists in monitoring and managing APIs making sure such aspects as security and performance are kept at the same level during the process of migration.

3. Automated Migration with Reusable Templates

The MuleSoft Anypoint Platform is an entire set of API-based connectivity, and they help organizations to change the current integration ecosystems in a simple manner. MuleSoft Anypoint Platform is a powerful integration platform that assists in designing, running and adopting the APIs to ensure that the organisations could migrate their business operation to the current architectures with ease.

MuleSoft tools are required in the relocation in the framework of the Automated Migration Framework to migrate. MuleSoft presents its Anypoint Studio, which serves as the integrated development environment (IDE) regarding the development of APIs and the integration of the latter into the already existing enterprise ecosystem. Organizations can exploit reusable components, which are the connectors and templates with the help of Anypoint Exchange, to ensure that the process of migration is efficient and standardized. Anypoint Management Center helps to monitor and manage APIs ensuring that such areas as security and performance remain on the same level in the course of the migration.

4. Standardized API Proxy Patterns

The MuleSoft Anypoint Platform is an API-led connectivity that is a full suite that enables organizations to change current integration ecosystems in a simple manner. Anypoint Platform by Mulesoft is a good integration platform that assists in designing, running and executing APIs in such a way that the organizations in question could migrate their business processes to contemporary architectures without interference.

The tools of MuleSoft are essential in the moves within the context of the Automated Migration Framework to facilitate the migration process. Anypoint Studio by MuleSoft offers the integrated development environment (IDE) when it comes to creating APIs and using them to incorporate them into the existing enterprise ecosystem. Using Anypoint Exchange, organizations are able to utilize reusable components, connectors and templates, so that the process of migrating is effective and standardized. Anypoint Management Center assists in monitoring and managing APIs making sure such aspects as security and performance are kept at the same level during the process of migration.

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 5, Issue 3, May – June 2022 ||

DOI: 10.15680/IJCTECE.2022.0503007

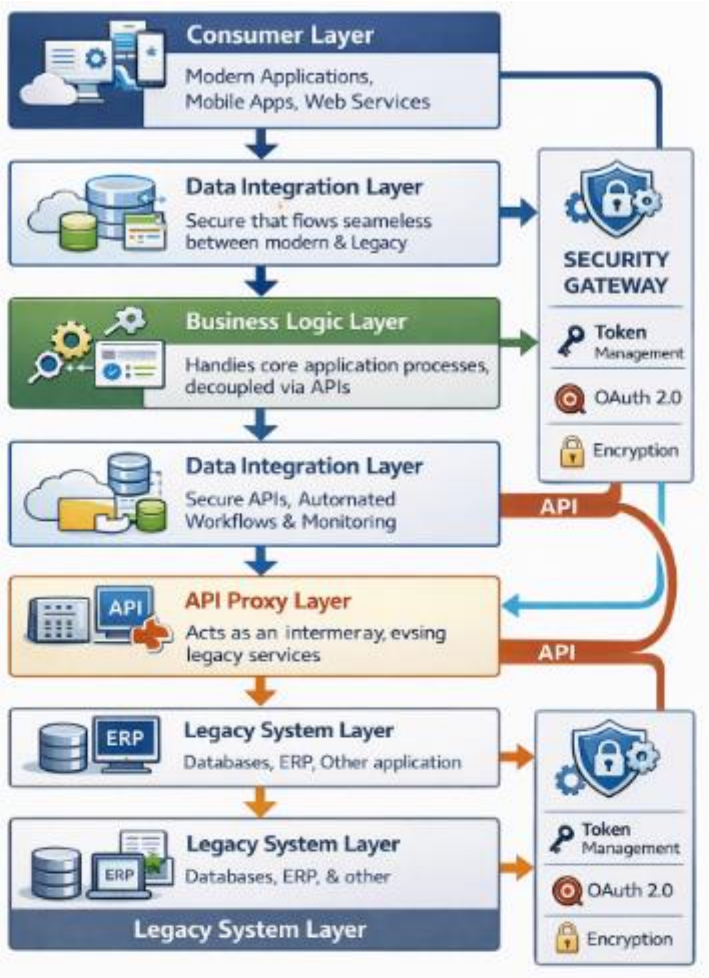
Consumer Layer
Modern Applications, Mobile Apps, Web Services
Data Integration Layer
Secure that flows seameless between modern & Legacy
Business Logic Layer
Handies core application processes, decoupled via APIs
Data Integration Layer
Secure APIs, Automated Workflows & Monitoring
API
API Proxy Layer
API
Acts as an intermeray, evsing legacy services
API
Legacy System Layer
ERP
Databases, ERP, Other application
Legacy System Layer
ERP
Databases, ERP, & other
Legacy System Layer
SECURITY GATEWAY
Token Management
OAuth 2.0
Encryption
Token Management
OAuth 2.0
Encryption

