International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

Evolution of Cloud Architecture for Global Corporate Learning Management Systems

Penmetsa Murali Krishna Raju*

Principal Learning Technology Administrator,CharlesRiver Laboratories,Charlotte, USA
Email:Raju.Penmetsa@CRL.com

Abstract

The article examines the evolution of cloud architecture in global corporate learning management systems as a response to the expansion of workforce training across dispersed organizational structures, hybrid work settings, cross-border compliance regimes, and continuous reskilling demands. The study aims to explain how architectural change has transformed the LMS from a centralized training platform into a distributed enterprise infrastructure embedded in broader systems of organizational capability. Its relevance stems from the growing dependence of multinational firms on digital learning environments that support scalability, resilience, integration, governance, and data protection. The novelty of the article lies in its synthesis of workplace learning research, cloud migration studies, software architecture scholarship, and data governance literature into a single sociotechnical account of LMS development. The article shows that the transition from on-premises systems to cloud-hosted legacy platforms, SaaS solutions, and cloud-native service ecosystems reflects a structural redefinition of enterprise learning infrastructure. The main findings indicate that cloud-native architectures provide stronger selective scaling, fault isolation, integration with HR and business systems, and support for analytics- and AI-based learning functions, while security, privacy, tenant isolation, and regulatory compliance remain constitutive design conditions. This article will be useful for researchers in digital education and information systems, enterprise architects, LMS developers, and corporate learning strategists.

Keywords: cloud architecture; learning management systems; corporate learning; cloud-native systems; SaaS; microservices.

Received: 3/24/2026
Accepted: 5/24/2026
Published: 6/2/2026

---

* *Corresponding author.*

1.Introduction

Corporate learning management systems have moved to the center of organizational capability because global firms now coordinate training across dispersed workforces, multiple legal regimes, diverse role profiles, and continuous skill renewal cycles. Research on workplace learning describes future work practices through collaboration, learning climate, stakeholder inclusion, and trust, placing digital learning infrastructures at the core of organizational adaptation [1]. This relevance became sharper under remote and hybrid work arrangements, where early professional adjustment, task mastery, and role clarity depend on sustained access to digital learning channels across time and location [2]. Evidence from workforce e-learning research also shows that digital training environments shape employee engagement with enterprise information systems and support knowledge acquisition in work settings, thereby providing LMS platforms with a direct link to operational performance and human capital development [3].

The strategic weight of LMS platforms in multinational corporations arises from scale and heterogeneity. A single corporate learning environment may need to serve onboarding, compliance, technical reskilling, leadership development, certification tracking, and partner education within a single governance framework. This burden increases when firms pursue digital transformation in workforce management, as the transformation of labor processes, decision flows, and performance systems depends on infrastructures that enable knowledge to circulate across business units and geographies [4]. Learning systems have also grown in functional breadth. Recent work on the development of immersive learning systems shows that contemporary learning environments combine pedagogical modeling, software engineering, domain knowledge, iterative prototyping, and reusable taxonomies, indicating that enterprise LMS ecosystems now operate as compound sociotechnical systems [5].

These pressures explain why cloud architecture became a decisive condition for global corporate LMS design. Legacy deployments face limits in scalability, maintainability, orchestration, and service evolution when learning demand fluctuates across regions and business cycles. A recent systematic review of cloud environments shows that contemporary architectural debate centers on trade-offs among performance, maintainability, deployment simplicity, orchestration overhead, and distributed complexity, which maps directly onto the design problems of enterprise learning platforms with global reach [6]. The move to the cloud also carries legal and governance consequences, as employee learning data, identity records, and assessment records fall under data protection requirements that must be managed across service layers and providers [7]. For that reason, cloud architecture entered the LMS domain as an infrastructural answer to elasticity, integration, availability, and compliance.

This study proceeds from the premise that the architectural evolution of corporate LMS platforms reflects the changing organizational, technical, and governance demands of global enterprise learning.

