International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

LMS Cybersecurity in the Age of AI: Rethinking Resilience in Higher Education

Serap Uğur

Asst. Prof. Dr., Anadolu University, Türkiye

Abstract

The rapid digital transformation of higher education and the integration of artificial intelligence (AI) into Learning Management Systems (LMSs) have expanded institutional cyber risk surfaces. While enterprise cybersecurity emphasizes infrastructure hardening and zero-trust models, LMS-focused scholarship remains dispersed across governance, behavioral, and AI-mediated domains. This study synthesizes peer-reviewed research published between 2020 and 2025 (N = 30) to examine the structural orientation of LMS cybersecurity in higher education. Bibliometric and thematic analyses reveal structural fragmentation and sociotechnical asymmetry: human and governance dimensions dominate, while empirically validated technical controls and AI-driven adaptive defenses remain underdeveloped. AI is primarily framed as an integrity and monitoring tool rather than as a core security mechanism. In response, the study advances the LMS Multilayer Resilience Architecture (LMRA), conceptualizing LMS cybersecurity as a bidirectionally interdependent sociotechnical system integrating governance, behavioral, AI-mediated, and technical layers. Rather than a technical blueprint, LMRA offers a conceptual resilience framework for coordinated cross-layer security. As generative AI and platform dependence intensify, LMS cybersecurity must evolve from isolated defenses toward systemic multilayer resilience.

Keywords: LMS, Learning Management Systems, Cybersecurity, Data Protection, Higher Education, Educational Technologies

1. Introduction

Learning Management Systems (LMSs) have evolved from auxiliary digital repositories in the late 1990s into mission-critical infrastructures underpinning higher education. Initially designed to distribute course materials and manage communication, LMS platforms progressively integrated assessment tools, grade management systems, analytics dashboards, cloud-based services, and mobile functionalities. Following the rapid digital transformation accelerated by the COVID-19 pandemic, LMS environments transitioned from supplemental learning tools to central institutional ecosystems mediating identity management, remote assessment, academic integrity monitoring, and large-scale data governance (Bradley, 2021; Sharma et al, 2025; Uğur & Kurubacak, 2019).

The integration of artificial intelligence (AI), generative systems, and predictive analytics has further intensified the complexity of LMS environments. Contemporary LMS platforms now function as sociotechnical infrastructures in which pedagogical processes, governance frameworks, behavioral practices, and technical security controls intersect. As a result, cybersecurity challenges in LMS contexts extend beyond conventional infrastructure protection to encompass issues of academic trust, institutional compliance, behavioral risk, and AI-mediated decision-making.

Despite increasing scholarly attention, LMS cybersecurity research remains conceptually fragmented. Studies tend to isolate technical hardening, behavioral compliance, policy design, or AI-driven monitoring mechanisms rather than examining how these elements interact systemically. In an era characterized by AI expansion and heightened cyber vulnerability, there is a pressing need to reconceptualize LMS security not as a discrete technical function but as a multilayer resilience architecture emerging from cross-layer coordination.

This study responds to that need by synthesizing recent research (2020–2025) and advancing the concept of a LMRA, positioning resilience as an emergent property of interdependent governance, behavioral, AI-mediated, and technical layers within higher education ecosystems.

Given the observed conceptual fragmentation and imbalance, this study addresses the following research questions:

- How has LMS cybersecurity research in higher education evolved in the context of accelerated AI integration between 2020 and 2025?
- What thematic and structural patterns characterize the current intellectual landscape of LMS cybersecurity scholarship?
- To what extent are governance, human, AI-mediated, and technical dimensions integrated within existing research?
- What structural discontinuities or imbalances persist across these dimensions?
- How can these patterns be synthesized into a multilayer resilience architecture for LMS cybersecurity in higher education?

2. THEORETICAL FRAMEWORK

The conceptual foundation of this study is grounded in sociotechnical systems theory and resilience governance literature. Sociotechnical systems theory posits that organizational outcomes emerge from the reciprocal interaction between social subsystems (e.g., human behavior, institutional norms) and technical subsystems (e.g., infrastructure, automation) (Bostrom & Heinen, 1977; Trist et al, 1988). In this perspective, neither social nor technical elements operate independently; system performance and vulnerability are co-constructed across layers.

Contemporary cybersecurity scholarship increasingly adopts resilience-oriented approaches emphasizing adaptive capacity, cross-layer coordination, and continuous monitoring rather than static perimeter defense (NIST, 2023; European Commission, 2022). Resilience, in this context, refers not merely to breach prevention but to the system's capacity to anticipate, withstand, adapt to, and recover from disruptions.

Within higher education, LMS environments embody complex sociotechnical ecosystems. Governance structures establish compliance frameworks and accountability boundaries; users enact policies through behavioral practices; AI systems mediate monitoring and predictive analysis; and technical controls implement authentication and infrastructure-level defense. However, the literature has largely examined these components separately.

LMS Cybersecurity as a Sociotechnical Ecosystem

This study is grounded in sociotechnical systems theory, which posits that organizational performance and system resilience emerge from the interaction between technical infrastructure and social subsystems (Bostrom & Heinen, 1977). Within LMS environments, vulnerabilities rarely originate from technical architecture alone; they emerge from the dynamic interplay between system configurations, user practices, institutional policies, and adaptive technologies.

Unlike enterprise IT systems governed primarily by centralized control, LMS platforms are pedagogically mediated environments characterized by distributed agency. Students upload assignments, faculty configure assessments, administrators adjust permissions, and AI tools generate feedback. Each action creates potential attack surfaces.

Therefore, LMS cybersecurity must be conceptualized not as a single-layer defense stack but as an interdependent ecosystem.

Human-Centric Security and Behavioral Risk

Contemporary cybersecurity literature increasingly recognizes human behavior as a primary risk vector (Bada & Nurse, 2019). In higher education contexts, behavioral vulnerabilities manifest as:

- Weak password practices
- Academic misconduct via AI tools
- Oversharing of credentials
- Low digital security awareness

Academic integrity research further demonstrates that technological enforcement mechanisms alone cannot ensure compliance without trust and ethical alignment (Denisova-Schmidt, 2016; Holmes, 2017).

Thus, human and behavioral dimensions function not merely as peripheral factors but as core determinants of LMS resilience.

AI as Dual-Use Security Infrastructure

AI technologies introduce a paradox in LMS security. On one hand, AI-assisted proctoring, anomaly detection, and predictive analytics enhance monitoring capabilities. On the other hand, generative AI introduces new integrity risks and automated exploitation possibilities (Gangavarapu, 2025).

This dual-use characteristic positions AI as both:

- A vulnerability amplifier

- A security multiplier

The theoretical implication is that AI must be conceptualized as a mediating adaptive layer rather than a purely pedagogical tool.

Governance and Institutional Resilience

Cybersecurity governance frameworks emphasize policy alignment, compliance standards, and risk management cycles (NIST, 2023; European Commission, 2022). In LMS contexts, governance defines:

- Access hierarchies
- Data retention policies
- Incident response procedures
- Academic integrity enforcement mechanisms

Governance structures thus function as foundational constraints that shape both technical implementation and user behavior.

However, existing literature rarely integrates governance with technical and behavioral layers within a unified model.

Theoretical Gap and Need for Integration

Current scholarship treats LMS cybersecurity dimensions in isolation:

- Technical hardening studies rarely engage governance theory.
- Behavioral studies seldom integrate AI-adaptive security.
- AI research often ignores infrastructure-level defense architecture.
- Policy analyses remain conceptually detached from system validation.
- This theoretical disaggregation limits explanatory power.

The LMRA conceptualizes cybersecurity as emerging from dynamic interdependence among four interacting layers: governance and policy foundations, human and behavioral dynamics, AI-mediated adaptive mechanisms, and technical security controls. Rather than representing a prescriptive blueprint, LMRA functions as a structural synthesis derived from observed fragmentation within the literature, aligning with resilience governance paradigms that prioritize cross-layer integration.

3. METHODS

Research Design

This study adopted a structured integrative synthesis design combining bibliometric mapping and qualitative thematic analysis to examine the intellectual structure and conceptual orientation of LMS cybersecurity research in higher education. Rather than conducting a purely descriptive review, the study sought to identify structural patterns, thematic imbalances, and inter-domain relationships within the literature. The methodological approach is grounded in integrative review principles, which allow the

combination of quantitative mapping techniques with interpretive thematic synthesis to generate conceptual advancement (Snyder, 2019).

The research design was structured in three sequential stages. First, a systematic retrieval and screening process was conducted to define the corpus. Second, bibliometric mapping techniques were applied to identify structural trends, citation anchors, and keyword clusters. Third, an iterative coding and synthesis procedure was used to derive cross-dimensional insights and inform the development of the LMRA. This mixed analytical strategy enabled both structural visualization and conceptual integration.