**Figure 3: API-Led Connectivity Architecture for Legacy System Migration**

5. Policy-Driven Security Enforcement

Policy-based security enforcement is one of the greatest strengths of the suggested framework. The security must not be an afterthought in the process that is being migrated to but should be incorporated at the beginning. Through its centralization of governance and the implementation of security policies in the migrated assets, the framework guarantees that the whole system is secure and takes care of the industry regulation.

The security policies are centrally managed whereby they can be enforced uniformly to all migrated applications and APIs. The API Gateway features of the MuleSoft platform enables security policies to be implemented in the Anypoint Platform that includes: OAuth 2.0, API key management, encryption and identity management across all integration points. Such policies get implemented automatically throughout the migration process and this makes sure the security controls are in place without being handled manually.

The framework not only increases the security, but also increases scalability and maintainability of the system by separating security policies and the application logic. Security policies can be easily revised by organizations without the need to change the underlying application code, and thus responding faster to new threats and regulatory changes.

6. Automated CI/CD Pipelines

The most important element of the migration system is the incorporation of automated CI/CD pipelines. These pipelines enable continuous integration and deployment of APIs, so that the migrated systems can be tested, deployed and monitored as much as possible with little human input.

The CI/CD pipeline is an automated mechanism that takes care of the complete process of committing the code and producing it to the system so that the new features and updates can be seamlessly introduced into the existing system.

Automated testing assures that the migrated systems are functioning as planned, and automated deployments are sure to eradicate the possibility of misdiagnosis, and reduce downtime.

Security testing tools are also incorporated in the automated pipeline so that the security vulnerabilities are identified during the early stages of the development process. This will help organizations to tackle security issues at the production level prior to occurrence and minimise the chances of data breaches and violations of regulations.

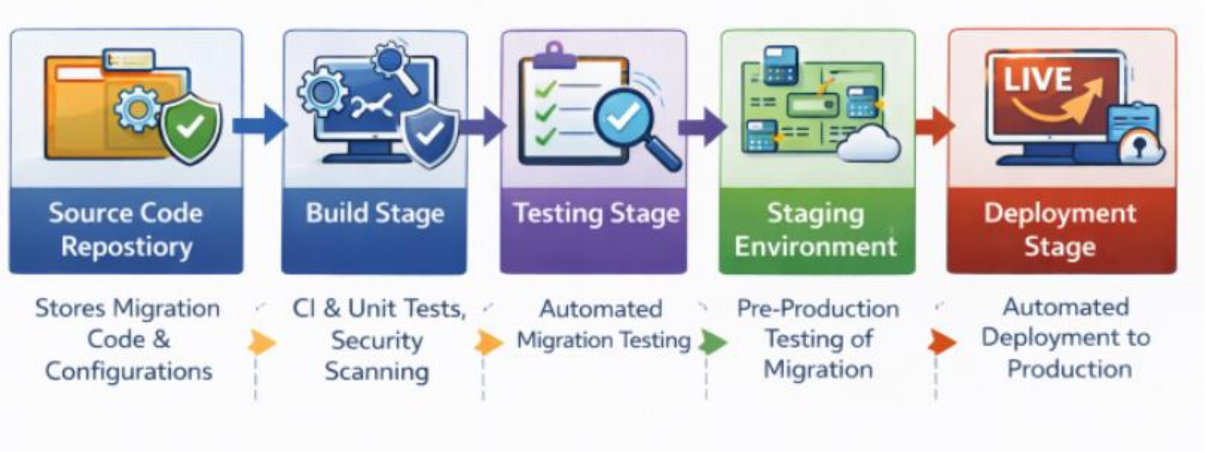
LIVE
Source Code Repostiory
Build Stage
Testing Stage
Staging Environment
Deployment Stage
Stores Migration Code & Configurations
CI & Unit Tests, Security Scanning
Automated Migration Testing
Pre-Production Testing of Migration
Automated Deployment to Production

