International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

System and Data Integration Approaches for Ensuring Scalability and Cloud in Enterprise Architectures

Shivdeep Kumar*

Integration Architect

Received 01 Dec 2024, Accepted 20 Dec 2024, Available online 23 Dec 2024, **Vol.14, No.6 (Nov/Dec 2024)**

Abstract

Interoperability has recently been considered by businesses as a potential competitive advantage. As a primary tactic, several businesses have reorganized themselves to facilitate interoperability. Enterprise architecture (EA) are critical for aligning business processes with IT infrastructure to meet evolving organizational needs. This paper explores system and data integration approaches for ensuring scalability and security in enterprise architectures. The integration of multiple information systems aims to enhance information accessibility, enable strategic alignment between business and IT, and streamline operations across various organizational levels. It discusses key characteristics of scalable integration systems, including load, space, and structural scalability, alongside security mechanisms like authentication, encryption, and API management. Furthermore, analyses enterprise integration frameworks, focusing on network, data, application, and business process levels. Comparative analyses of various methodologies and models highlight their performance, limitations, and future research directions. This study provides insights into achieving a secure, scalable, and efficient enterprise architecture to support modern organizational growth and resilience.

Keywords: *Enterprise architecture, System integration, Data integration, Scalability, Security, Information systems.*

Introduction

It is common practice for businesses in the modern day to use several complementary information systems. Companies use these techniques and have a hard time taking advantage of possibilities in very competitive marketplaces. To take advantage of long-term investments in IT infrastructure while effectively meeting the demands of businesses and customers in this environment, it is becoming more and more essential to integrate current information systems [1]. Enterprise systems (ES) are becoming more important to almost every company in the globe these days. Business process automation and data management are two of the many functions that ES's suite of apps may provide. Management and planning of the enterprise system's resources are the primary functions of the integrity and information system configuration, which are essential capabilities of the enterprise system.

The creation and use of information system architectures laid the groundwork for the specialised discipline known as enterprise architecture (EA) [2].

In order to facilitate the alignment of their business and IT processes, organisations use enterprise architecture to create an integrated environment[3]. The complexity of EAIM's procedures, models, methodologies, and strategy renders the EA implementation methodology useless for supporting Enterprise Architecture Implementation [4]. The overarching goal of information system integration is to merge certain systems into a single, cohesive whole, creating the impression to consumers that they are dealing with a single system[5]. Integration is necessary for two reasons: Starting with an existing collection of information systems, an integrated view may be made to make it easier to access and reuse information via a single point of access. Secondly, when an information need arises, data from various supplementary information systems is merged to provide a more thorough foundation for meeting that need [6].

In contrast, a different body of literature views information systems integration as a necessary first step towards IT and business strategy alignment[7]. Making individual components of a system function as a whole is known as systems integration. When working on big, complicated projects with a wide variety of information and components, both real and intangible, that must be coordinated, modified, and

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.14.6.12

fitted together, systems integration becomes even more of a challenge[8]. Systems integration is the process of bringing together different systems that are delivered by different organisations via collaborative efforts across organisational boundaries [9]. A complete security solution requires not just these methods but also the development of a security architecture for the business environment, which must include rules, procedures, and technology [10][11].

Architects may use EA to apply architectural methods and concepts to help organisations navigate the technological, business, information, and process changes required to implement their plans. These methods identify, inspire, and accomplish these changes by leveraging the many facets of an organisation. Despite the time and financial costs, the installation of EA often results in higher profitability due to its efficiency and cost reduction. Additionally, the larger the company, the better the EA quality needed [2].

Organization of the paper

The structure of this paper is as follows: Section II covers enterprise architecture fundamentals and types. Section III discusses integration approaches for scalability and security. Section IV explores scalability solutions and security mechanisms. Section V presents a literature review and comparative analysis. Section VI concludes with future research directions.

Fundamentals Of Enterprise Integration

Enterprise integration emerged from the Industrial Computing world of the 70s, with an emphasis on Computer Integrated Processes with Harrington's thoughts on CIM integration. It was perceived as a massive leap forward, as it improved the ability to leverage organisational goals by means of resource management, keeping organisation consolidation and process information systems in perspective. Effective communication and information sharing, as crucial to intra- and inter-organization bonding, are at the centre of these strategies [12].