Data Sources and Search Strategy

To ensure coverage of high-quality peer-reviewed scholarship, data were collected from two major citation databases: Web of Science Core Collection and Scopus. These databases were selected due to their rigorous indexing standards, citation tracking capabilities, and comprehensive coverage of interdisciplinary research.

The search strategy was developed to capture studies addressing LMS security within higher education contexts while avoiding overgeneralized cybersecurity literature unrelated to educational platforms. Boolean combinations of key constructs were used, including variations of "Learning Management System" or "LMS," combined with "cybersecurity," "data security," or "information security," and restricted to "higher education" contexts. The search was limited to publications between 2020 and 2025 to capture research reflecting the rapid digital acceleration following the COVID-19 pandemic and the subsequent integration of AI technologies into LMS environments.

The search strings were iteratively refined to balance sensitivity and specificity, ensuring inclusion of relevant studies without inflating results with peripheral cybersecurity literature. Only English-language peer-reviewed articles and review papers were considered.

Screening and Eligibility

The initial database search yielded 40 records across both databases. Following retrieval, duplicate entries were identified and removed through DOI comparison and title-year matching procedures, resulting in a final corpus of 30 unique studies.

Eligibility screening was conducted in two stages. In the first stage, titles and abstracts were reviewed to assess alignment with the study's focus. In the second stage, full-text examination was conducted where relevance was ambiguous. Studies were included if they explicitly addressed security-related dimensions within LMS environments in higher education settings. Eligible publications comprised empirical studies, conceptual analyses, and systematic reviews directly engaging with cybersecurity, data protection, academic integrity enforcement, AI-based security mechanisms, or governance frameworks within LMS contexts.

Studies were excluded if they focused on LMS usability without security implications, addressed cybersecurity in non-educational contexts, were limited exclusively to K–12 settings, or consisted of editorials, opinion pieces, or non-research commentary.

Data Extraction and Thematic Coding

An iterative coding framework was developed to classify studies according to dominant security dimensions and conceptual orientations. The coding scheme was constructed inductively during initial reading and subsequently refined to ensure analytical clarity.

The framework included the following analytical dimensions: technical security controls, human and behavioral factors, AI-mediated security mechanisms, governance and policy structures, and explicit threat landscape focus. Each study was coded based on its primary analytical emphasis, while allowing for cross-category tagging when multiple dimensions were substantively addressed.

Coding was conducted through abstract-level screening and extended to full-text examination when necessary to determine conceptual orientation. This process enabled identification of thematic dominance, dimensional imbalance, and cross-layer integration patterns across the corpus.

Bibliometric Analysis Procedures

Bibliometric analysis was employed to identify structural characteristics of the field. Publication trend analysis was conducted to examine temporal distribution patterns between 2020 and 2025. Keyword co-occurrence mapping was performed to identify thematic clusters and dominant conceptual linkages. Co-authorship network analysis was applied to examine institutional and country-level collaboration structures, revealing the geographic and organizational distribution of knowledge production.

Citation anchor analysis was conducted to determine which publications exerted the greatest intellectual influence within the dataset. Rather than simply reporting citation counts, anchor studies were analyzed qualitatively to identify their thematic orientation and conceptual positioning. This allowed the study to assess whether intellectual influence aligned with technical, behavioral, AI-driven, or governance-focused narratives.

Architectural Derivation Logic

The LMRA was derived through a structured synthesis process integrating bibliometric findings with thematic coding results. The derivation procedure involved identifying structural imbalances across dimensions, examining the thematic orientation of highly cited anchor publications, and synthesizing cross-layer conceptual gaps.

Rather than imposing a predefined theoretical structure, the framework emerged inductively from observed fragmentation patterns within the literature. Sociotechnical systems theory provided the interpretive lens guiding integration, allowing the positioning of governance, human behavior, AI-mediated adaptation, and technical controls within a bidirectionally interdependent architecture.

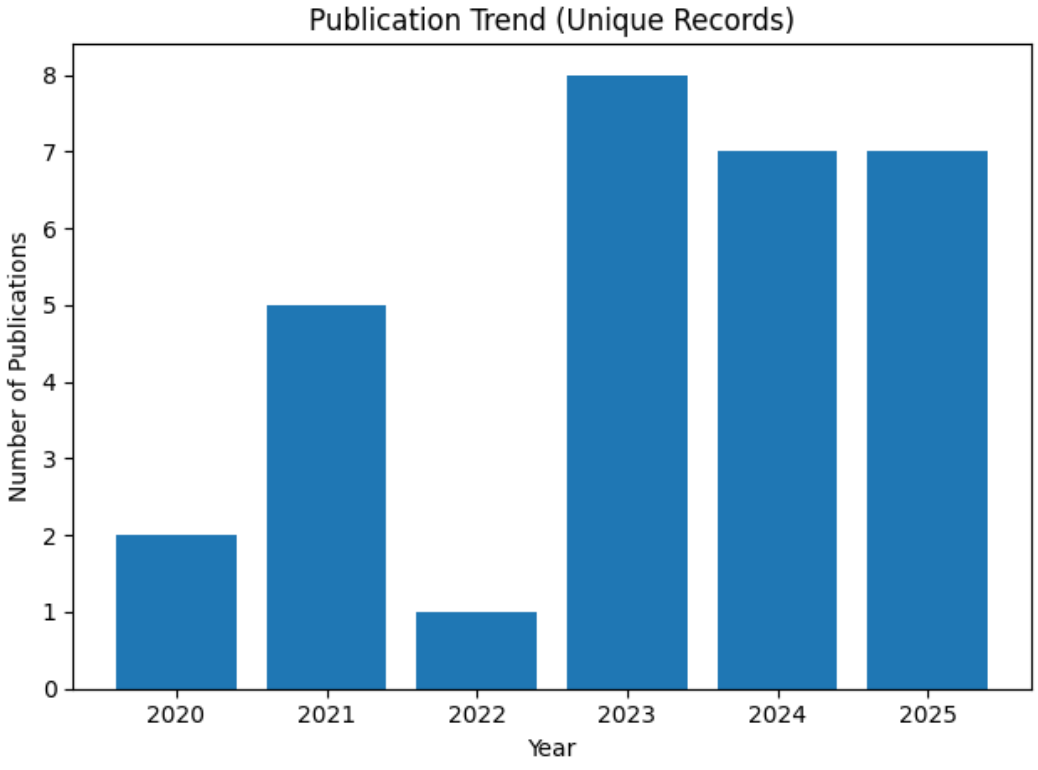
The LMRA was inductively derived through the convergence of bibliometric dispersion patterns, thematic asymmetry, citation anchor orientation, and gap synthesis. The architecture does not claim empirical validation but represents a conceptual integration responsive to documented structural fragmentation.

4. RESULT

Bibliometric Evolution and Structural Fragmentation of the Field

While the corpus size is modest, the dispersion across journals, weak co-authorship density, and thematic asymmetry collectively indicate early-stage structural dispersion rather than mature consolidation. The bibliometric synthesis of 30 unique studies published between 2020 and 2025 indicates a steadily increasing research trajectory, with a pronounced rise after 2022. This post-2022 acceleration is consistent with two interlocking dynamics in higher education: the normalization of platform-mediated teaching and assessment after the COVID-19 pivot, and the expansion of cyber risk surfaces as LMS infrastructures became mission-critical systems for instruction, identity management, assessment, and institutional data flows (Bosiu, 2025; Karras et al, 2025). In this period, LMS platforms evolved beyond content delivery to become integrated ecosystems incorporating learning analytics, cloud services, remote assessment, and AI-enabled functionalities—each introducing new vulnerabilities and governance demands. Figure 1 visualizes this temporal trend.

Figure 1. Publication trends in LMS cybersecurity research (2020–2025).



Note. Annual distribution of publications included in the final corpus (N = 30).

Importantly, growth in publication volume does not necessarily signal conceptual maturation. Despite rising output, the field shows persistent structural fragmentation. The included studies are distributed across 28 journals, indicating the absence of a consolidated disciplinary hub and suggesting that LMS cybersecurity remains positioned at the intersection of computer science, educational technology, institutional governance, and AI ethics. Comparable fragmentation patterns have been reported in adjacent domains of educational cybersecurity and interdisciplinary digital risk research, where scattered

publication outlets reflect emergent rather than stabilized knowledge structures (Bahmanova & Lace, 2024; Dhawan et al, 2024).