H1: The transition from on-premises and cloud-hosted legacy LMS platforms to cloud-native LMS architectures increases the capacity of global corporate learning systems to support scalability, fault isolation, selective service evolution, and enterprise-wide integration.

H2: The evolution of cloud architecture in global corporate LMS platforms has made security, privacy, tenant isolation, and regulatory compliance core architectural requirements that shape platform design alongside learning

functionality.

2.Materials and Methodology

The study of the evolution of cloud architecture for global corporate learning management systems is grounded in a focused review of recent scholarship drawn from workplace learning, digital transformation, cloud migration, modular and cloud-native software design, SaaS adoption, information security, data protection, and access governance. The material base comprises eleven sources that frame the LMS as a strategic enterprise infrastructure shaped by dispersed workforces, hybrid work arrangements, continuous reskilling, and cross-border governance demands. Future work and remote professional adjustment studies and organizational studies were included to capture the contextual antecedents leading to the elevation of digital learning systems in multinational enterprises Reference [1, 2]. Studies on workforce upskilling, digital transformation, and engaging learning systems construction were included to capture the further expansion of enterprise learning environment functional domains and their increasing adoption in operational capability formation [3, 4, 5]. The source base area also includes works on modular monoliths, cloud migration, cloud-native architectures, microservice elasticity, SaaS adoption, and context-aware access control. These works provide a framework, where LMSs evolve from legacy monolithic deployments to a distributed service ecosystem, which in turn becomes demanding of scalability, resilience, tenant isolation, and policy control [6, 8, 9, 10, 11, 12]. Regulatory and governance dimensions were addressed through research on GDPR compliance in cloud services, since employee learning records, identity data, and assessment traces circulate across jurisdictions and service layers within global LMS environments [7].

The methodological design combines conceptual synthesis, comparative architectural analysis, and structured interpretive review. Conceptual synthesis was used to connect organizational studies of learning and workforce adaptation with the software-architectural literature to explain why changes in corporate learning demand have generated pressure for infrastructural transformation in LMS design [1, 2, 4]. Comparative architectural analysis was applied to trace the movement from on-premises LMS deployments to cloud-hosted legacy systems, SaaS platforms, and cloud-native service compositions, with attention to scalability, maintainability, release coordination, selective scaling, integration capacity, and operational resilience as recurrent evaluative dimensions Reference [6, 8, 9, 10, 11]. A structured interpretive review was then used to examine how security, privacy, access management, and legal compliance condition the architecture of globally distributed learning systems, especially where multi-tenancy, employee data processing, and regional governance constraints intersect with platform design [7, 12]. This methodological configuration enables reading LMS evolution as a sociotechnical process in which architectural form, enterprise integration, and governance obligations develop along a shared historical trajectory.

3.Results and Discussion

The infrastructural pressures identified emerged from the design logic of traditional LMS platforms, which were built as on-premises enterprise systems with tightly coupled application layers and centralized operational control. In such environments, user management, course catalogs, assessment workflows, reporting functions, and administrative tools were assembled into a single deployable unit, reducing architectural separation and tying maintenance to the full application lifecycle. Recent research on cloud-era modular monoliths traces this lineage

to the persistence of simplified deployment models and direct codebase control inherited from earlier monolithic systems, while also documenting recurring difficulties in maintainability, release management, and service evolution as system scope expands [6]. For global corporations, these characteristics produced structural friction because the same LMS instance had to support geographically dispersed users, varied compliance regimes, and uneven demand peaks generated by onboarding cycles, certification deadlines, and regional training mandates. This design pattern also constrained global accessibility, since performance and availability were shaped by the physical concentration of infrastructure and by scaling practices that depended on manual provisioning and high capital expenditure. The result was a platform form that could sustain stable internal operations in bounded institutional settings, yet it imposed rising technical and financial strain when corporate learning became continuous, distributed, and data-intensive.