Overview of Enterprise Architectures

Enterprise architecture is a methodical approach to business evaluation, design, management, and execution that uses a comprehensive approach at each stage to effectively define and implement strategy. With the help of enterprise architectural standards and processes, businesses are able to better organise their IT software operations and policies, which in turn helps them achieve their company goals, deal with changing market conditions, and overcome obstacles. Assuring a plan and preventing haphazard block construction are two aspects of enterprise architecture [13][14]. By "the rational framework for categorising and arranging the descriptive representations of an enterprise that are crucial to the administration of the enterprise and the growth of its systems," John Zachman means the Zachman framework. The primary objective is to provide a rational framework for the organisation of the design artefacts of the company[15]. A benefit of the framework is its selection ability, which lets architects concentrate on a certain part of the system rather than the complete without sacrificing any data from the rest of the system. This paradigm provides architects with a structured perspective on corporate systems, facilitating holistic analysis [16].
It consists of a 6x6 matrix.

Data, functions, networks, people, time, and motivation are the six facets of the business that may be represented or modelled by the columns.

The six perspectives shown by the rows of the Zachman framework—scope, business, system, technology, detailed representation, and running enterprise—allow for the description of the aspects.
Each cell, formed by the junction of a column and a row, represents a different perspective on the company that is being modelled.

A business architect may then assign a particular function to each cell.

Types of Enterprise Architectures

Figure 1 shows four interconnected sub-architectures that make up an enterprise's overall architecture. These are:

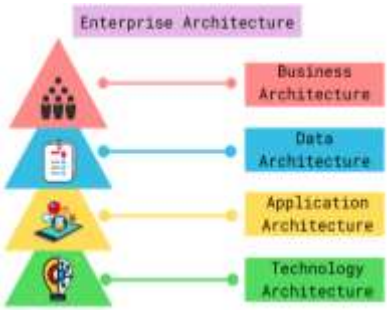

Fig.1 Types of Enterprise Architecture

Business Architecture

Enterprise Architecture as a whole relies on sound business architecture to provide desirable results. In order to make the change in a business climate that might be both competitive and disruptive[17], it lays out the organisation's drivers, strategy, operational models, goals, and objectives. All other types of architects need to have a firm grasp of business architecture so they can accurately describe their own practices and follow them in achieving the desired business results.

Data Architecture

Data Architecture is an essential part of any Enterprise Architecture Program since all of the other architectures rely on it for creation, consumption, and

destruction of information[18]. To achieve business results, it is necessary to understand which technologies store and alter the data, which apps act as the master record, which functions and processes use the data, and where the data is produced and deleted.

Application Architecture

An essential inventory of the enterprise's applications, the application architecture details the tasks performed by these programs in relation to data transformation, transmission, and storage[19]. In addition to outlining the business models' activities—like Capability models and Business Process diagrams—the architecture details the interfaces that programs must have or supply in order to carry them out.

Technology Architecture

Application services[20], which in turn enable information and business operations and services, rely on the logical, physical, and virtual infrastructure described by the technological architecture, which is the foundational architecture.

The Need for Scalable Enterprise Solutions in the Modern Era

Businesses in today's digital-first, highly competitive environment are under constant pressure to adapt quickly and effectively handle massive volumes of data[21]. The sheer amount, diversity, and velocity of data that modern organisations must handle is putting traditional on-premise data management solutions to the test. As the world becomes more interconnected, the capacity to expand operations, access data in real-time, and make decisions more quickly are of the utmost importance. To meet their ever-increasing data demands in an efficient, secure, and cost-effective manner, enterprises need scalable solutions.

Characteristics of Scalable and Secure Integration Systems

Scalable and secure integration systems are critical for modern enterprises to support seamless operations, growth, and protection of data. Here are the key characteristics of such systems:

Scalability Characteristics

This section discusses four different kinds of scalability: structural, load, space, and space-time. It is possible for a system or its parts to possess many of these characteristics. In addition, there may be an interaction between two or more scalability types.

Load scalability: They say that a system is load scalability fit if it can handle low, moderate, or high loads gracefully, meaning that it can make excellent use of its resources without causing unnecessary delays, wasted resource usage, or resource contention.

Space scalability: The capacity of a system or program to handle an increasing number of things without experiencing unmanageable memory needs is known as space scalability.

Space-time scalability: They say that a system is space-time scalable if it retains its functionality as the number of items it contains grows by many orders of magnitude.

Structural scalability: A system is considered structurally scalable if and only if its standards and implementation do not, or will not, limit the expansion of the number of objects it can accommodate within a certain time period [22].