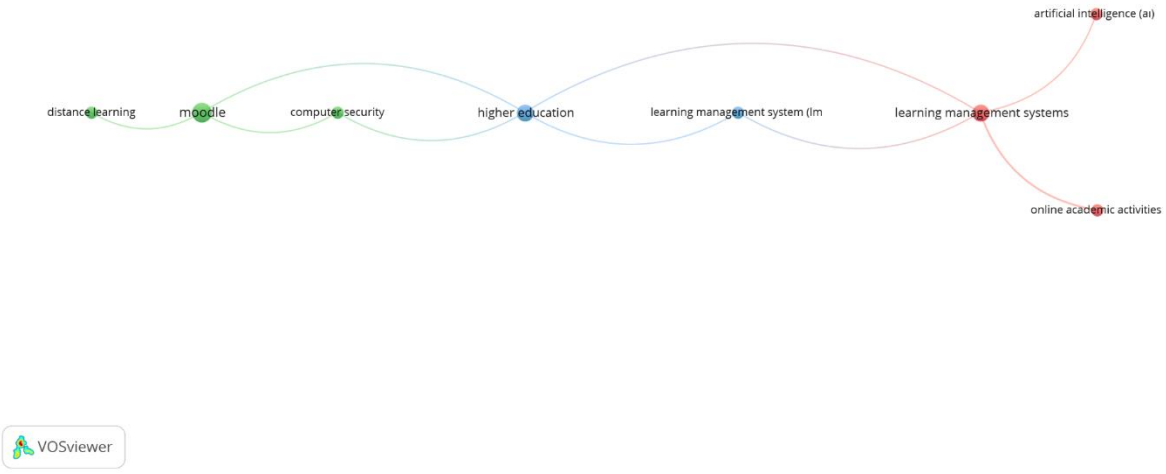
This dispersion implies that LMS cybersecurity is currently developing as a cross-disciplinary concern with diverse entry points (technical controls, policy, integrity, AI monitoring) rather than as a mature domain characterized by shared constructs, dominant methods, and stable research programs.

To examine the field's conceptual organization and its underlying collaboration structure more directly, we analyzed (a) keyword co-occurrence networks and (b) co-authorship networks at country, organization, and author levels for both WoS and Scopus datasets using VOSviewer.

Keyword Co-occurrence Structure in Web of Science

To examine the intellectual structure of the field, keyword co-occurrence networks were generated using VOSviewer. Figure 2 presents the Web of Science keyword co-occurrence network.

Figure 2. Keyword co-occurrence network of LMS cybersecurity research (Web of Science dataset, 2020–2025).



Note. Nodes represent author keywords; link strength indicates frequency of co-occurrence.

The WoS network indicates that the most central and densely connected clusters revolve around "cybersecurity," "higher education," "policy," and "academic integrity." The prominence of governance and integrity terms suggests that LMS cybersecurity is frequently conceptualized through institutional rules, compliance, and assessment trust rather than through infrastructure-centric cyber defense. Technical security keywords such as "encryption," "intrusion detection," or "zero-trust" appear more peripheral and weakly connected, implying comparatively limited attention to LMS-specific technical validation research within the WoS-indexed corpus. This pattern aligns with broader scholarship

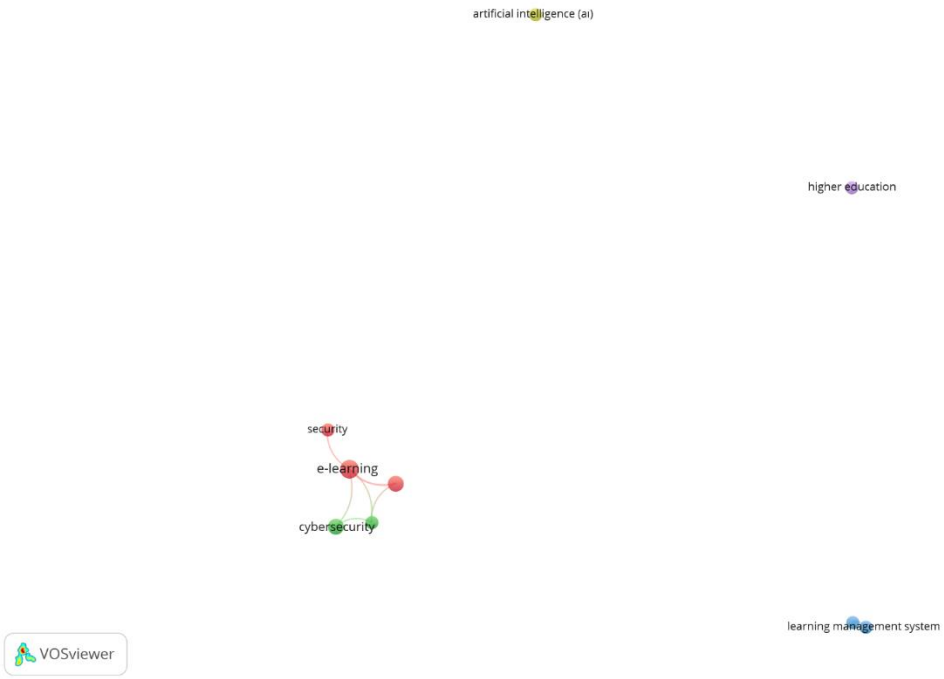
emphasizing human-centric and governance-centered cybersecurity narratives, where socio-organizational vulnerabilities often dominate applied research agendas (Bada & Nurse, 2019).

Critically, this does not imply that technical controls are absent from the domain; rather, the network structure suggests that technical terms are less likely to function as conceptual "bridges" across clusters, and therefore less likely to serve as integrating constructs in the scholarly discourse.

Keyword Co-occurrence Structure in Scopus

Figure 3 presents the Scopus keyword co-occurrence network.

Figure 3. Keyword co-occurrence network of LMS cybersecurity research (Scopus dataset, 2020–2025).



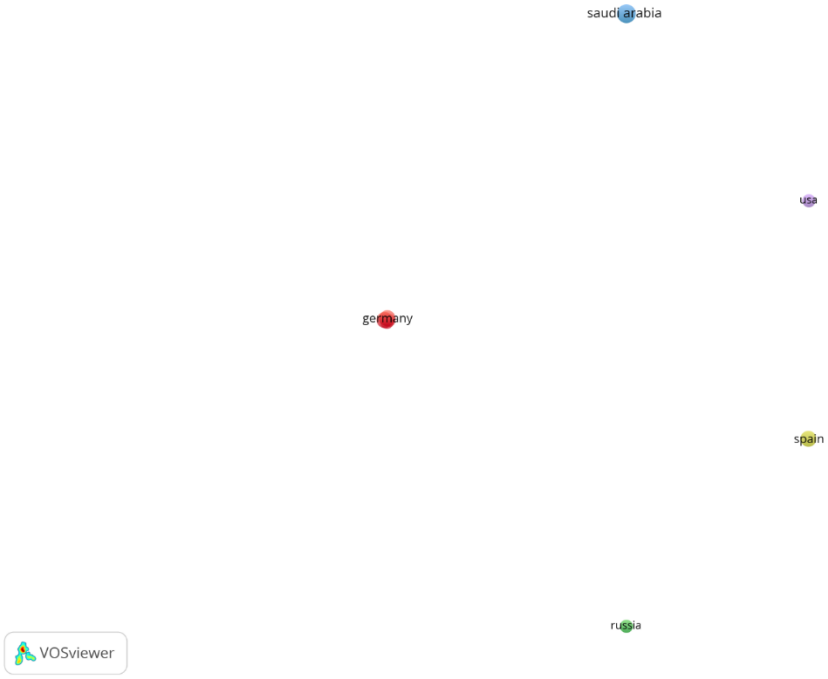
Compared to WoS, Scopus reveals a stronger presence of AI-related terms such as "artificial intelligence" and "learning analytics." However, these AI-related nodes are most often structurally connected to clusters associated with academic integrity, monitoring, and institutional decision-making rather than to clusters explicitly oriented toward threat detection, intrusion prevention, or adaptive cyber defense. This clustering suggests that AI in LMS contexts is still predominantly framed as a pedagogical monitoring or evaluative mechanism (e.g., proctoring, analytics-informed oversight) rather than as a security engine that performs anomaly detection, automated response, or continuous vulnerability mitigation.

Figures 2 and 3 together, provide early justification for the model logic developed later: AI is present, but its security role remains partially conceptualized and unevenly integrated into technical defense discourse. This bibliometric pattern directly informed the development of the LMRA, which seeks to structurally integrate these dispersed dimensions.

Global Collaboration Patterns (Country Co-authorship Networks)

Figure 4 shows the country co-authorship network in LMS cybersecurity research of Web of Science dataset, 2020–2025.

Figure 4. Country co-authorship network in LMS cybersecurity research

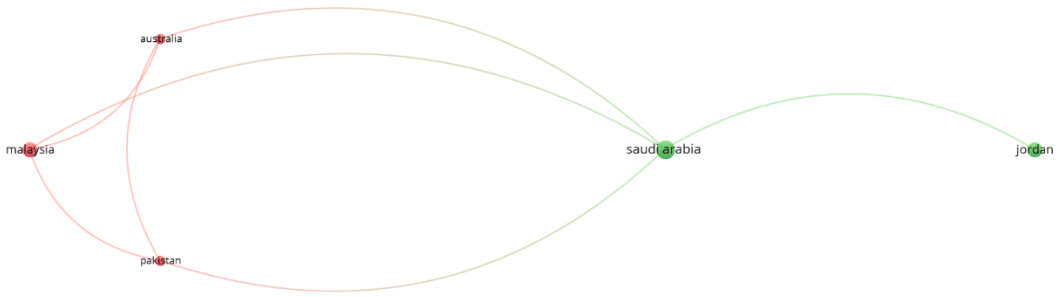


Note. VOSviewer visualization based on co-authorship by country; node size reflects publication output; links indicate international collaboration ties.