The move to cloud infrastructure followed from these limitations and began in many organizations with migration strategies that preserved the inherited application structure. Research on legacy-system modernization shows that rehosting, often described as lift-and-shift, remains a common first migration step because it lowers entry barriers, shortens transition time, and allows organizations to relocate critical workloads without immediate redesign of the software core [8]. For migrations from static deployment to containers and orchestration, availability, scalability and operational resilience were the primary drivers [9]. For LMSs, cloud migration also offers advantages such as disaster recovery, lower hardware refresh costs and extended service availability for multinational organizations. Deployment of the legacy LMS's application logic was often monolithic, leaving the LMS's release coordination, tenant isolation, integration, and selective scalability bottlenecks in place for the cloud. Cloud elasticity in microservices shows a similar problem, as compared to monolithic applications that represent a single entity, the components of the modern architecture have different workload profiles [10]. A cloud-hosted monolith could deliver infrastructure relief, though it cannot resolve the deeper mismatch between global learning operations and a tightly coupled software structure.

This mismatch helped drive the emergence of the SaaS LMS model as a dominant arrangement in corporate learning. Multi-tenant SaaS was serving multiple enterprise customers from a single application environment and specifically targeted the reduction of deployment times, shift of upgrade and maintenance responsibilities to the SaaS provider, and the service provider's capacity to support release cycles of multi-national user bases. A systematic literature review of SaaS adoption for use by enterprise identified cost, customization strategy, integration, and security as the major influence with multi-tenancy and data protection as the most frequent architectural consideration [11]. In corporate learning, this model aligned with the need for unified governance across subsidiaries and business units because one platform could support standard policy enforcement, global feature rollout, and coordinated analytics. At the same time, the SaaS turn introduced a new layer of architectural tension. Tenant isolation, privacy controls, and differentiated access management became central design requirements as heterogeneous organizations began sharing common service infrastructure. Recent work on advanced access management for multi-tenant environments treats tenant isolation, security, and privacy as primary criteria for platform design, which is directly relevant for LMS platforms that store employee identities, progress records, certifications, and assessment traces [12]. The evolution of LMS infrastructure models and their implications for global corporate learning are shown in Table 1.

Table 1: Evolution of LMS infrastructure models and their implications for global corporate learning

Architectural stage	Infrastructural model	Advantages	Limitations
Traditional on-premises LMS	Single, tightly coupled system with centralized control	Stable administration, direct infrastructure control	Limited scalability, difficult maintenance, high infrastructure cost, weaker global access
Cloud-hosted legacy LMS	Monolithic LMS moved to cloud without major redesign	Better availability, disaster recovery, broader reach	Persistent monolithic bottlenecks, weak selective scaling, integration limits
SaaS LMS	Multi-tenant platform managed by the provider	Faster deployment, lower maintenance burden, unified governance	Tenant isolation, privacy, access control, and customization challenges

The limits of multi-tenant SaaS platforms created the conditions for a deeper architectural shift toward cloud-native LMS design. In this model, the learning platform ceased to function as a single, cohesive software system and began operating as a constellation of bounded services, each responsible for a distinct domain of learning activity. Authentication, learner identity, course catalog management, content delivery, assessment processing, certification tracking, notifications, analytics, and recommendation logic could be separated into autonomous units with their own release cycles and scaling rules. This decomposition changed the LMS's internal logic from accumulated functional density to service granularity. It also altered the rhythm of platform evolution, since development teams could revise a single capability without forcing a synchronized change across the entire system. An API-first approach became central in this environment because service boundaries required stable and explicit communication contracts. The APIs allowed the LMS to become a platform for integration with HR systems, commercial content providers, collaboration systems, and external assessment engines. This resulted in a more modular architecture with greater fault isolation, shorter lead times for new features and updates, and a greater capacity to address regional business requirements.