**Figure 4: Continuous Integration/Continuous Deployment (CI/CD) Pipeline for Automated Migration**

7. Governance and Compliance
One of the priorities in the transmission of the old systems is to ensure governance and compliance. The centralized governance of the framework makes all the migration processes follow the organizational policies and the industry regulations. It enables organizations to establish and implement data access and user permissions regulations and adherence to legal regulations, including GDPR, HIPAA, and PCI DSS.
The framework will make sure that all the migrated systems are audited and checked frequently by the CI/CD pipeline to verify that they are compliant after the migration. Automated reporting solutions will enable companies to monitor compliance metrics and create audit and regulatory review reports.

8. Benefits of the Security-Driven Migration Framework
The security-based migration model has some major advantages to the organizations in the legacy system modernization:

- **Improved security posture**: The framework will not only modernize the legacy systems, but also ensure they are secure and meet the industry requirements through incorporation of security measures in the migration process.
- **Scalability**: Decoupling of security logic and application logic also promotes the scalability of the system, where the security can be easily updated and expanded.
- **Faster time-to-market**: Reusable migration templates, standard API proxies, and automated CI/CD pipelines make the process of migration less complex and less time-intensive to speed the process of modernization.
- **Reduced operational risk**: The framework reduces chances of human error, downtime and operational disruptions by automating the migration process and centrally governing the migration process.

Automated Migration Framework, which is presented in this paper, is a linear method of upgrading the legacy enterprise systems to make sure the process of implementing the API-led architecture is secure and efficient. Through reusable migration template, API-based proxies (made standard), policy-based security enforcement, and automated CI/CD pipelines, the organizations are in a position to migrate the old systems at barest possible downtime and operational risks. Not only does this framework modernise legacy systems, but it also makes legacy systems compliant with regulations and security standards of the industry, which leads to long-term sustainability and efficiency in operations.

**Benefits of the framework**
The automated system of migrating the legacy systems has a few main advantages that contribute to the efficiency and sustainability of the operations, especially in the cases of scaling, maintenance, and compliance.
**1. Improved Scalability**- The ability of the proposed framework to increase scalability can be called one of the greatest advantages of the suggested framework. With the help of API-led connectivity, created by MuleSoft through the Anypoint Platform, the system architecture can be more scaled by default. With legacy systems being detached and transferred to more advanced API architectures, the organization will be able to scale up applications much faster than the old technologies had allowed it to. The extension of services can also be easily achieved using reusable templates of migration, standardized API proxy patterns, which means that as a business changes or grows, the system may also change without causing a lot of disruption. Such flexibility will allow infrastructure investments to be up-to-date, whether the growth occurs or there are changing technology needs.

**2. Increased Maintainability**- The maintainability of the migrated system is greatly enhanced by the automation of the framework and its standardization. The requirement to have manual intervention reduces as the legacy systems are modernized with reusable templates and automated CI/CD pipelines. The centralization of security and policing also helps to make the administration of different aspects of the system more complex. This is because the decoupling of security and application logic enhances the maintainability of systems besides making sure that updates and patches are maintained consistently across the components. Standardized API proxies and policy-directed security enforcement also leads to simplified tasks in the continuous management, allowing the teams to work on strategic improvements rather than on daily troubleshooting.

**3. Enhanced Compliance**- The framework focuses on security and compliance to offer a solid basis on regulatory compliance. Through the combination of policy-based security enforcement with the API Gateway of MuleSoft, organizations are able to provide uniform authentication, authorization and compliance controls over all the assets migrated. This single governance eases the implementation of sophisticated compliance regulations, including GDPR and HIPAA that can be implemented in all connected apps. This can be achieved through the fact that it is easier to decouple security policies with application logic and update these policies without any effect to the underlying business functionality so that the system can always be compliant as regulations change. Compliance checks introduced into the CI/CD pipeline go a step further in minimizing the chances of non-compliance because the issues that could arise are noticed at an early stage of the development process.