Figure 4 suggests that international collaboration in the WoS-indexed corpus remains structurally thin and cluster-bound rather than globally dense. The network is characterized by a small number of connected ties and several isolated or weakly linked country nodes, indicating that cross-border collaboration has not yet matured into a stable "global hub." Such limited density is consistent with emergent interdisciplinary domains, where research activity expands faster than sustained international team formation and shared methodological repertoires (Clark et al, 2017).

Figure 5 shows the country co-authorship network in LMS cybersecurity research of Scopus dataset, 2020–2025.

Figure 5. Country co-authorship network in LMS cybersecurity research



Note. VOSviewer visualization based on co-authorship by country; node size reflects publication output; links indicate international collaboration ties.

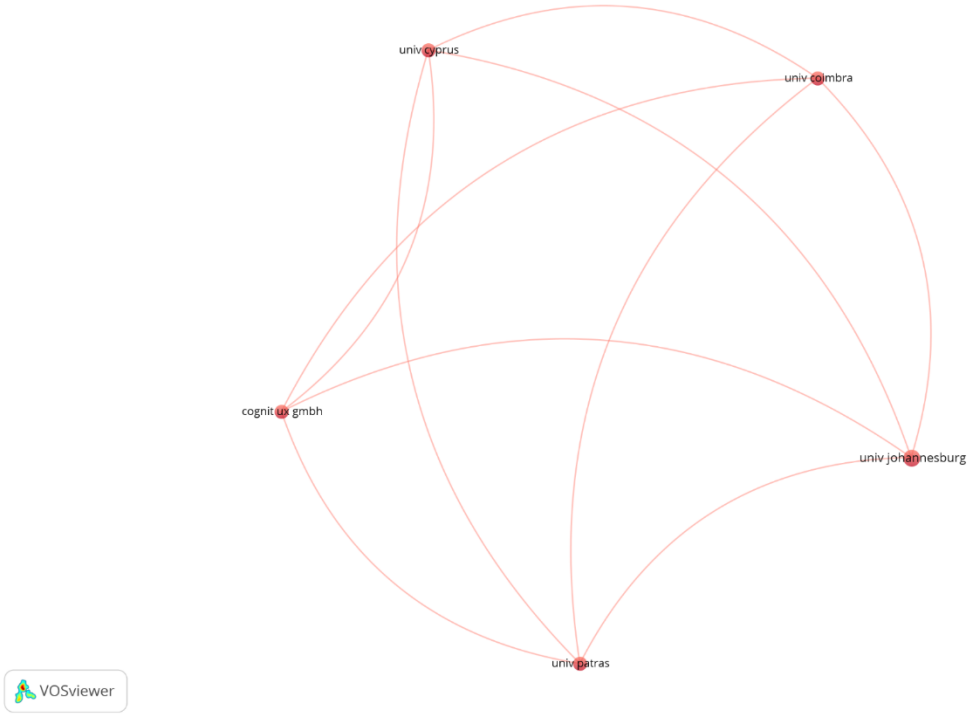
As shown in Figure 5, the Scopus dataset similarly reflects geographically distributed but weakly integrated collaboration patterns. The presence of multiple separated nodes with relatively few bridging links indicates that LMS cybersecurity research remains shaped by regional research agendas rather than consolidated transnational programs. Importantly, this dispersed collaboration ecology aligns with the field's conceptual dispersion observed in keyword networks (Figures 2–3), reinforcing the interpretation that the domain is expanding in volume while remaining structurally fragmented in both ideas and collaboration architectures.

Institutional and Author-Level Concentration (Co-authorship Networks)

Beyond keyword-level conceptual structures and country-level collaboration patterns, examining institutional and author-level co-authorship networks provides insight into the epistemic consolidation of the field. In emerging interdisciplinary domains, dense and cross-cluster collaboration networks often signal methodological convergence, shared theoretical frameworks, and cumulative knowledge building. Conversely, fragmented institutional and author-level structures may indicate compartmentalized research trajectories, localized expertise clusters, and limited cross-domain integration (Dhawan et al, 2024; Serrano et al, 2024). Therefore, analyzing organization- and author-based co-authorship networks allows for assessing whether LMS cybersecurity research is coalescing into a coherent scholarly community or continuing to evolve through parallel, semi-independent research streams.

Figure 6 presents the organization-level co-authorship network derived from the Web of Science dataset (2020–2025), illustrating institutional collaboration patterns in LMS cybersecurity research.

Figure 6. Organization co-authorship network in LMS cybersecurity research

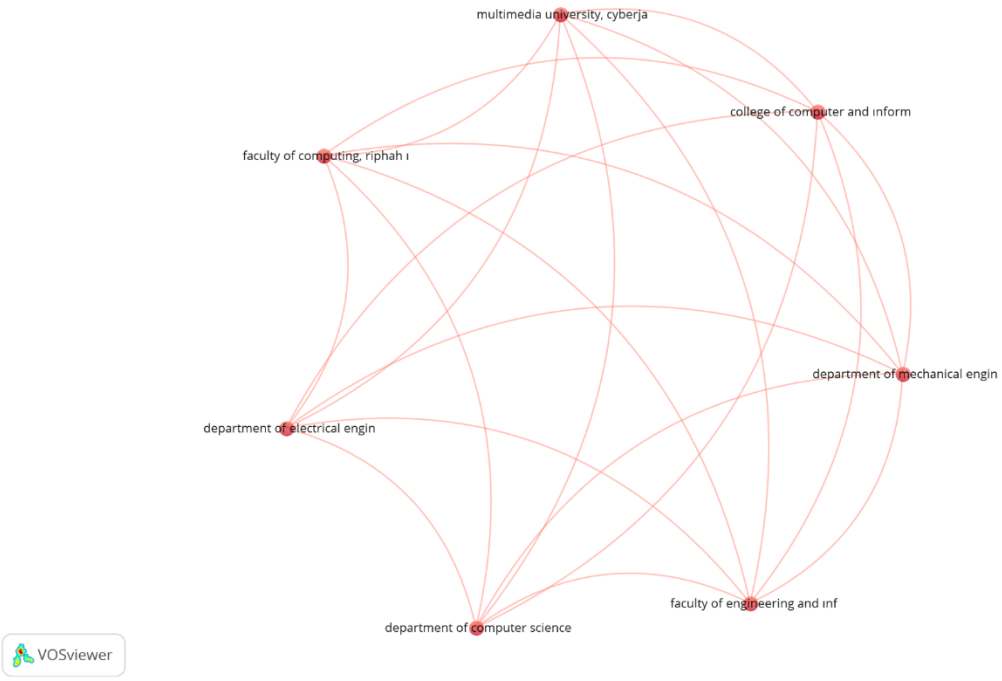


Note. VOSviewer visualization based on institutional co-authorship; node size reflects institutional output; links indicate collaboration strength.

Figure 6 indicates that institutional collaboration is clustered around small, tightly connected units, with limited cross-cluster bridging. This pattern suggests that the research base is institutionally localized and project-driven rather than organized around large inter-institutional consortia, which would typically act as stabilizing mechanisms for methodological convergence and shared research programs.

Figure 7 illustrates the organization-level co-authorship network based on the Scopus dataset (2020–2025), revealing the structural configuration of institutional collaboration within LMS cybersecurity research.

Figure 7. Organization co-authorship network in LMS cybersecurity research



Note. VOSviewer visualization based on author co-authorship; node size reflects productivity; links indicate collaboration ties.

At the institutional level, Figure 7 shows small collaboration micro-clusters with limited evidence of field-wide connector authors. This implies that knowledge production may be segmented into micro-communities, which can reinforce conceptual compartmentalization—especially in interdisciplinary fields where technical security, educational technology, and governance research often evolve in parallel (Chaterji et al, 2019).

Figure 8 (WoS) and Figure 9 (Scopus) presents the author-level co-authorship network derived from the dataset (2020–2025), illustrating institutional collaboration patterns in LMS cybersecurity research.

Figure 8. Author co-authorship network in LMS cybersecurity research (WoS dataset, 2020–2025).