Security Characteristics

Since wireless communication is more susceptible to interception and manipulation, physical threats are more common in wireless networks compared to wired networks. In heterogeneous wireless networks, some desired security aspects include:

Authentication: prevents unauthorised client stations from connecting to the network with its robust authentication functionality.

Confidentiality: aims to make it harder for casual eavesdroppers to get sensitive information.

Integrity: stops the transmission of altered messages between the wireless client and the access point.

Confirmation services: Digital receipts may be generated by message transfer agents to prove the sending and receiving of messages [23].

Integration Approaches and Frameworks In Enterprise

The following points provide the integration approaches and frameworks in enterprise:

System Integration in Enterprise

Data may be easily transferred across different systems, independent of their kind or vendor, with the help of Enterprise Systems Integration, a method for integrating businesses. It also paves the way for data transfer among systems that are geographically separated or of different generations. The foundation of any company is its enterprise systems integration architecture. It streamlines your company's operations and data exchange on one platform, making you more productive.

Improved Productivity: Streamline your company's operations and cut down on job completion times via systems integration. Your capacity to finish tasks on schedule will grow, leading to happier customers.

Improved Efficiency: System integration and smooth operation reduce the need for human workarounds and redundant procedures. In addition to lowering stress levels and saving time, this frees up staff to concentrate on other initiatives that directly impact the bottom line.

Reduced Costs: Companies may save money by cutting out unnecessary operations like customer

service or human resources when all departments are linked via a single system, thanks to integration, which improves data management across departments.

Data integration in enterprise

Data teams face several hurdles as the significance of corporate business data integration continues to expand at an unprecedented pace. Data integration strategies are used by data engineering teams to handle complicated data integration. Enterprise data integration has long included moving previously siloed or unrelated datasets into a common database, data warehouse, or data lake from their original, more dispersed locations. In addition to facilitating company operations, these storage solutions provide the groundwork for data organisation, often via data marts, which data engineers use to their advantage when processing and managing data.

Key enterprise data integration approaches

There are two main approaches to data integration:
Data warehousing: A data warehouse consolidates all of an organisation's data into one place, making it easier to run sophisticated queries, compile comprehensive reports, and discover actionable insights. Business intelligence and analytics rely heavily on it because of its superiority for structured data that is often queried.
Data lakes: A data lake provides versatility by enabling several data kinds to coexist in one repository. This includes movies, photos, data from Internet of Things sensors, and feeds from social media. Data lakes are capable of handling large amounts of both structured and unstructured data, in contrast to data warehouses, which only deal with structured data. This method is perfect for companies working with large data, complex analytics, and Machine Learning models since it lets them keep raw data in its original format until it's time to analyse it.
APIs for Data Integration: Integrating data with RESTful APIs or GraphQL allows businesses to link different systems in real time and keep data flowing in a unified fashion across all services.

Integration framework in enterprise

The purpose of this conceptual framework on business integration is to break down the company into its component parts in order to better understand the many forms of integration. The four tiers of an enterprise system and the forms of integration at each tier are shown in Figure 2. Here are the four tiers: platform/network, data, application, and process. More abstract objects appear in subsequent levels. What follows is a description of the stages, kinds of integration, and integration challenges that are experienced at each level.

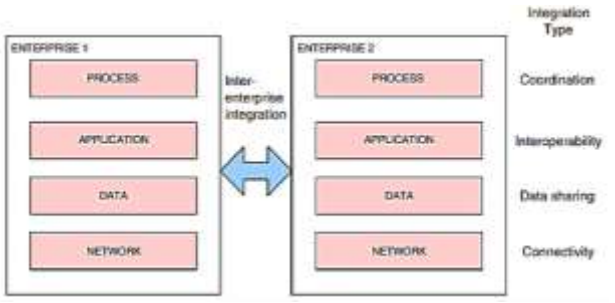

Fig.2 Enterprise information integration framework

Network level

Network or platform level is the most basic level of a business. The integration problem at this level is the physical heterogeneity of a physical network's hardware, computers, devices, and operating systems. At the network level, integration is all about connectivity, which is the links between modules, systems, and applications. Connectivity does not guarantee that the data supplied can be understood; rather, it just guarantees that data and/or messages may be exchanged from one system to another.