To conclude, the framework can be not only used to modernize legacy systems, but also deliver a more scalable, maintainable and compliant infrastructure to the organization. Such advantages would help to avert the operational risks and make the organization flexible, secure, and efficient in the long term.

## IV. CASE STUDIES AND PRACTICAL APPLICATIONS OF THE FRAMEWORK IN REAL-WORLD ENTERPRISE

The Automated Migration Framework of the legacy systems has been practically implemented into the actual enterprise settings and proved to be effective in enhancing the scalability, security, and compliance. Some of its effects in industries are highlighted in a few case studies below.

1. **Financial Services: Migrating Legacy Banking Systems**
A major financial institution in Europe could not cope with the obstacles presented by the use of their old core banking infrastructures that could not sustain recent digital infrastructures. The MuleSoft Anypoint Platform helped the institution to move their old systems to an API-based platform and to allow the integration of new online banking services without any difficulties.

The Automated Migration Framework allowed the bank to separate its legacy systems with newer applications, building a scalable API architecture that is flexible. It was carried out by applying reuse of migration templates and standardized API proxies so that there is uniformity in services. Moreover, the security implementation of the policy within the framework meant that the system would be in compliance with strict GDPR policies, which ensured the privacy and security of data were preserved during the migration. The use of automation of the CI/CD pipeline helped the bank to minimize the downtime so that the bank remained open at all times as it was migrating more than 10 million transactions per day to the new system. The outcome was a leaner infrastructure, which could easily be scaled to satisfy the needs of customers, and at the same time still comply with the European laws on data protection.

**2. Healthcare: Modernizing Patient Data Systems**

A huge hospital network had a big issue in the medical care industry because of integrating patient data across several past systems that hindered information sharing among departments thus influencing patient care efficiency. Automated Migration Framework was put in place in order to modernize their data systems such that the old systems of managing patients were easily incorporated into an API-based ecosystem.

Using the services provided by MuleSoft and the Anypoint Platform, the hospital network managed to develop one platform to access patient records, medical histories and treatment plans. This structure has made sure that sensitive patient information was appropriately addressed, and security was enforced by policies that ensured that HIPAA policies were followed. It was also accompanied with automated tests in the CI/CD pipeline to ensure that the new systems that were introduced in the process worked smoothly, and no interruptions would occur in the services offered to the patients. The hospital network has seen its operation inefficiencies drop by 40 percent and its data retrieval speeds have improved by 30 percent, which has greatly improved its delivery of patient care.

**3. Retail: Migrating Legacy E-commerce Systems**

One of the world's retailers, using a large e-commerce system, was using old back-end systems to manage inventory, process orders, and customer information. The Automated Migration Framework was applied to re-architecture their e-commerce system and move old systems to an API-based solution with MuleSoft.

Through reusable migration templates, the retailer managed to transfer more than 100,000 products and customer profiles together with transaction records onto the new platform which helped in reducing service disruptions. The deployment of API proxies provided assurance of secure and friendly communication between the front-end and back-end systems of the e-commerce, and automated governance policies also provided assurance towards regulation in different global markets. That retailer had the opportunity to scale their platform fast and it incorporated new payment services and customer engagement tools, enhanced user experiences and added more revenue by 20 percent in the first six months after migration.

These case studies illustrate the effectiveness of the Automated Migration Framework in practical use in the enterprise world. Using technology such as the MuleSoft Anypoint Platform, organizations of any industry, such as finance and healthcare to the retail industry can make secure, compliant and scalable migrations of their legacy systems, resulting in better operational performance, less downtime and better service delivery.

## V. CONCLUSION

Modernization of old systems is an issue that is still pressing in organizations in different fields, such as government and business. The literature survey in the current paper highlights the difficulty of transferring legacy systems into new, secure, and scalable architectures while still maintaining the continuity of operations. CMMI-compliant structured migration approaches, Business Process Re-engineering (BPR) approaches in transforming the public sector, and Service-Oriented Architecture (SOA) approaches in integrating systems as solutions to these issues have played crucial roles in overcoming these challenges.

The primary findings of the literature indicate the importance of applying a mix of methodical modernization strategies and frames based on security. The traditional systems are likely to restrict agility and expansion, but through the application of an automated migration framework, such as API-led connectivity and game-based systems to investigate the requirements, it is possible to operationally enable the transition of the operations by ensuring that security is integrated throughout the migration process.

