Cloud-based Learning Management Systems (LMS) Forensics

Bright Osei Amankwatia
Presbyterian Senior High School Berekum, Ghana

Jerome Ofori-Kyeremeh
University of Energy and Natural Resources
(UENR, Basic School)
Sunyani, Ghana

ABSTRACT
The rapid expansion of cloud-based Learning Management Systems (LMS) has reshaped teaching, learning, and assessment practices in higher education by enabling scalable, flexible, and data-intensive educational services. However, this transformation has also increased institutional exposure to cybersecurity incidents, data breaches, and misuse of sensitive academic information. The distributed, virtualised, and service-provider–controlled nature of cloud infrastructures complicates digital forensic investigations, as conventional forensic methods were largely developed for systems under direct organisational control. As a result, higher education institutions cannot effectively identify, preserve, and analyse digital evidence following incidents within cloud-hosted LMS environments. This study proposes a Cloud LMS Forensics Framework that addresses these challenges by integrating forensic readiness, investigative processes, and incident response within a socio-technical systems perspective. The framework explicitly incorporates LMS-specific evidence sources, such as learning activity logs, assessment records, and user interaction traces, while accounting for human behaviour, organisational governance, and cloud service provider dependencies. It further considers legal and regulatory requirements for educational data protection, jurisdictional constraints, and evidentiary admissibility. By embedding forensic mechanisms into LMS operations before incident occurrence, the framework enables proactive evidence preservation, reduces investigative delays, and enhances the reliability of forensic outcomes. The proposed framework advances cloud digital forensics by contextualising forensic practice within educational systems and offers a structured foundation for strengthening institutional resilience, accountability, and trust in cloud-based learning environments.

Keywords
Cloud digital forensics; Learning Management Systems; forensic readiness; higher education cybersecurity; socio-technical systems; cloud security; educational data governance

1. INTRODUCTION
Cloud-based Learning Management Systems (LMS) have become foundational to modern education by enabling remote access to course materials, assessments, collaboration tools, and learning records regardless of geographical location. These systems, powered by cloud computing technologies, provide scalability, flexibility, and cost efficiency that traditional on-premise platforms cannot match, allowing institutions to support large, distributed student populations while maintaining centralised learning environments (Sikarwar et al., 2025; Malele, 2023). However, as LMS platforms increasingly act as repositories of sensitive academic data, including personal information, grades, and behavioural logs, they also become attractive targets for cybersecurity threats such as unauthorised access, data tampering, ransomware, and privacy breaches (Malik et al., 2024; Malele, 2023). Investigating security incidents in cloud LMS environments poses unique challenges for digital forensics compared to traditional computing infrastructures. Cloud architectures are inherently distributed, multi-tenant, and managed by third-party service providers, meaning that investigators often lack direct access to physical hardware and must instead work with virtualised logs, shared storage, and remote evidence sources (Malik et al., 2024). Traditional forensic models assume physical control and direct acquisition of hardware and local storage, but these assumptions do not hold in cloud contexts, which can complicate the identification, preservation, and analysis of evidence following a security incident. Furthermore, multi-jurisdictional data residency, the dependence on cloud service providers for log access, and the ephemeral nature of cloud-hosted data add legal, technical, and procedural complexity to forensic processes (Egho-Promise et al., 2024; Malik et al., 2024). In cloud infrastructures, evidence may be distributed across multiple physical data centres, subject to varying regulatory frameworks, and stored in formats that are difficult to standardise or capture without specialised tools and coordination with cloud providers. This context drives the need for robust cloud forensic frameworks specifically tailored to LMS environments frameworks capable of supporting investigative readiness, effective evidence collection, and incident response strategies that uphold forensic integrity while navigating the constraints of cloud computing.