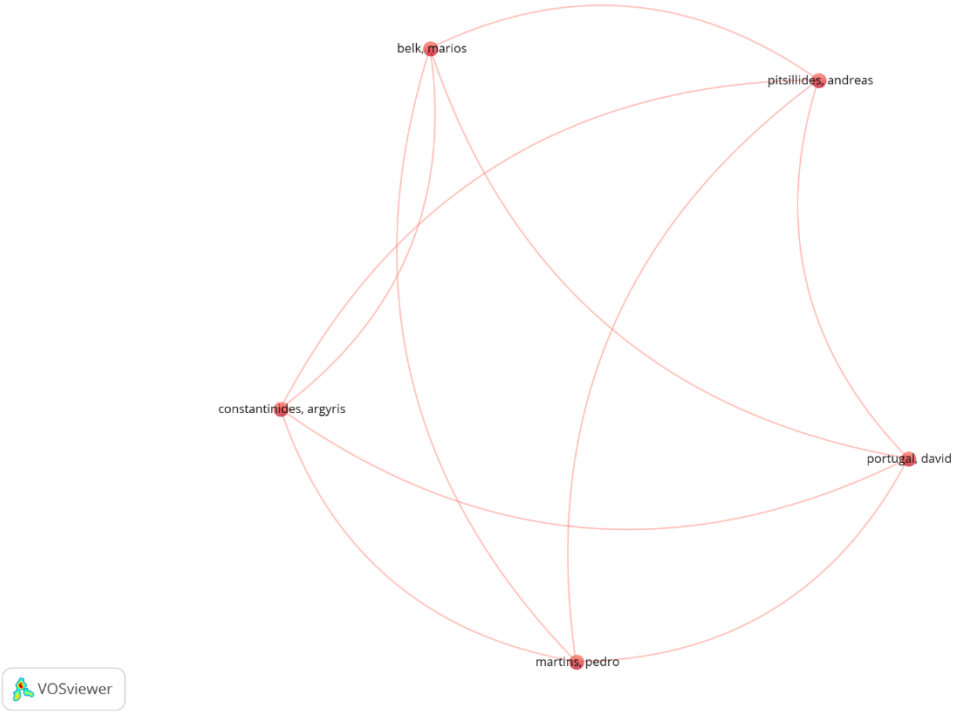
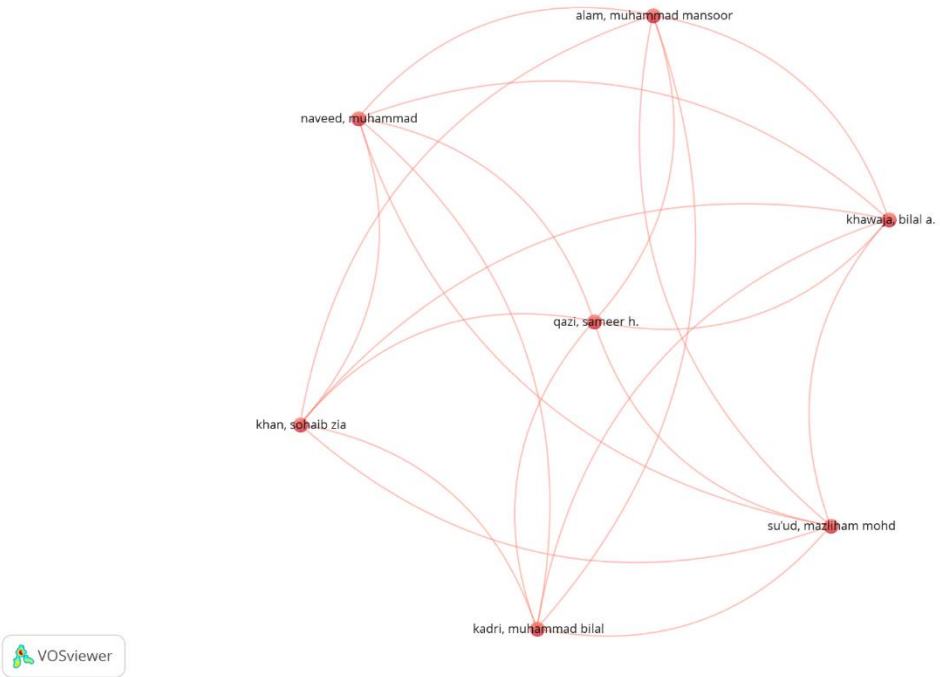


Figure 9. Author co-authorship network in LMS cybersecurity research (Scopus dataset, 2020–2025).



Figures 8 and 9 mirror the WoS pattern, showing that institutional and author collaborations in Scopus are also dominated by small clusters with few bridging structures. The absence of dense, cross-cutting collaboration networks is consistent with the field's multi-entry nature (technical controls, governance/policy, academic integrity, AI monitoring). Methodological and conceptual consolidation often requires sustained multi-site collaboration; thus, the observed network topology provides

additional structural evidence that LMS cybersecurity research is still transitioning from "fragmented defenses" toward integrated sociotechnical resilience logic.

Thematic Dominance of Human and Behavioral Dimensions

Thematic coding reveals pronounced imbalance across four dimensions: human and behavioral factors, governance and policy structures, technical security controls, and AI-mediated security mechanisms.

Human and behavioral dimensions dominate the corpus, appearing in 73% of studies. These works primarily address academic integrity, AI-assisted proctoring, user awareness, trust in digital environments, and risk mitigation through behavioral compliance. This dominance aligns with contemporary higher education cybersecurity discourse emphasizing sociotechnical vulnerabilities over purely infrastructural weaknesses (Bada & Nurse, 2019).

Governance and policy dimensions appear in 37% of studies but exert disproportionately high citation influence. Policy-oriented analyses, including institutional LMS policy alignment studies, constitute the most cited works within the dataset. This suggests that macro-organizational adaptation commands greater intellectual authority than micro-technical optimization.

Technical security controls are explicitly addressed in only 33% of studies, and many of these discussions remain conceptual rather than empirically validated. Enterprise-level standards such as zero-trust architecture and continuous monitoring frameworks (NIST, 2023; ISO/IEC 27001 updates, 2022) are rarely operationalized in LMS-specific contexts.

AI-based security mechanisms appear in only 13% of studies. Even within this subset, AI is typically deployed for monitoring academic misconduct rather than for anomaly detection, intrusion identification, or automated response systems. This underrepresentation contrasts sharply with AI-driven cybersecurity expansion in other sectors (George, 2024). These patterns are summarized in Table 1.

Table 1. Thematic Distribution and Citation Influence Across Dimensions

Dimension	Representation in Corpus	Citation Influence	Empirical Depth
Human & Behavioral	High (73%)	Moderate–High	Moderate
Governance & Policy	Moderate (37%)	Very High	Moderate
Technical Controls	Low–Moderate (33%)	Low	Low–Moderate
AI-Based Security	Low (13%)	Emerging	Low

The imbalance indicates that LMS cybersecurity is predominantly conceptualized as a governance and behavioral challenge rather than as a systems engineering problem. This asymmetry parallels broader digital transformation literature, where ethical and governance discourse frequently outpaces technical validation studies (Holmes, 2017).

Governance and Policy as Citation Drivers

The most cited study in the dataset (88 citations) analyzes common LMS policy elements in higher education institutions. This dominance of policy-oriented work indicates that governance frameworks significantly shape scholarly influence within the domain.

Recent policy-oriented cybersecurity analyses similarly argue that institutional readiness and compliance structures are central determinants of digital resilience (European Commission, 2022; NIST, 2023).

Moreover, AI-driven LMS transformation studies (65 citations) demonstrate that strategic integration of AI technologies — particularly generative AI — raises new governance concerns, including data protection, academic misconduct detection, and automated decision-making bias (Al-Kfairy, 2024; Markarian, 2025).

The citation structure suggests that institutional governance and AI integration concerns are more academically influential than infrastructure-level technical evaluations.

This indicates a research priority skewed toward macro-organizational adaptation rather than micro-technical optimization.

Underdevelopment of Technical Security Controls

Only one-third of studies explicitly address technical security mechanisms such as:

- Multi-factor authentication (MFA)
- Encryption protocols
- Intrusion detection systems
- Access control mechanisms

Furthermore, most of these discussions remain conceptual or prescriptive rather than empirically validated.

Recent cybersecurity frameworks (NIST, 2023; ISO/IEC 27001 updates, 2022) emphasize zero-trust architectures and continuous monitoring models. Yet, these frameworks are scarcely operationalized in LMS-specific contexts within the reviewed literature.

This gap indicates a disconnect between enterprise-level cybersecurity standards and LMS-specific implementation research. The absence of experimental validation studies suggests that LMS infrastructures may be theoretically discussed but not rigorously stress-tested.

AI-Based Security: Emerging but Peripheral

AI appears in the literature primarily in relation to:

- AI-assisted proctoring
- Learning analytics
- Predictive modeling for student behavior

However, only 13% of studies explicitly employ AI for adaptive threat detection or automated vulnerability mitigation.

This finding is noteworthy given the rapid expansion of AI-driven cybersecurity systems in other sectors (George, 2024). In contrast, LMS research remains predominantly focused on AI as a pedagogical or evaluative tool rather than as a security engine.