Containerization gave this architectural shift its operational form. Services that once depended on fragile server-specific configurations can now run within standardized execution environments, reducing deployment friction across testing, staging, and production landscapes. Docker became useful as a packaging layer because it encapsulated code, dependencies, and runtime settings into a single, reproducible artifact. Kubernetes extended this design with an orchestration layer that delivered deployment and service discovery mechanisms, as well as health checking, self-healing and load balancing at scale across clusters. This was important for large company LMSs, as they experienced traffic spikes corresponding with compliance campaigns, onboarding sessions or enterprise certification cycles, straining their existing deployments. Orchestration allowed the platform to absorb such spikes through automated scaling. It also simplified regional deployment strategies, since the same service

stack could be replicated across geographic zones with fewer environment-specific adjustments. DevOps practices and continuous integration pipelines gave these systems a disciplined delivery process in which testing, packaging, deployment, and rollback were part of a single repeatable chain. This operational regime shortened release intervals and reduced the institutional cost of change.

Global performance became a defining concern once the LMS matured into a distributed cloud-native platform. International corporations depend on stable access across time zones, network conditions, and device types, yet latency can erode the learning experience when content and application logic remain distant from the learner. Cloud architecture avoided the problem through use of regional infrastructure, CDNs, edge-networking, and separating static resources from transactional services. Video lectures, mobile learning packages, simulations, and other interactive content were cached and served by infrastructure geographically close to the user. Learner-specific actions, such as tracking progress, submitting assessments, and grading, were executed by backend services. This distinction improved response times and reduced pressure on the core application layer. User experience also depended on localization at the interface, content, and data levels. A global LMS had to support multilingual navigation, region-specific compliance content, local date and time formats, and differentiated learning paths aligned with legal or cultural context. These requirements pushed architecture beyond performance engineering alone and tied it to the social geography of enterprise learning, where access, language, and responsiveness shape the platform's credibility. The advantages of cloud-native LMS architecture are summarized in Figure 1.

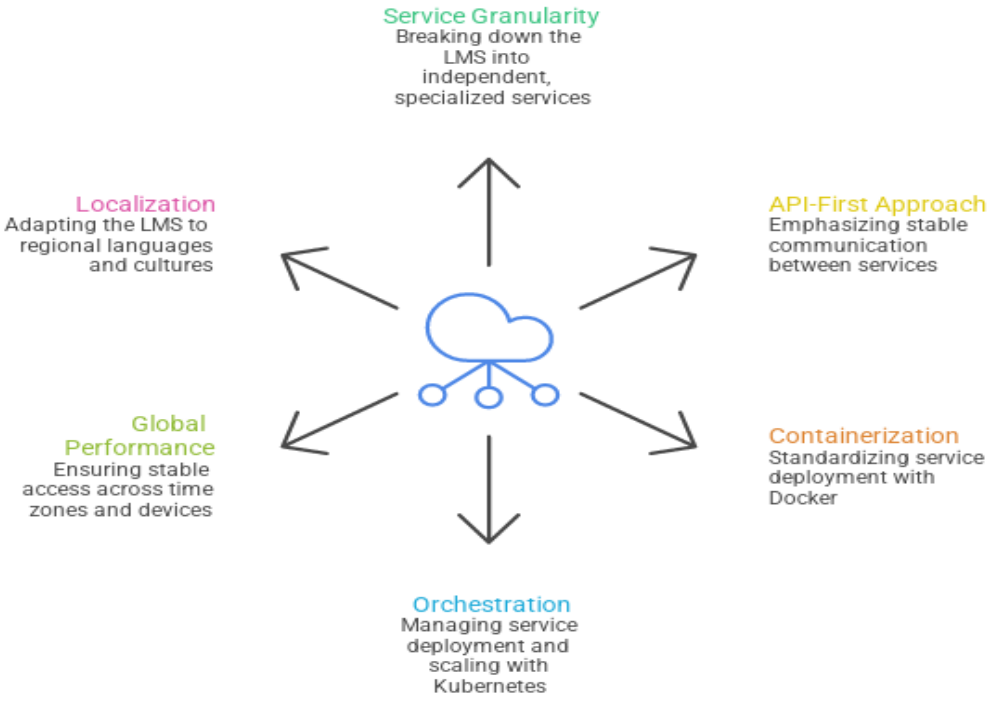

Figure 1: Advantages of Cloud-Native LMS Architecture

As cloud-native LMS platforms matured, their value depended on the quality of their integration with the broader corporate technology landscape. A learning system operating in isolation could store courses and completion