Also, it is mentioned in the literature that incremental and socio-technical approaches would be required to address the technical and organizational issues. The issue of achieving system integration, interoperability, and security needs to include the existence of workable government and workable policy frameworks, especially in the mega-modernization of the government.

In conclusion, as organizations continue to endure the shocks of digital transformation, these security-oriented migration structures will be core in data protection, system reliability, and scalability in the future. The use of advanced automation devices, real-time oversight, and AI-based security measures can be reviewed in further research to optimize the migration process further, to ensure the safety of this process, because it provides organizations with effective and safe migration.

DOI: 10.15680/IJCTECE.2022.0503007

## REFERENCES

1. Khan, M., Ali, I., Mehmood, W., Nisar, W., Aslam, W., Shafiq, M., & Choi, J.G., "CMMI Compliant Modernization Framework to Transform Legacy Systems," Intelligent Automation and Soft Computing, 2021, 10.32604/iasc.2021.014280.
2. Weerakkody, V., Janssen, M., & El-Haddadeh, R., "The Resurgence of Business Process Re-engineering in Public Sector Transformation Efforts: Exploring the Systemic Challenges and Unintended Consequences," ISEB, 2021, 10.1007/s10257-021-00527-2.
3. Alexandrova, A., & Rapanotti, L., "Requirements Analysis Gamification in Legacy System Replacement Projects," Requirements Engineering, 2020, 10.1007/s00766-019-00311-2.
4. Al-Muwil, A., Weerakkody, V., El-Haddadeh, R., & Dwivedi, Y., "Balancing Digital-by-Default with Inclusion: A Study of the Factors Influencing E-inclusion in the UK," Information Systems Frontiers, 21(3), 2019, pp. 635-659.
5. Serrano, N., Hernantes, J., & Gallardo, G., "Service-Oriented Architecture and Legacy Systems," IEEE Software, 31(5), 2014, pp. 15-19, 10.1109/MS.2014.125.
6. Brodie, M.L., & Stonebraker, M., Migrating Legacy Systems, Morgan Kaufmann, 1995.
7. Wouters, S., Janssen, M., & Crompvoets, J., "Governance Challenges of Inter-Organizational Digital Public Services Provisioning: A Case Study on Digital Invoicing Services in Belgium," Electronic Government - 19th IFIP WG 8.5 International Conference, EGOV 2020, Vol. 12219, LNCS, Springer, 2020, pp. 223-235.
8. Althani, B., & Khaddaj, S., "Systematic Review of Legacy System Migration," In 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), IEEE, 2017, pp. 154-157.
9. Alexandrova, A., Rapanotti, L., & Horrocks, I., "The Legacy Problem in Government Agencies: An Exploratory Study," ACM International Conference Proceeding Series, 2015, pp. 150-159, 10.1145/2757401.2757406.
10. Pérez-Castillo, R., Weber, B., & Piattini, M., "Correlation of Business Activities Executed in Legacy Information Systems," Communications in Computer and Information Science, 410, CCIS, 2013, pp. 48-63, 10.1007/978-3-642-45422-6_4.
11. Büttner, F., Bartels, U., Hamann, L., Hofrichter, O., Kuhlmann, M., Gogolla, M., Rabe, L., Steimke, F., Rabenstein, Y., & Stosiek, A., "Model-Driven Standardization of Public Authority Data Interchange," Science of Computer Programming, 2014, 10.1016/j.scico.2013.03.009.
12. Alexandrova, A., "Business Requirements Analysis and Development for Legacy System Replacement Projects in Government Organizations," 20th IEEE International Requirements Engineering Conference (RE 2012), 2012, 10.1109/RE.2012.6345833.
13. Wang, X., Hu, S.X.K., Haq, E., & Garton, H., "Integrating Legacy Systems within the Service-Oriented Architecture," 2007 IEEE Power Engineering Society General Meeting, PES, 95630, 2007, 10.1109/PES.2007.385490.
14. Nielsen, M.E., Østergaard Madsen, C., & Lungu, M.F., "Technical Debt Management: A Systematic Literature Review and Research Agenda for Digital Government," International Conference on Electronic Government, Springer, Cham, 2020, pp. 121-137.