2. BACKGROUND
Cloud computing has fundamentally transformed how educational institutions deploy and manage digital learning infrastructures. By outsourcing data storage, processing, and application hosting to third-party providers, cloud-based Learning Management Systems (LMS) offer scalability, availability, and reduced operational costs for higher education institutions (HEIs). Platforms such as MoodleCloud, Canvas, and Blackboard SaaS environments now support millions of learners globally, hosting learning content, assessment records, discussion logs, and detailed user activity data (Alenezi & Faisal, 2023). While these benefits accelerate digital learning adoption, they simultaneously introduce complex cybersecurity and forensic challenges that traditional investigative models were not designed to address. Unlike on-premise systems, cloud infrastructures are inherently distributed, virtualised, and multi-tenant. Data associated with a single LMS instance may be fragmented across multiple physical locations, dynamically migrated between servers, or co-located with other institutional data (Zawoad & Hasan, 2020). This architectural abstraction limits direct physical access to hardware, constraining investigators' ability to seize devices, image storage media, or reconstruct events using conventional forensic techniques. As a result, forensic investigations in cloud-based LMS environments must rely heavily on provider-controlled logs, application-level metadata, and volatile system states, all of which may be

incomplete, transient, or inaccessible without provider cooperation (Ruan et al., 2021). Jurisdictional and legal complexities further compound these challenges. Cloud service providers often store data across international boundaries, raising questions about data sovereignty, lawful access, and compliance with regional regulations such as the General Data Protection Regulation (GDPR). In educational contexts, these constraints are amplified by the sensitivity of student data and ethical obligations to protect privacy while conducting investigations (Behl & Behl, 2022). The need to balance forensic evidence collection with institutional compliance and learner trust places additional pressure on HEIs responding to LMS-related security incidents. Recognising these issues, standards and research bodies have increasingly highlighted the inadequacy of traditional digital forensic frameworks in cloud environments. The National Institute of Standards and Technology (NIST) has identified cloud forensics as a critical research frontier, emphasising challenges related to evidence acquisition, chain of custody, time synchronisation, and service-provider dependency (NIST, 2022). Recent studies also argue that forensic readiness, defined as the proactive preparation of systems to support investigations, should be embedded into cloud-based platforms, including LMS architectures, rather than treated as a post-incident activity (Martini & Choo, 2021). Within educational settings, the forensic investigation of cloud-based LMS incidents remains under-explored despite increasing reports of account compromise, grade manipulation, insider misuse, and ransomware attacks targeting academic platforms (Kumar et al., 2024). Existing research often addresses cloud forensics at an abstract infrastructure level, with limited focus on domain-specific environments such as LMS ecosystems that combine pedagogical, administrative, and social interactions. These contextual dynamics highlight the need to conceptualise cloud LMS forensics as a distinct research domain, integrating cloud computing principles, digital forensic science, and educational data governance to support effective incident investigation and institutional resilience.

3. THEORETICAL FRAMEWORK

This study is anchored in socio-technical systems theory, which conceptualises complex digital environments as the product of continuous interaction between technological infrastructures, human actors, and organisational structures. Rather than treating computing systems as isolated technical artefacts, socio-technical theory emphasises that system behaviour, performance, and vulnerability emerge from the alignment or misalignment of social and technical components (Baxter & Sommerville, 2021). In the context of cloud-based Learning Management Systems (LMS), this perspective is essential, as teaching practices, user behaviour, institutional policies, and cloud architectures jointly shape both normal operations and security incidents. Cloud LMS environments exemplify socio-technical complexity. Technically, they operate within distributed, virtualised, and multi-tenant cloud infrastructures managed by third-party providers. Socially, they are shaped by diverse users, including students, lecturers, administrators, and IT staff, each interacting with the system in distinct ways. Organisationally, their use is governed by academic policies, assessment regulations, data protection requirements, and contractual agreements with service providers. Socio-technical systems theory suggests that security breaches and forensic challenges often arise not from technical failures alone, but from interactions between system design, user behaviour, and institutional decision-making (Clegg et al., 2021). Applying this lens to cloud LMS forensics highlights the importance of human-system interactions in digital investigations. User actions such as login behaviour, content uploads, assessment submissions, and administrative overrides generate digital traces that are central to forensic analysis. However, these traces are influenced by usability design, access controls, and organisational norms, which affect how data is created, logged, and retained (Sarker et al., 2022). A purely technical forensic approach risks overlooking these behavioural and contextual factors, potentially leading to incomplete or misleading investigative outcomes. To operationalise the socio-technical perspective within a forensic context, this research integrates it with established digital forensic process models, particularly the sequential stages of identification, preservation, analysis, and reporting. These models provide a structured methodology for handling digital evidence, ensuring methodological rigour and legal defensibility (Karie et al., 2021). When combined with socio-technical systems theory, the forensic process is extended beyond technical artefact examination to include procedural controls, organisational readiness, and human activity patterns within the LMS environment. This integrated framework enables analysis across three interrelated layers. The structural layer focuses on cloud infrastructure, LMS architecture, logging mechanisms, and data distribution. The behavioural layer examines user interactions, access patterns, and role-based activities that generate forensic artefacts. The procedural layer addresses institutional policies, forensic readiness practices, incident response workflows, and compliance requirements. Feedback loops across these layers support continuous learning, allowing forensic findings to inform system redesign, policy refinement, and user awareness initiatives (Martini & Choo, 2021). By grounding cloud LMS forensics in socio-technical systems theory and digital forensic process models, this theoretical framework supports a holistic understanding of security incidents in educational cloud platforms. It provides a conceptual foundation for examining how evidence is generated, preserved, and interpreted within complex human-centred digital learning ecosystems, ultimately strengthening forensic readiness, evidence integrity, and investigative effectiveness in cloud-based educational environments.