AI's role in LMS cybersecurity remains emergent and peripheral. There is limited integration of machine learning-based intrusion detection, anomaly detection, or automated response systems tailored to educational platforms.

This underrepresentation suggests a substantial research opportunity in AI-mediated adaptive security architectures.

Sociotechnical Imbalance in LMS Cybersecurity Research

The synthesis of thematic distribution and citation patterns reveals a clear sociotechnical asymmetry within the field. Human and behavioral dimensions dominate the empirical landscape, while governance-oriented studies exert disproportionate citation influence. In contrast, technical security controls and AI-driven adaptive mechanisms remain comparatively underrepresented and less empirically validated.

This imbalance does not indicate neglect of infrastructure but reflects the distinctive sociotechnical configuration of LMS environments, where institutional trust, academic integrity, and policy compliance intersect with technical safeguards. However, the limited integration of enterprise-level security validation and AI-based adaptive detection suggests that resilience remains conceptually articulated rather than operationally consolidated.

These findings reinforce the need for a multilayer architectural perspective capable of structurally integrating governance, behavioral, AI-mediated, and technical domains within a unified resilience logic.

Towards an LMS Multilayer Resilience Architecture (LMRA)

The findings collectively indicate that LMS security research operates across four interacting layers:

- Technical Security Controls
- Human & Behavioral Dynamics
- AI-Mediated Mechanisms
- Governance & Policy Structures

However, these layers are rarely integrated within a single coherent framework. Based on the thematic synthesis, has been proposed the LMRA, which conceptualizes LMS security as a multilayered sociotechnical ecosystem rather than a discrete technical problem.

The LMRA model emphasizes:

- Alignment between enterprise security standards and LMS deployment
- Integration of AI-driven adaptive detection systems
- Institutional policy operationalization
- Continuous user competence development

This integrative approach responds directly to the structural fragmentation identified in the bibliometric analysis.

Identified Research Gaps and Future Directions

The analysis highlights four critical research gaps:

- Lack of empirical validation of LMS-specific technical security implementations
- Limited AI-driven adaptive security architectures
- Weak operationalization of policy frameworks
- Insufficient integration between human and technical security layers

Addressing these gaps requires interdisciplinary collaboration between cybersecurity engineers, educational technologists, AI specialists, and institutional policy makers.

The findings demonstrate that LMS cybersecurity research is not underdeveloped in volume, but under-integrated in structure. The dominance of governance and behavioral themes, combined with the peripheral status of technical validation studies, underscores the need for a cohesive resilience architecture.

Derivation of the LMS Multilayer Resilience Architecture (LMRA)

Analytical Pathway to Architectural Synthesis

The LMRA was not imposed as a prescriptive design but inductively derived through a structured synthesis of empirical patterns observed across the corpus. The architecture emerged from the convergence of four analytical procedures: bibliometric structure mapping, thematic distribution analysis, citation anchor examination, and cross-dimensional gap synthesis.

Rather than treating these procedures as isolated steps, they were interpreted relationally to identify structural tensions within the field. This integrative approach aligns with conceptual synthesis methodologies in systematic knowledge integration, where theoretical structures are derived from cross-theme patterns rather than from single-variable dominance (Snyder, 2019; Torraco, 2016).

The analytical progression unfolded across four interrelated interpretive movements.

Structural Dispersion in Bibliometric Networks

Keyword co-occurrence analysis revealed dispersed conceptual clusters linking cybersecurity, higher education, AI, privacy, e-learning, authentication, and policy-related constructs. However, no single dominant integrating node emerged across both Web of Science and Scopus datasets. Instead, the field appeared characterized by multiple semi-autonomous clusters, each organized around specific focal concerns such as academic integrity, governance compliance, or technical access control.

This pattern reflects what interdisciplinary cybersecurity scholarship identifies as epistemic dispersion, where research develops at the intersection of multiple domains without consolidating into a shared theoretical core (O'Donovan et al, 2023). The absence of a stabilizing conceptual center suggested that LMS cybersecurity research, while expanding, lacks integrative structural articulation.

This dispersion did not indicate intellectual weakness; rather, it highlighted the need for architectural synthesis capable of organizing coexisting but disconnected strands of inquiry.

Thematic Asymmetry Across Dimensions

Thematic coding revealed significant asymmetry in representational weight across four analytical domains. Human and behavioral factors constituted the dominant orientation, followed by governance and policy considerations. Technical security controls appeared less frequently, and AI-based adaptive security mechanisms were minimally represented.

This imbalance mirrors broader trends in educational AI and cybersecurity literature, where governance, ethics, and behavioral adaptation often advance more rapidly than infrastructure-level validation research (Holmes, 2017; Yan et al, 2025). The observed asymmetry indicated that LMS cybersecurity is predominantly framed as a sociotechnical governance challenge rather than as a narrowly technical systems engineering problem.

Importantly, this does not diminish the importance of technical controls; instead, it reveals that technical mechanisms are rarely treated as central organizing constructs within the discourse. The asymmetry therefore reinforced the necessity of a multilayered perspective capable of repositioning technical, behavioral, AI-mediated, and governance elements within a coherent resilience architecture.

Citation Anchors and Intellectual Orientation

Citation anchor analysis further clarified the field's intellectual orientation. The most influential publications emphasized institutional policy alignment, AI transformation in LMS environments, and academic integrity frameworks. No highly cited study focused exclusively on infrastructure-level mechanisms such as encryption performance, zero-trust implementation, or LMS-specific intrusion detection testing.

This citation ecology aligns with institutional cybersecurity narratives emphasizing governance capacity, compliance readiness, and organizational adaptation (NIST, 2023; OECD, 2023). The prominence of governance and AI transformation themes suggests that scholarly influence in this domain is shaped more by macro-organizational and strategic concerns than by micro-technical experimentation.

Taken together, bibliometric dispersion, thematic imbalance, and citation asymmetry indicated a structural gap: LMS cybersecurity research is conceptually rich but insufficiently integrated.

Cross-Dimensional Gaps and the Need for Resilience Architecture

Gap synthesis revealed four persistent discontinuities. First, there is limited empirical validation of LMS-specific technical control deployments under realistic institutional conditions. Second, AI-driven adaptive threat detection tailored to educational platforms remains underdeveloped. Third, governance and policy frameworks are frequently discussed normatively but rarely operationalized into measurable resilience outcomes. Fourth, integration between user competence development and infrastructure-level hardening is minimal.

These discontinuities collectively point to the absence of a unifying architectural logic linking governance, human behavior, AI mediation, and technical defense mechanisms.

In response to these observed structural tensions, the LMRA was conceptualized as an integrative structural synthesis.

Structure of the LMRA

The LMS Multilayer Resilience Architecture conceptualizes LMS cybersecurity as an interdependent system composed of four interacting layers: governance and policy foundations, human and behavioral dynamics, AI-mediated adaptive mechanisms, and technical security controls.

Unlike hierarchical defense models, LMRA does not assume linear causality or top-down enforcement. Instead, it positions resilience as an emergent property of coordinated interaction across layers. Weakness in any single layer may propagate systemically, while strengthening cross-layer alignment enhances overall adaptive capacity. This structural logic is consistent with sociotechnical systems theory, which emphasizes reciprocal influence between social and technical subsystems.

At its foundational level, governance and policy structures define compliance boundaries, accountability mechanisms, and risk management procedures. These structural parameters shape how technical controls are deployed and how AI systems are regulated.

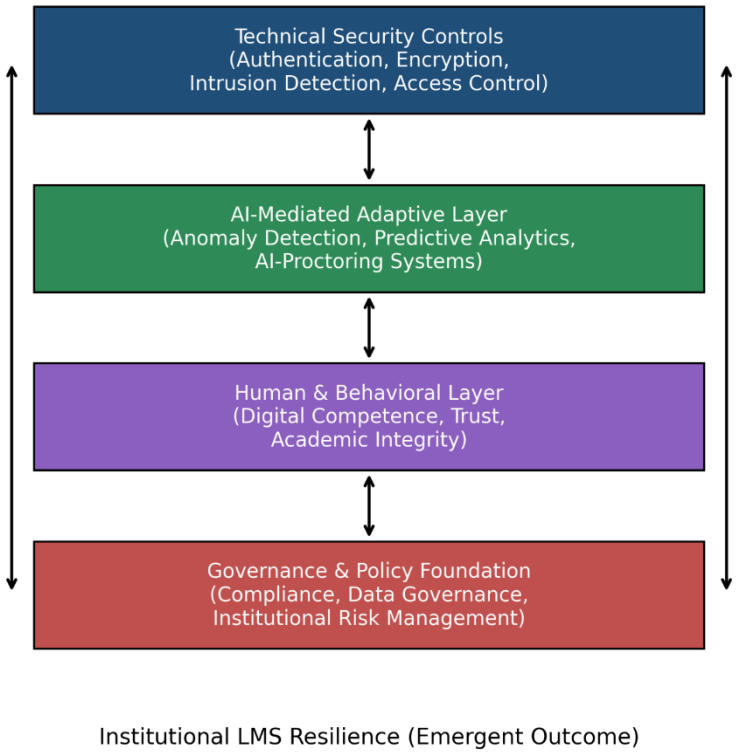
The human and behavioral layer operationalizes governance principles through user awareness, digital competence, trust formation, and academic integrity practices. This layer mediates between institutional design and everyday system use.