Data level

Separating data from business logic and algorithms is a fundamental aspect of information system architecture. All of the information that the enterprise system needs to run its operations is provided at the data level. Where two or more subsystems or organisational units share data with each other, that is the purpose of integration. When it comes to data schema diversity, there are a few different categories that need to be addressed via sharing:
Different perspectives: local terms for the same or related ideas. Different companies may use different terms when referring to the same document.
Equivalence among constructs: A variety of approaches may be used to simulate the domain of an application. One possible representation is as subtypes of Persons for the genders male and female.
Inter-schema properties: When several schemas are combined, it's possible for items in one schema to have meaningful connections with things in another schema.

Application level

A service-providing application is an information system. The usage of data and communication formats that are specified locally by each application, programming language, or system results in heterogeneity. The capacity for one software program to access and use data created by another software program is known as interoperability.

Business process level

Business processes are represented at the process level, and applications serve one or more activities

inside those processes. Tasks within the business process are often carried out by other functional units or even by other organisations in the supply chain. "Managing the dependencies that arise among business tasks" is one definition of coordination. The need to carefully consider the function of coordination in corporate integration is becoming more and more acknowledged by studies.

Scalability Solutions in Integration

Scalability is a cornerstone of a successful enterprise integration architecture (EIA). A process or system is considered scalable if it can easily manage a growing workload. An increase in consumer demand, entry into untapped areas, or brand-new offerings are all ways this may play out for a business. In the world of entrepreneurship, scalability is a fundamental idea, especially when evaluating the possibilities and feasibility of new businesses. The ability of a company to develop and expand without experiencing a corresponding rise in operating expenses is the essence of scalability. In today's fast-paced and cutthroat business world, the capacity to scale up quickly and efficiently is crucial for entrepreneurial endeavours.

Key Components of an Expandable EIA

An EIA designed for scale comprises several key components that work together to expand and adapt to an organisation's changing needs. Modular design plays an integral part, as it enables independent scalability of components without overhauling their architecture altogether.

Furthermore, API Management facilitates smooth communication among different systems and applications while simplifying integration as new services are added.

Data Management strategies are essential to ensure data consistency and accuracy across various platforms. These strategies employ techniques like virtualisation and real-time information processing.

Load Balancing distributes workload evenly among servers to avoid becoming bottlenecks. Monitoring and Analytics tools help organisations monitor real-time performance as demands increase to make informed decisions on resource allocation and infrastructure adjustments.

Risk Management

Real-time fraud detection in banking is made possible by system and data integration, which combines transaction data and consumer behaviour from several platforms. Advanced analytics and artificial intelligence are used by integrated systems to identify suspicious activity and take prompt action to stop fraud. Furthermore, by combining information from several departments, data integration improves risk assessment and the bank's capacity to assess operational, market, and credit risks. This integrated strategy enhances decision-making and prompt risk mitigation by offering a thorough understanding of potential risks.

Business Continuity

For financial operations to have as little downtime as possible, integrated disaster recovery solutions are crucial. Businesses can create failover systems that automatically move to backup locations during outages by integrating vital systems and data. The bank can continue operations with a few outages thanks to this integration, which guarantees current data synchronisation. Moreover, interconnected systems simplify the process of identifying and fixing breaks down, cutting down on recovery time and preserving business continuity, protecting client confidence and legal compliance.

Security Mechanisms for Integrated Architectures

Security mechanisms in integrated architectures are essential for safeguarding enterprise systems, data, and applications from vulnerabilities and threats while ensuring reliable communication and data exchange[24]. Access passwords, devices, and biometric devices all work together to ensure authenticity. The use of a password for initial authentication on most computers is now commonplace. Additionally, with the assistance of external authentication methods offered by certain businesses, they may encrypt these passwords inside the information systems [25].

Data encryption standards for integration layers

In 1974, the United States government and IBM worked together to create the Data Encryption Standard (DES) (US patent 3,962,539) so that everyone could send and receive encrypted data. Protecting non-classified information required a robust cryptographic method, according to the National Institute of Standards and Technology (formerly the National Bureau of Standards) in 1972. The algorithm has to meet three criteria: low cost, high availability, and high security. The NIST aimed to create a public good with many potential uses. As a result, they posted a call for suggestions for this kind of algorithm. In 1974, IBM presented the Lucifer algorithm, which seemed to fulfil the majority of NIST's specifications[26].