records, yet it could not reflect the full movement of employees through the organization or respond to changes in role, performance, or business demand. Integration with the HRIS enabled synchronization of employee profiles, organizational hierarchies, job families, and onboarding status. Connections with CRM and ERP environments opened a path for training linked to sales readiness, product knowledge, operational procedures, and compliance tasks embedded in business workflows. Collaboration tools extended the LMS into employees' daily communication spaces, where learning could occur in meetings, channels, project spaces, and knowledge exchanges. In this setting, APIs and middleware became the connective tissue of the digital learning ecosystem. They supported data exchange across systems with different structures, release cycles, and governance rules. The LMS therefore evolved from a destination platform into a nodal platform within a larger enterprise learning fabric. A promotion could trigger leadership training. A new product launch could assign role-specific modules to sales teams. A regulatory change could trigger certification workflows across multiple regions. Such integration scenarios gave the LMS a stronger organizational presence and tied learning to the real tempo of enterprise activity.

This shift in integration reshaped the internal meaning of LMS data. Earlier systems focused on completion logs, quiz scores, and administrative reports produced for audits or managerial review. In a distributed learning ecosystem, data began to circulate across operational and analytical layers, which changed both its volume and its interpretive value. Learning records could be combined with workforce, performance, and mobility data inside data lakes or warehouse environments designed for cross-system analysis. This made it possible to move from retrospective reporting toward learning analytics centered on behavior, progression, and capability formation. The platform could trace how learners navigated content, how they returned to specific materials, where they paused, which assessments led to repeated failure, and how skill profiles shifted over time. Such signals supported more precise decisions in HR and learning and development. Managers could identify emerging skill gaps inside teams. Learning leaders could identify weaknesses in course design. Talent functions could connect training pathways with internal mobility, succession planning, and capability planning. The LMS thus became a generator of organizational intelligence whose data value depended on interoperability, storage architecture, and analytic coherence.

This growth in integration and data intensity raised the stakes of security, privacy, and compliance across the entire architecture. A global corporate LMS processes employee identities, job information, learning histories, certification outcomes, and assessment traces that may affect career movement, audit exposure, or legal accountability. Such data requires layered protection across access, transmission, storage, and processing. Identity and access management established control over who could enter the platform and which resources each user could access. Single sign-on reduced credential fragmentation across enterprise applications. Multi-factor authentication secures privileged accounts and other high-risk workflows. Encryption protects data in transit and at rest, through in-house and external data integrations. Global organizations deal with data residency scenarios where keeping employee records must be compliant with national or sector-specific regulations, concerning where to store, who can access and where can they be transferred. Regulatory obligations such as GDPR include retention, consent management, subject access requests and auditability. In this environment, security ceased to be a peripheral technical layer and became a structural condition of the LMS as an enterprise platform. The more deeply learning systems entered the corporate ecosystem, the more they had to function as governed

infrastructures for trusted data exchange. The integration process of cloud-native LMS platforms is shown in Figure 2.