The AI-mediated adaptive layer introduces monitoring, predictive analytics, anomaly detection, and automated response capacities. Positioned between behavioral and technical dimensions, this layer functions as a dynamic intermediary capable of translating behavioral signals into adaptive system-level adjustments.

The technical security control layer implements infrastructure-level safeguards, including authentication systems, encryption mechanisms, intrusion detection systems, and access control protocols. However, within LMRA, technical controls are not treated as isolated protective shells but as components embedded within governance constraints and behavioral realities.

The architecture is visually represented in Figure 10.

Figure 10. LMRA: Bidirectional Interdependency Model.



Theoretical Interpretation

The LMRA reflects a paradigmatic shift from conceptualizing LMS security as infrastructure protection toward understanding it as sociotechnical resilience governance. Rather than focusing exclusively on preventing breaches, the architecture emphasizes adaptive capacity, cross-layer feedback, and systemic robustness.

This orientation aligns with contemporary resilience governance discourse, which prioritizes continuous monitoring, institutional accountability, and human-factor resilience within cybersecurity ecosystems (European Commission, 2022; Kurubacak et al, 2022; NIST, 2023). In this perspective, resilience emerges not from the strength of individual components but from the quality of their coordination.

Architectural Contribution to the Literature

The LMS Multilayer Resilience Architecture contributes to scholarship in four primary ways. First, it integrates fragmented thematic domains into a coherent structural perspective. Second, it bridges technical and behavioral scholarship, repositioning them as mutually conditioning elements rather than competing explanatory frames. Third, it reconceptualizes AI as an adaptive mediating layer embedded within resilience logic rather than as a purely pedagogical monitoring tool. Fourth, it operationalizes governance as a structural foundation influencing all other dimensions.

Within the reviewed corpus, no prior study explicitly organizes LMS cybersecurity around a multilayer resilience architecture grounded in sociotechnical interdependency. By articulating this structure, the

present study advances a conceptual synthesis responsive to the field's documented fragmentation and imbalance.

5. DISCUSSION

Beyond Technical Hardening: Repositioning LMS Cybersecurity as Resilience Governance

The findings of this study challenge the implicit assumption that LMS cybersecurity is primarily a technical systems engineering problem. While enterprise cybersecurity discourse foregrounds zero-trust architectures, encryption standards, and intrusion detection systems (NIST, 2023), the LMS-focused literature reveals a markedly different orientation.

The bibliometric and thematic synthesis demonstrates that the intellectual center of gravity in LMS cybersecurity research lies within human behavior, governance structures, and AI-mediated academic integrity mechanisms rather than infrastructure hardening. This asymmetry is not incidental; it signals a paradigmatic repositioning of cybersecurity within educational ecosystems.

In LMS environments, breaches do not merely represent unauthorized access or data exfiltration. They manifest as academic misconduct, credential misuse, generative AI exploitation, assessment manipulation, and governance non-compliance. Consequently, cybersecurity in educational contexts expands beyond the classical triad of confidentiality, integrity, and availability into the domain of epistemic integrity and institutional trust.

This shift necessitates reconceptualizing LMS cybersecurity not as static defense architecture but as resilience governance within a multilayer sociotechnical ecosystem.

Behavioral Dominance: Adaptive Awareness or Structural Substitution?

The predominance of human and behavioral research (73% of the corpus) reflects what recent scholarship describes as the "behavioralization" of cybersecurity (Bada & Nurse, 2022). Awareness training, digital competence, trust-building, and integrity reinforcement have become dominant mitigation narratives.

While acknowledging that many cyber incidents originate in human action (OECD, 2023), this orientation risks over-individualizing responsibility. When behavioral adaptation becomes the primary security strategy, infrastructural fragility may remain insufficiently interrogated. In such cases, users are implicitly positioned as compensatory buffers for architectural limitations.

Our findings suggest that LMS research may inadvertently normalize a reactive posture: educating users to mitigate systemic weaknesses rather than strengthening adaptive system-level resilience.

The LMRA addresses this imbalance by repositioning behavioral dimensions as interdependent components within a coordinated system rather than as primary safeguards. Within LMRA, user awareness interacts with governance constraints, AI-mediated monitoring, and technical enforcement in bidirectional feedback loops. Behavioral competence enhances resilience only when embedded within supportive architectural alignment.

Governance as Structural Conditioning Force

Citation anchor analysis revealed that policy-oriented publications exert disproportionate influence within the field. Governance frameworks shape scholarly impact more strongly than technical experimentation. This pattern aligns with contemporary resilience governance discourse emphasizing institutional readiness, compliance alignment, and accountability mechanisms as central determinants of cybersecurity robustness (European Commission, 2022; NIST, 2023).

However, governance without operationalization risks symbolic compliance. Few studies empirically evaluate how LMS policy reforms affect measurable outcomes such as breach probability, detection latency, recovery time, or adaptive learning system robustness. This governance–implementation gap reinforces the need for an architectural perspective.

Within the LMRA, governance functions as a conditioning foundation rather than a sufficient solution. Policies define structural boundaries within which technical controls are implemented, AI systems are regulated, and behavioral norms are enacted. Resilience emerges when governance translates into operational coherence across layers.

AI as a Structural Inflection Point

AI occupies a paradoxical position within LMS cybersecurity research. Although present in the literature, it remains conceptually under-integrated as a security mechanism. Most AI applications focus on proctoring, learning analytics, and misconduct detection rather than adaptive threat mitigation.

Yet generative AI simultaneously introduces new risk vectors and new defense capacities. It can amplify misconduct while enabling anomaly detection, predictive monitoring, and automated response.

This dual-use characteristic positions AI as a structural mediator within the LMRA. AI connects behavioral signals to technical enforcement mechanisms and feeds governance structures through analytics-driven feedback loops. Its current peripheral treatment in LMS cybersecurity literature suggests not maturity but frontier potential. AI-based adaptive resilience remains an underdeveloped research trajectory.

From Fragmentation to Interdependent Resilience

The most significant theoretical contribution of this study lies in reframing LMS cybersecurity as a bidirectionally interdependent resilience architecture. Prior scholarship frequently isolates technical hardening, human awareness, AI transformation, or governance policy as discrete domains.

However, our synthesis demonstrates that these dimensions co-evolve and propagate influence across layers. Technical breaches may necessitate policy revision; governance gaps may erode user compliance; AI anomaly detection may trigger institutional restructuring; behavioral misuse may expose architectural fragility.

The LMRA thus moves beyond defense-in-depth logic toward adaptive interdependency. Resilience is conceptualized not as a property of individual components but as an emergent quality arising from coordinated cross-layer alignment.

To the best of our knowledge, this multilayer resilience perspective has not been explicitly articulated in prior LMS cybersecurity syntheses.

Structural Imbalance as Research Opportunity

The observed thematic imbalance should not be interpreted solely as deficiency. However, the relative scarcity of empirically validated technical controls and AI-mediated adaptive security mechanisms indicates a critical opportunity.

Future research must transition from conceptual discourse to measurable resilience science. This requires experimental validation of LMS-specific security implementations, integrated evaluation of behavioral interventions against breach reduction metrics, and empirical testing of AI-driven anomaly detection within real-world educational infrastructures.

Interdisciplinary collaboration between cybersecurity engineers, educational technologists, AI specialists, and governance scholars will be essential for advancing from fragmentation to operational integration.

6. CONCLUSION

This study mapped the intellectual structure of LMS cybersecurity research between 2020 and 2025 and identified a field characterized by thematic expansion but structural fragmentation. The evidence indicates that LMS cybersecurity is predominantly conceptualized as a governance and behavioral challenge, supplemented by emerging AI-mediated integrity mechanisms, rather than as a rigorously validated technical security architecture.

This orientation reflects the sociotechnical complexity of educational ecosystems rather than infrastructural neglect. By synthesizing bibliometric patterns, thematic distributions, and citation anchors, this study advances the LMRA, conceptualizing LMS security as a bidirectionally interdependent system composed of governance, behavioral, AI-mediated, and technical layers.

The LMRA repositions LMS cybersecurity from isolated defensive mechanisms toward coordinated multilayer resilience. Theoretically, it integrates fragmented research streams within a sociotechnical resilience paradigm. Practically, it provides institutions with a structural lens to evaluate vulnerabilities across governance, behavior, AI systems, and technical controls simultaneously.