Authentication and authorisation protocols

Authentication ensures that you are consistently identified as the same person, while authorisation establishes whether you are granted permission to access or do the desired activity. Unfortunately, that resource is not accessible to you at this time. In a

nutshell, authentication—sometimes shortened to AuthN—is checking the identity of the user attempting to access a resource or start a session. Following authentication, the system or service will authorise you to execute certain actions based on your identified identity [27].

Secure API development and management

A software application interface (API) facilitates communication and connection between various digital devices, software programs, and data servers. A lot of cloud services employ an API gateway, which is a single point of entry for user verification and identification placed in front of an API in the network architecture. As a security gateway, the API gateway keeps tabs on and consolidates identity management.

Threat modelling in integrated systems

Threat modelling is a crucial part of ensuring the security of integrated systems within enterprise architectures. It involves a systematic approach to identifying and categorising potential threats in a given system by analysing actors, the system itself, and organisational context. This process helps security teams uncover vulnerabilities that may lead to compromises. By leveraging threat modelling, organisations can better understand potential security risks, leading to improved scalability and stronger security measures for enterprise architectures [28].

Literature Review

In this section, they provide some previous research on System and Data Integration Approaches for Ensuring Scalability and Security in Enterprise Architectures.

In, Aldea et al. (2018) they present their plans for Enterprise Architecture 4.0, an enhanced Enterprise Architecture methodology tailored to Industry 4.0, and detail their ongoing endeavours to develop a software platform for model management and analytics that will underpin these plans. To tackle this problem, one strategy is to look at how IT-driven design methods, like Enterprise Architecture, might work with this deluge of (large) operational data[29].

In, Ahmed, Bhuiya and Rahman (2018) suggested design incorporates a kernel-based security architecture that incorporates audit, risk, and incident management tools. It is a high-performing design that incorporates all the key elements of contemporary enterprise architecture (EA) while also improving security and ensuring sustainability. A company's ability to adapt to changing market conditions and meet its present and future objectives is directly related to the quality of its business processes, technology, and information systems[30].

In, Al-Turkistani, Aldobaian and Latif (2021) demonstrates that, in addition to meeting business needs, Enterprise Architecture Frameworks (EAF) should have detailed cybersecurity standards that harmonise EA business plans. Businesses must now shift their attention to developing a resilient strategy that goes beyond traditional perimeter defences. Unfortunately, these frameworks aren't comprehensive enough to cover the whole company when it comes to security, leaving businesses vulnerable to serious security threats and potential financial losses[31].

In, Diefenbach, Lucke and Lechner (2019) their goal is to find out how EAM, RM, and ISM initiatives may work together for "the greater good" so that RM and ISM can be made easier by adopting EAM. For example, their study suggests that enterprise architecture management (EAM) may aid risk management (RM) and information security management (ISM) by giving a wealth of data on an organisation's information assets, which is relevant to their interest in information security[12].

In, Costa and Brito (2022) this article concludes with a recommendation for ongoing EA maintenance that mprove the EA's quality and, by extension, the organisation's performance. EA models help achieve these aims by making things more consistent, transparent, and measurable. To be effective, EA must ensure that all data, information, processes, architectures, and technologies are in line with the business. This necessitates ongoing maintenance of the enterprise architecture to keep everything up to date[32].

Comparative Table I highlights various approaches and methodologies for system and data integration to ensure scalability and security in enterprise architectures. It outlines five key studies, detailing their methodologies, performance outcomes, and limitations.

Table 1 Comparative Analysis of System and Data Integration Approaches for Scalability and Security in Enterprise Architectures

Ref.	Methodology	Performance	Limitations & Future Work
[29]	Vision for Enterprise Architecture (EA) 4.0, emphasising system integration and model management in Industry 4.0.	Improved information flow and integration across organisations and supply chains.	Lacks specific implementation details; future work includes developing a comprehensive model management and analytics platform.
[30]	Kernel-based security architecture with integrated risk, incident, and audit management systems.	High-performing architecture with features supporting security, sustainability, and flexibility.	Limited empirical validation requires further evaluation of long-term scalability and adaptability to rapidly changing enterprise environments.
[31]	Enterprise Architecture Frameworks (EAF) enhanced with precise	Promotes resilient enterprise strategies aligned with business	Limited focus on holistic enterprise-wide security practices; future work should address

	cybersecurity guidelines.	goals, extending beyond detection and prevention.	integrating end-to-end security measures to avoid exposure to risks.
[12]	Integration of Enterprise Architecture Management (EAM) with Risk Management (RM) and Information Security Management (ISM).	Facilitates RM and ISM by leveraging EA for improved information transparency and asset management.	Lacks real-world implementation case studies; future research should validate the integration model in diverse organisational contexts.
[32]	Proposal for constant maintenance of EA models to ensure synchronisation of data, processes, and technologies with business goals.	Enhanced transparency, measurability, and consistency, contributing to organisational success.	Requires ongoing resources and effort for maintenance; future work should focus on automation tools and frameworks for reducing maintenance overhead.