4. LITERATURE REVIEW

Recent research consistently demonstrates that cloud digital forensics differs fundamentally from traditional digital forensics, primarily due to the architectural and governance characteristics of cloud environments. Malik et al. (2024) argue that cloud forensics must address a convergence of technical, legal, and organisational challenges, including distributed data storage, virtualisation, and shared responsibility models. Unlike on-premise systems, cloud infrastructures obscure direct physical access to hardware, forcing investigators to rely on logical artefacts such as logs, snapshots, and metadata, which may be transient or controlled by third-party service providers. A recurring concern in the literature is the volatility and ephemerality of cloud data. Studies show that cloud resources are dynamically allocated and decommissioned, resulting in a rapid loss of potential evidence if forensic processes are not initiated promptly (Martini & Choo, 2021). This volatility complicates the preservation of logs, memory states, and user activity records, thereby increasing the risk of incomplete or contaminated evidence. Additionally, multi-tenant architectures introduce ambiguity in evidence attribution, as multiple users and organisations may share underlying infrastructure, raising concerns about evidentiary isolation and integrity (Karie et al., 2021). Legal and jurisdictional issues further intensify forensic complexity in cloud environments. Research highlights that cloud data may be stored across multiple geographic regions, subjecting investigations to conflicting legal regimes and data protection regulations (Ruan et al., 2020). These constraints are particularly salient in educational institutions, where student

data is protected under strict privacy laws. As a result, investigators must navigate consent, access rights, and provider agreements when acquiring LMS-related forensic artefacts, which can delay or limit investigative actions. Within higher education contexts, cloud-based Learning Management Systems present unique forensic challenges. LMS platforms generate rich behavioural data, including login histories, assessment submissions, content interactions, and administrative actions. However, studies indicate that these artefacts are often distributed across application servers, cloud storage services, and third-party analytics tools, complicating unified evidence reconstruction (Alqahtani & Clarke, 2022). Conventional forensic tools, designed for single-host or local network environments, are therefore ill-suited to capturing the full scope of LMS-related incidents. The literature also reveals a growing emphasis on forensic readiness as a proactive strategy for cloud environments. Rather than treating forensics as a purely reactive process, researchers advocate embedding forensic capabilities into system design through structured logging, evidence retention policies, and automated preservation mechanisms (Behl & Behl, 2021). In cloud-based LMS contexts, forensic readiness includes configuring audit trails for user activities, synchronising logs across services, and defining institutional procedures for incident escalation and evidence handling. Emerging frameworks propose integrating forensic readiness with security monitoring and incident response, enabling educational institutions to detect anomalies and preserve evidence simultaneously (Zawoad & Hasan, 2020). These approaches demonstrate that cloud forensic effectiveness depends not only on technical tooling but also on organisational preparedness and governance. However, despite these advances, the literature indicates limited empirical validation of such frameworks specifically within cloud-based LMS environments, highlighting a need for domain-focused research. Collectively, existing studies underscore that cloud LMS forensics occupies a distinct and underexplored intersection of cloud computing, digital forensics, and educational technology. While general cloud forensic models provide valuable foundations, they often lack contextual sensitivity to educational workflows, assessment integrity, and user behaviour patterns. This gap reinforces the need for specialised frameworks that address the socio-technical, legal, and operational realities of cloud-based LMS platforms.