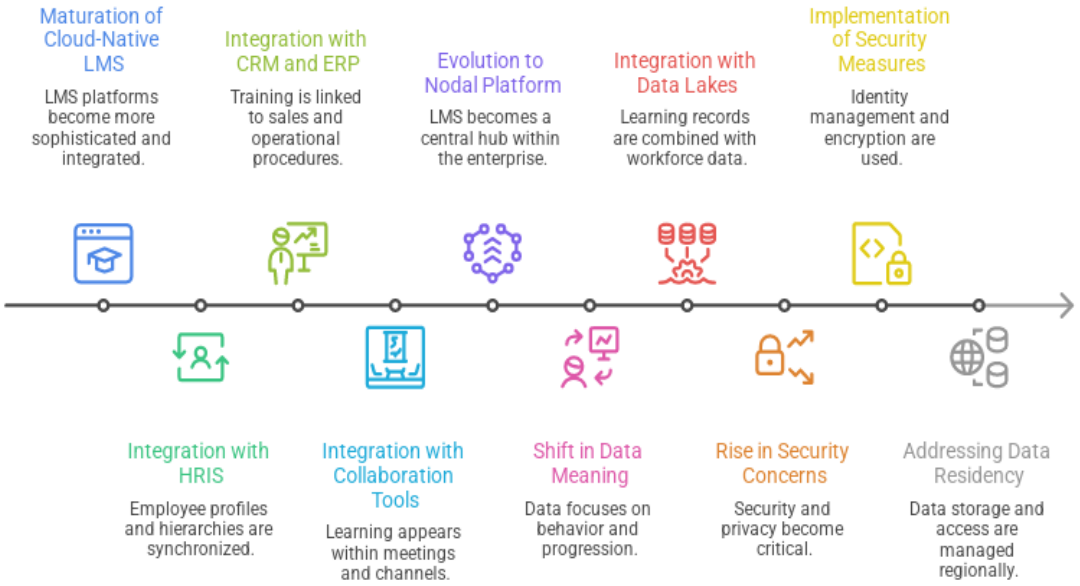

Figure 2: Integration Process of Cloud-Native LMS Platforms

The expansion of integration, analytics, and governance created the conditions for the incorporation of artificial intelligence into LMS architecture. AI transformed the platform from a system that delivered assigned content into one that interpreted learner signals and generated adaptive responses. Recommendation engines could map learning paths to role profiles, prior activity, certification status, and inferred skill needs. Intelligent search reduced dependence on rigid catalog navigation by connecting queries with semantic relations across courses, documents, and knowledge objects.

These characteristics were then employed in digital assistants with conversational content discovery, procedure guidance, and task-based moments of learning, embedded at the point of need. Predictive analytics further extended the LMS with insights relating to disengagement, delayed completion of requirements, skill decay and readiness to transition into new roles. Skills intelligence consists of behavioral data, assessment evidence, workforce taxonomies, and organizational demand signals. This shift imposed new architectural requirements. AI-enabled LMS platforms required pipelines for continuous data ingestion, storage layers suited to heterogeneous data, model training and inference services, vector-based retrieval, feedback loops for recommendation quality, and governance mechanisms for transparency, bias control, and model monitoring. The architecture of the LMS thus moved further away from the bounded logic of the course platform and toward the layered logic of an intelligent learning environment.

These changes point toward a future in which global corporate LMS platforms become more composable, event-driven, automated, and observable. With composable architecture the ecosystem becomes easier to assemble. Learning ecosystems with interoperable services for content, credentialing, skill assessments, analytics,

conversational assistants, etc., offer more freedom to the enterprise in deciding how best to compose the elements of the platform, within a set of global standards and the local context. Event-driven systems further this flexibility. Learning can respond to business events such as a new staff appointment, internal promotion, a role change, project allocation, compliance with new regulation, and performance feedback.

Greater automation extends across provisioning, deployment, scaling, policy enforcement, and content workflows, reducing operational burden and shortening response time to organizational change. Observability becomes essential in this environment because distributed services require continuous visibility into latency, failure propagation, user behavior, model drift, data quality, and regional system health. Adaptive learning ecosystems are gaining importance within this architectural horizon because enterprise learning now depends on systems that can sense context, interpret signals, and reshape pathways in response to workforce movement and business volatility. The future cloud architecture of global LMS platforms will be defined by modular intelligence, responsive infrastructure, and sustained alignment between technical design and the changing morphology of organizational learning.