Conclusion and Future Scope

The integration of enterprise architectures is essential for aligning business objectives with IT capabilities, enabling organisations to remain competitive in dynamic markets. This paper has explored various system and data integration approaches that ensure scalability and security in enterprise architectures. By examining frameworks, methodologies, and security mechanisms, they have highlighted how integration enhances information accessibility, operational efficiency, and strategic alignment. Key scalability characteristics such as load, space, and structural scalability are critical for designing adaptable systems, while robust security mechanisms like authentication, encryption, and secure API management safeguard integrated architectures from vulnerabilities.

Future research can focus on developing automated tools and frameworks for enterprise architecture maintenance, reducing operational overhead while improving transparency and efficiency. Integration approaches can be enhanced with emerging technologies such as artificial intelligence, blockchain, and advanced analytics to strengthen decision-making and security.

References

[1] M. Thirasakthana and S. Kiattisin, "Sustainable government enterprise architecture framework," Sustain., 2021, doi: 10.3390/su13020879.

[2] Z. Zhou, Q. Zhi, S. Morisaki, and S. Yamamoto, "A Systematic Literature Review on Enterprise Architecture Visualization Methodologies," 2020. doi: 10.1109/ACCESS.2020.2995850.

[3] S. Kambhampaty and S. Chandra, "Enterprise architecture definition framework for IT service providers," IFIP Int. Fed. Inf. Process., 2006, doi: 10.1007/0-387-34456-x_27.

[4] A. Nakakawa, P. Van Bommel, and H. A. E. Proper, "Quality enhancement in creating enterprise architecture: Relevance of academic models in practice," in Lecture Notes in Business Information Processing, 2009. doi: 10.1007/978-3-642-01859-6_7.

[5] M. S. Rajeev Arora, "Applications of Cloud Based ERP Application and how to address Security and Data Privacy Issues in Cloud application," Himal. Univ., 2022.

[6] P. Ziegler and K. R. Dittrich, "Data Integration — Problems, Approaches, and Perspectives," in Conceptual Modelling in Information Systems Engineering, 2007. doi: 10.1007/978-3-540-72677-7_3.

[7] N. Mohamed, B. Mahadi, S. Miskon, and H. Haghshenas, "Information System Integration : A Review of Literature and a Case Analysis," no. March 2014, pp. 68–77, 2013.

[8] O. Odukoya, "The Transformative Impact of Cloud Computing on Small and Medium-sized Enterprises (SMEs): A Comprehensive Analysis," in 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), IEEE, May 2024, pp. 1–5. doi: 10.1109/SmartNets61466.2024.10577703.

[9] J. Whyte and A. Davies, "Reframing Systems Integration: A Process Perspective on Projects," Proj. Manag. J., 2021, doi: 10.1177/8756972821992246.

[10] S. R. M. Zeebaree, R. R. Zebari, K. Jacksi, and D. A. Hasan, "Security approaches for integrated enterprise systems performance: a review," Int. J. Sci. Technol. Res., 2019.

[11] M. Marian, A. Cusman, F. Stîngă, and D. Popescu, "A Digital Enterprise Architecture based on Cloud-Based Services and Digital Signatures," in 2024 25th International Carpathian Control Conference (ICCC), IEEE, May 2024, pp. 1–6. doi: 10.1109/ICCC62069.2024.10569192.

[12] T. Diefenbach, C. Lucke, and U. Lechner, "Towards an integration of information security management, risk management and enterprise architecture management - A literature review," in Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, 2019. doi: 10.1109/CloudCom.2019.00057.

[13] J. Faircloth, "Enterprise Applications Administration Teams," in Enterprise Applications Administration, 2014. doi: 10.1016/b978-0-12-407773-7.00007-7.

[14] A. and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 06, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.11.