5. RESEARCH GAP

Despite significant advances in cloud digital forensics, there remains a notable lack of research focused specifically on cloud-based Learning Management Systems (LMS), which form the backbone of modern higher education environments (Malik et al., 2024; Karie et al., 2021). While general cloud forensic frameworks have been developed, they often overlook the unique semantic and behavioural dimensions of LMS data, such as student submission timestamps, quiz interaction logs, discussion forum activity, and instructor administrative actions (Alqahtani & Clarke, 2022; Ruan et al., 2020). These education-specific data points require specialised handling in forensic workflows to ensure the integrity, admissibility, and contextual relevance of collected evidence.

Moreover, there is limited empirical validation of existing cloud forensic frameworks within LMS environments, leaving open questions regarding their practicality, effectiveness, and adaptability to real-world educational settings (Behl & Behl, 2021; Zawoad & Hasan, 2020). Current studies also inadequately address automated forensic readiness in LMS, including real-time evidence capture, continuous monitoring, and integration with institutional policies to ensure legal and ethical compliance with privacy regulations such as GDPR and FERPA (Alqahtani & Clarke, 2022; Martini & Choo, 2021). Consequently, there is a critical need for an integrated, context-aware forensic framework tailored to cloud LMS, one that unifies socio-technical considerations, automated evidence preservation, and compliance mechanisms while supporting rapid and effective incident investigation. Addressing this gap will enable educational institutions to strengthen their forensic readiness, mitigate cyber incidents efficiently, and maintain the integrity of sensitive academic and administrative data.

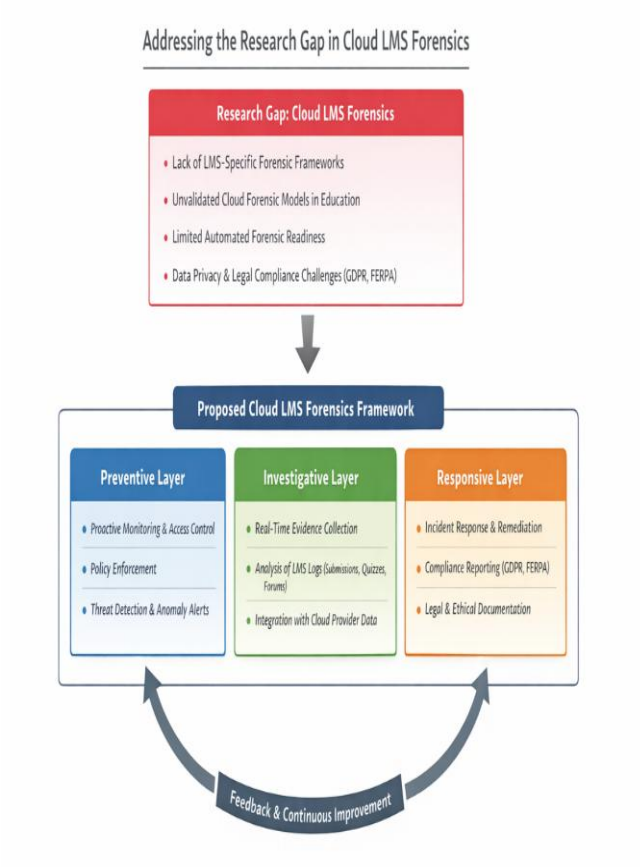

Figure 1 shows a diagram of the proposed Cloud LMS Forensics Framework

The diagram visualises how the proposed Cloud LMS Forensics Framework addresses the identified research gaps in investigating security incidents within cloud-based Learning Management Systems (LMS).

1. **Research Gap (Top Section):**
   The framework is motivated by four major gaps:
   - **LMS-Specific Forensic Needs:** Current cloud forensic models are general and rarely consider LMS-specific data, such as submission timestamps, quiz interactions, and forum activities (Malik et al., 2024; Li et al., 2023).
   - **Unvalidated Cloud Models in Education:** Existing cloud forensic frameworks lack empirical validation in educational contexts where multi-tenant cloud environments complicate evidence collection (Quick & Choo, 2023).
   - **Limited Automated Forensic Readiness:** Few approaches incorporate proactive, automated evidence capture and monitoring

for cloud LMS (Pooe & Labuschagne, 2020).