The scope of this researchis bounded by its design as a conceptual and comparative synthesis drawn from a curated corpus of eleven peer-reviewed sources, which fixes the analytical aperture around architectural transitions documented in that body of work. The investigation proceeds through interpretive review of secondary literature, which situates the findings within the register of structural argumentation and leaves quantitative magnitudes of latency, fault containment, and cost displacement to adjacent empirical programs. The sociotechnical orientation directs attention toward the convergence of organizational, architectural, and governance trajectories, with pedagogical efficacy and instructional design belonging to complementary lines of research. The temporal envelope of the cited material extends from 2020 through 2025, which locates the architectural horizon within a defined historical interval and opens space for follow-up work on generative AI integration, agentic learning systems, and post-microservice paradigms as those domains mature.

3.Conclusion

The evolution of cloud architecture for global corporate learning management systems reveals a structural transition in the role of enterprise learning infrastructure within multinational organizations. LMS platforms emerged as central elements of organizational capability because they support workforce development across dispersed personnel, heterogeneous regulatory settings, differentiated job functions, and recurrent cycles of reskilling. The analyzed material shows that this expansion in strategic relevance placed growing pressure on inherited architectural models. Traditional on-premises systems could sustain controlled institutional settings, yet their tightly coupled design generated mounting friction under conditions of global scale, fluctuating demand, and data-intensive learning operations. The first wave of cloud migration reduced this burden by enabling broader availability, stronger disaster recovery, and reduced reliance on hardware, though monolithic application logic preserved critical constraints in release coordination, selective scaling, and integration. The architectural problem of the corporate LMS is a matter of the architecture of the platform and its ability to accommodate the complexities of modern enterprise learning.

The transformations of the LMS as sociotechnical system are further accelerated by Software as a Service and

cloud-native LMS. SaaS is often multi-tenant, so the rapid rollout, provider-influenced maintenance cycle, and continual governance drive streams through the various subsidiaries and business units inside the organization. Delegated authorities enforce policy and coordinate analytics. At the same time, shared infrastructure intensified the importance of tenant isolation, privacy safeguards, access control, and customization logic. These tensions created the conditions for cloud-native decomposition, in which the LMS ceased to operate as a single functional block and evolved into a distributed arrangement of bounded services connected via API-based communication. Within this model, authentication, catalog management, assessment processing, certification tracking, analytics, and recommendation functions could evolve through separate release cycles and differentiated scaling rules. Containerization, orchestration, and DevOps pipelines gave this architecture operational coherence through reproducible deployments, workload balancing, automated recovery, and shorter release intervals. The result was an LMS architecture with stronger fault isolation, higher adaptive capacity, and greater alignment with the temporal and geographic variability of global learning demand.

The discussion further shows that the mature cloud-native LMS derives its value from integration, data circulation, governance, and intelligence layers that extend far beyond course delivery. More considerably, however, these interconnections between HRISs, CRM systems, ERP systems and collaboration environments with LMSs enabled a central platform within the corporate technology ecosystem for training to respond to promotions, onboarding, regulatory requirements, product releases, and business model changes that is more wide-ranging than simply tracking course completion. Then developed into cross-system analytics for behavioral performance, capability development, and workforce mobility. Such growth in interoperability also raised the stakes of security, privacy, data residency, and compliance, making governed data exchange a constitutive property of the platform. Within this architectural horizon, the incorporation of artificial intelligence marks the next stage of development, since recommendation engines, intelligent search, predictive analytics, and skills intelligence depend on continuous data pipelines, model services, retrieval layers, and mechanisms for transparency and monitoring.

The study confirms both hypotheses. Hypothesis 1 is supported by the comparative analysis of architectural stages, which shows that cloud-native LMS architectures provide stronger scalability, service-level fault isolation, independent release cycles, API-based interoperability, and closer alignment with the variable demands of global learning operations than on-premises and cloud-hosted legacy systems. Hypothesis 2 is also supported, as the article demonstrates that expanding multi-tenancy, cross-system integration, analytics, and cross-border data processing places security, privacy, access control, tenant isolation, and regulatory compliance at the center of the architectural design of global corporate LMS platforms. The article concludes that the future of global corporate LMS architecture lies in composable, event-driven, observable, and intelligent infrastructures, whose design must remain tightly coupled to the evolving morphology of organizational learning, workforce movement, and enterprise governance.