[15] A. Malhotra, A. Elsayed, R. Torres, and S. Venkatraman, "Evaluate Canary Deployment Techniques Using Kubernetes, Istio, and Liquibase for Cloud Native Enterprise Applications to Achieve Zero Downtime for Continuous Deployments," IEEE Access, vol. 12, pp. 87883–87899, 2024, doi: 10.1109/ACCESS.2024.3416087.

[16] B. M., "Enterprise Architecture Frameworks: A Critique Review from a Security Perspective," Int. J. Comput. Appl., 2017, doi: 10.5120/ijca2017915416.

[17] Y. M. Maulana, Z. R. M. Azmi, and D. N. E. Phon, "Business-IT Alignment through Enterprise Architecture in a Strategic Alignment Dimension: A Review," 2023. doi: 10.26594/register.v9i1.3084.

[18] S. Deryabin, I. Temkin, U. Rzazade, and E. Kondratev, "Models and Methods of Designing Data-Centric Microservice Architectures of Digital Enterprises," Informatics, 2023, doi: 10.3390/informatics10010004.

[19] D. Hindarto, "Application Of Customer Service Enterprise Architecture In The Transportation Industry," J. Comput. Networks, Archit. High Perform. Comput., 2023, doi: 10.47709/cnahpc.v5i2.2744.

[20] Y. Gong and M. Janssen, "Roles and capabilities of enterprise architecture in big data analytics technology adoption and implementation," J. Theor. Appl. Electron. Commer. Res., 2021, doi: 10.4067/S0718-18762021000100104.

[21] I. Iswahyudi, D. Hindarto, and R. E. Indrajit, "Digital Transformation in University: Enterprise Architecture and Blockchain Technology," sinkron, 2023, doi: 10.33395/sinkron.v8i4.12977.

[22] A. Bondi, "Characteristics of Scalability and Their Impact on Performance," in Proceedings Second International Workshop on Software and Performance WOSP 2000, 2000, pp. 195–203. doi: 10.1145/350391.350432.

[23] S. Prakash, R. B. Patel, and V. K. Jain, "Secure , Scalable and Intelligent Model for Heterogeneous Wireless Ad Hoc Networks : a Review," vol. 3, no. 1, pp. 353–358, 2012.

[24] S. Murri, "Data Security Challenges and Solutions in Big Data Cloud Environments," Int. J. Curr. Eng. Technol., vol. 12, no. 6, 2022, doi: https://doi.org/10.14741/ijcet/v.12.6.11.

[25] V. José Carrillo, H. Danilo Jaramillo, S. Armando Cabrera, and M. Abad, "Including security mechanisms into systems architecture supporting vulnerabilities," in ICSTE 2010 - 2010 2nd International Conference on Software Technology and Engineering, Proceedings, 2010. doi: 10.1109/ICSTE.2010.5608751.

[26] K. Rabah, "Theory and Implementation of Data Encryption Standard: A Review," Inf. Technol. J., 2005, doi: 10.3923/itj.2005.307.325.

[27] M. Epping and M. Morowczynski, "Authentication and Authorization," IDPro Body Knowl., vol. 1, 2021, doi: 10.55621/idpro.78.

[28] 1Ayush Dewangan and 2Mr. G Raghavendra Prashad, "Integrated Threat Modelling," pp. 1–113, 2017, [Online]. Available: https://www.duo.uio.no/bitstream/handle/10852/55699/dae-thesis.pdf?sequence=1

[29] A. Aldea, M. E. Iacob, A. Wombacher, M. Hiralal, and T. Franck, "Enterprise architecture 4.0-A vision, an approach and software tool support," in Proceedings - 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference, EDOC 2018, 2018. doi: 10.1109/EDOC.2018.00011.

[30] M. T. U. Ahmed, N. I. Bhuiya, and M. M. Rahman, "A secure enterprise architecture focused on security and technology-transformation (SEAST)," in 2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017, 2018. doi: 10.23919/ICITST.2017.8356386.

[31] H. F. Al-Turkistani, S. Aldobaian, and R. Latif, "Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review," in 2021 1st International Conference on Artificial Intelligence and Data Analytics, CAIDA 2021, 2021. doi: 10.1109/CAIDA51941.2021.9425343.

[32] A. B. Costa and M. A. Brito, "Enterprise Architecture Management Constant maintenance and updating of the Enterprise Architecture," in Iberian Conference on Information Systems and Technologies, CISTI, 2022. doi: 10.23919/CISTI54924.2022.9820068.