In digitally mediated higher education ecosystems, resilience is no longer a supplementary safeguard but a structural necessity. As generative AI, remote assessment infrastructures, and platform dependency intensify, LMS cybersecurity cannot remain confined to isolated technical hardening or policy compliance checklists. The findings of this study demonstrate that sustainable protection emerges from coordinated interaction across governance, behavioral, AI-mediated, and technical domains.

The LMS Multilayer Resilience Architecture (LMRA) offers a conceptual foundation for understanding this interdependence, reframing LMS security as an adaptive sociotechnical system rather than a static defensive perimeter. Future empirical investigations examining cross-layer interaction effects and operational resilience metrics will be essential for translating this conceptual synthesis into measurable institutional robustness.

Ultimately, the evolution of LMS cybersecurity will depend not on strengthening individual components in isolation, but on cultivating coherent, multilayer resilience capable of adapting to an increasingly intelligent and volatile digital learning environment.

Implications and Recommendations

Implications for Research

Future research should prioritize empirical validation of LMS-specific technical security implementations, including encryption performance, multi-factor authentication efficacy, and zero-trust deployment within educational platforms. AI-driven adaptive security models tailored to LMS contexts require development and systematic testing. Cross-layer studies examining how governance policies influence technical enforcement and behavioral compliance are essential for advancing resilience measurement. Additionally, the development of sociotechnical resilience metrics integrating behavioral, technical, AI, and governance indicators would significantly enhance methodological maturity.

Implications for Practice

Universities should avoid treating LMS cybersecurity as solely an IT responsibility. Governance policies must translate into measurable technical deployment, and AI-assisted monitoring systems should be aligned with behavioral training and institutional accountability mechanisms. Institutional audits should adopt cross-layer evaluation logic rather than checklist-based compliance review.

Policy Recommendations

Policy makers should consider developing LMS-specific cybersecurity guidelines aligned with international resilience frameworks. Regular cross-layer security audits integrating governance, AI, behavioral, and technical assessments are recommended. Institutions should establish interdisciplinary cybersecurity task forces bridging information technology, pedagogy, data governance, and AI oversight units to operationalize resilience architecture principles.

Limitations

This study has several limitations that should be considered when interpreting the proposed LMRA.

First, the corpus size (N = 30) reflects the specificity of the search criteria—LMS, cybersecurity, higher education, and the 2020–2025 timeframe—but nevertheless limits the breadth of representation. While the dataset captures the most relevant peer-reviewed literature within major citation databases (Web of Science and Scopus), it does not encompass gray literature, industry reports, institutional white papers, or non-indexed regional publications. Given that cybersecurity practices often evolve faster in operational environments than in academic publications, some implementation-level innovations may not yet be reflected in the scholarly corpus.

Second, the analysis is restricted to English-language publications indexed in two major databases. Although these platforms provide high-quality coverage, they may underrepresent research published in

local languages or emerging regional journals. As a result, collaboration patterns and thematic distributions may reflect indexing dynamics rather than the full global knowledge ecosystem.

Third, the LMRA is a conceptual synthesis derived from bibliometric dispersion, thematic imbalance, and citation structure analysis. It does not constitute an empirically validated security model tested in operational LMS environments. The architecture should therefore be interpreted as an integrative analytical construct rather than as a prescriptive technical blueprint. Empirical validation studies are required to test cross-layer interaction effects and resilience outcomes in real institutional settings.

Fourth, bibliometric network visualization tools (e.g., VOSviewer) provide structural representations of co-occurrence and collaboration but do not capture qualitative depth, contextual nuance, or causal mechanisms. Network centrality does not necessarily equate to conceptual superiority, and peripheral themes may represent emerging research frontiers rather than marginal importance.

Finally, the study focuses on higher education contexts. LMS cybersecurity dynamics in K–12 environments, corporate learning systems, or governmental training platforms may exhibit distinct governance and behavioral configurations that were outside the scope of this analysis.

These limitations do not diminish the value of the LMRA but delineate its scope. The architecture should be understood as a theoretically grounded synthesis responsive to observed structural fragmentation, inviting further empirical refinement and cross-context validation.

Declaration by Authors

Ethical Approval: Since no data involving human contact was collected in this study, ethical permission is not required, and the study was conducted in accordance with ethical criteria.

Conflict of Interest: No conflicts of interest declared.

Example of List of References

1. Al-Kfairy, M., Mustafa, D., Kshetri, N., Insiew, M., & Alfandi, O. (2024, August). Ethical challenges and solutions of generative AI: An interdisciplinary perspective. In Informatics (Vol. 11, No. 3, p. 58). MDPI.
2. Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393-410.
3. Bahmanova, A., & Lace, N. (2024). Cyber risks: systematic literature analysis. Journal of Systemics, Cybernetics and Informatics, 22(2), 37-47.
4. Bosiu, L. (2025). Cybersecurity Risks and Initiatives at Higher Education Institutions. University of Johannesburg (South Africa).
5. Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective: Part II: The application of socio-technical theory. MIS quarterly, 1(4), 11-28.

6. Bradley, V. M. (2021). Learning Management System (LMS) use with online instruction. International Journal of Technology in Education, 4(1), 68-92.
7. Chaterji, S., Naghizadeh, P., Alam, M. A., Bagchi, S., Chiang, M., Corman, D., ... & Weller, J. (2019). Resilient cyberphysical systems and their application drivers: A technology roadmap. arXiv preprint arXiv:2001.00090.
8. Clark, J., Laing, K., Leat, D., Lofthouse, R., Thomas, U., Tiplady, L., & Woolner, P. (2017). Transformation in interdisciplinary research methodology: the importance of shared experiences in landscapes of practice. International Journal of Research & Method in Education, 40(3), 243-256.
9. Denisova-Schmidt, E. (2016). The Global Challenge of Academic Integrity. International Higher Education, (87), 4-6.
10. Dhawan, D., Gupta, B. M., Mamdapur, G. M. N., Walke, R., & Bansal, M. (2024). Bibliometrics Research in India: A Scientometric Assessment of High-Cited Publications During 1994-2023. Journal of Data Science, 3(3), 275-293.
11. European Commision, (2026). EU cybersecurity policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies . 04.01.2026.
12. Gangavarapu, R. (2025). Unmasking the Security Risks of Generative AI: Threats and Strategies for Defense. In Mastering AI Governance: A Guide to Building Trustworthy and Transparent AI Systems (pp. 63-76). Cham: Springer Nature Switzerland.
13. George, A. S. (2024). Emerging trends in AI-driven cybersecurity: an in-depth analysis. Partners Universal Innovative Research Publication, 2(4), 15-28.
14. Holmes, E. J. (2017). Development and Leadership of a Faculty-led Academic Integrity Education Program at an Ontario College.
15. ISO/IEC 27001 updates (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001
16. Karras, A., Theodorakopoulos, L., Karras, C., Theodoropoulou, A., Kalliampakou, I., & Kalogeratos, G. (2025). LLMs for Cybersecurity in the Big Data Era: A Comprehensive Review of Applications, Challenges, and Future Directions. Information, 16(11), 957.
17. Kurubacak, G., Sharma, R. C., & Uğur, S. (2022). Living in the meta immersive smart 21st century and beyond: A digital transformation in Open and Distance Learning (ODL). TAM Akademi Dergisi, 1(2), 86-95.
18. Markarian, M. (2025). Evaluating International AI Governance: Balancing Technological Innovation in the Development of a Global Model for Generative AI (Doctoral dissertation).
19. NIST, (2023). Cybersecurity Framework. https://www.nist.gov/cyberframework, 02.01.2026
20. O'Donovan, B., Kirke, C., Pate, M., McHugh, S., Bennett, K., & Cahir, C. (2023). Mapping the Theoretical Domain Framework to the Consolidated Framework for Implementation Research: do multiple frameworks add value?. Implementation science communications, 4(1), 100.

21. OECD, (2023). National cybersecurity strategy and action plan (2020-2023). https://depp.oecd.org/policies/TUR1360

22. Serrano, S. A., Martinez-Carranza, J., & Sucar, L. E. (2024). Knowledge transfer for cross-domain reinforcement learning: A systematic review. IEEE Access, 12, 114552-114572.

23. Sharma, A., Gurram, N. T., Rawal, R., Mamidi, P. L., & Gupta, A. S. G. (2025). Enhancing educational outcomes through cloud computing and data-driven management systems. Vascular and Endovascular Review, 8(11s), 429-435.

24. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339.

25. Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. Human resource development review, 15(4), 404-428.

26. Trist, E., Pasmore, W. A., & Sherwood, J. J. (1960). Socio-technical systems. London: Tavistock.

27. Uğur, S., & Kurubacak, G. (2019). Technology management through artificial intelligence in open and distance learning. In Handbook of research on challenges and opportunities in launching a technology-driven international university (pp. 338-368). IGI Global Scientific Publishing.

28. Yan, Y., Liu, H., Zhang, H., Chau, T., & Li, J. (2025). Designing a generalist education AI framework for multimodal learning and ethical data governance. Applied Sciences, 15(14), 7758.