4.Funding

No financial support received.

5.Competing Interests

The authors declare no competing interests.

6.Author Contributions

The authors contributed solely to the conception, design, writing, and approval of the final manuscript.

7.Ethics and Transparency Statement

The manuscript is an honest and accurate account of the study; no key details omitted; ethical practices followed.

References

[1] A. Svensson, U. Lundh Snis, and I. Bernhard, "Guest editorial: Learning capabilities for future work practices," *Journal of Workplace Learning*, vol. 35, no. 6, pp. 465–469, 2023, doi: 10.1108/jwl-08-2023-198.

[2] M. Karlsson, O. Z. Mårs, B. Jenner, and E. Frögéli, "Effect of working remotely on new professionals' learning and adjustment during the first five weeks after professional entry," *Journal of Workplace Learning*, vol. 37, no. 2, pp. 93–113, 2024, doi: 10.1108/jwl-04-2024-0079.

[3] P. Bitrián, I. Buil, S. Catalán, and D. Merli, "Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours," *Journal of Business Research*, vol. 179, 2024, Art. no. 114685, doi: 10.1016/j.jbusres.2024.114685.

[4] S. Akter, K. Biswas, D. Vrontis, C. L. Cooper, and S. Y. Tarba, "Mastering digital transformation in workforce management," *Production Planning & Control*, vol. 35, no. 13, pp. 1525–1532, 2023, doi: 10.1080/09537287.2023.2270465.

[5] K. A. Mat Sanusi, D. Majonica, D. Iren, N. Fanchamps, and R. Klemke, "MILSDeM: Guiding immersive learning system development and taxonomy evaluation," *Education and Information Technologies*, vol. 29, pp. 16283–16316, 2024, doi: 10.1007/s10639-024-12479-4.

[6] L. F. Al-Qora'n and A. A.-S. Ahmad, "Modular monolith architecture in cloud environments: A systematic literature review," *Future Internet*, vol. 17, no. 11, 2025, Art. no. 496, doi: 10.3390/fi17110496.

[7] M. E. Cambronero, M. A. Martínez, J. L. de la Vara, D. Cebrián, and V. Valero, "GDPRValidator: A tool to enable companies using cloud services to be GDPR compliant," *PeerJ Computer Science*, vol. 8, 2022, Art. no. e1171, doi: 10.7717/peerj-cs.1171.

[8] M. Aslam et al., "Cloud migration framework clustering method for social decision support in modernizing the legacy system," *Transactions on Emerging Telecommunications Technologies*, vol. 35,

no. 4, 2023, Art. no. e4863, doi: 10.1002/ett.4863.

[9] B. Nascimento, R. Santos, J. Henriques, M. V. Bernardo, and F. Caldeira, "Availability, scalability, and security in the migration from container-based to cloud-native applications," *Computers*, vol. 13, no. 8, 2024, Art. no. 192, doi: 10.3390/computers13080192.

[10] M. H. Fourati, S. Marzouk, and M. Jmaiel, "Cloud elasticity of microservices-based applications: A survey," *Concurrency and Computation: Practice and Experience*, vol. 37, no. 2, 2024, Art. no. e8329, doi: 10.1002/cpe.8329.

[11] O. A. Adenuga, R. M. Kekwaletswe, and O. T. Adenuga, "A systematic literature review to uncover SaaS adoption issues by SMEs – Reasons and solutions to the adoption problem," *International Journal for Digital Society*, vol. 11, no. 2, pp. 1645–1653, 2020, doi: 10.20533/ijds.2040.2570.2020.0205.

[12] P. Nguyen, H.-H. Nguyen, P. Phung, H.-L. Truong, and T. Cheung, "Advanced context-sensitive access management for edge-driven IoT data sharing as a service," *ACM Transactions on Internet Technology*, vol. 25, no. 2, pp. 1–31, 2025, doi: 10.1145/3721430.