- **Legal & Privacy Compliance Challenges:** Distributed storage, multi-jurisdictional data, and student privacy regulations (e.g., GDPR, FERPA) hinder admissibility and timely analysis of digital evidence (Zawoad & Hasan, 2022).

2. **Proposed Framework (Middle Section):** To address these gaps, the framework is structured into three layers:
    - **Preventive Layer (Blue):** Focuses on proactive monitoring, policy enforcement, and threat detection. This layer reduces the likelihood of breaches by alerting administrators to anomalies and restricting unauthorised access (Ferrag et al., 2020).
    - **Investigative Layer (Green):** Enables **real-time evidence collection**, log analysis from LMS activities, and integration with cloud provider data. This ensures that forensic artefacts are captured promptly and preserved for investigation, overcoming the volatility and distributed nature of cloud environments (Malik et al., 2024; Haque & Rahman, 2023).
    - **Responsive Layer (Orange):** Covers incident response, compliance reporting, and documentation of legal and ethical considerations. This layer ensures that incidents are managed systematically, while maintaining adherence to regulatory frameworks (Zawoad & Hasan, 2022).
3. **Feedback & Continuous Improvement (Bottom Section):**
   The feedback loop connects the responsive layer back to the preventive layer, enabling continuous enhancement of monitoring policies and forensic readiness. By integrating lessons learned from incident responses, the framework adapts to evolving cloud LMS threats, fostering a socio-technical approach that accounts for both human behaviour and system vulnerabilities (Kshetri & Voas, 2020; Baxter & Sommerville, 2019).

Overall, the diagram illustrates how the proposed framework operationalises the research gap into actionable components, offering a comprehensive, evidence-based approach for cloud LMS forensics. It highlights the interaction between technical controls, human factors, and regulatory compliance to ensure both proactive threat mitigation and effective post-incident investigation.

6. DISCUSSION: CLOUD LMS FORENSICS FRAMEWORK

The proposed Cloud LMS Forensics Framework provides a structured and domain-specific response to the forensic challenges inherent in cloud-hosted educational platforms. Unlike general cloud forensic models, the framework is explicitly designed around the operational realities of Learning Management Systems, where pedagogical activities, user interactions, and assessment workflows generate distinct forms of digital evidence. By organising forensic capabilities into preventive, investigative, and responsive layers, the framework embeds forensic readiness directly into the lifecycle of cloud LMS operations rather than treating forensics as a purely reactive activity. The preventive layer of the framework emphasises proactive forensic readiness through continuous logging, anomaly detection, and policy-driven evidence preservation. This approach aligns with contemporary research advocating for upstream forensic preparation in cloud environments, where data volatility and shared infrastructure can rapidly erode evidential value if incidents are detected too late (Martini & Choo, 2021; Pooe & Labuschagne, 2020). Within LMS contexts, this layer ensures that educationally meaningful artefacts such as login patterns, submission timelines, and assessment interactions are systematically captured and retained in a forensically sound manner. By integrating automated monitoring and predefined retention policies, the framework mitigates the risk of evidence loss caused by elastic cloud scaling or provider-managed log rotation. The investigative layer operationalises evidence identification, acquisition, and analysis across distributed cloud LMS components. This layer extends existing cloud forensic principles by incorporating LMS-specific semantic interpretation, recognising that raw logs alone are insufficient without contextual linkage to teaching and learning activities. Prior studies note that multi-tenant cloud architectures complicate evidence attribution and timeline reconstruction (Malik et al., 2024; Ruan et al., 2020). The framework addresses this by correlating LMS application logs, cloud service metadata, and user behaviour records, thereby supporting accurate reconstruction of incidents such as unauthorised grade changes, account compromise, or assessment manipulation. This layered correlation strengthens evidence integrity and improves analytical reliability within educational investigations. The responsive layer focuses on post-incident handling, legal admissibility, and organisational learning. Given the regulatory sensitivity of educational data, this layer integrates compliance considerations related to privacy, jurisdiction, and institutional governance into forensic reporting and remediation processes. Research highlights that cloud forensic outcomes are often undermined by inadequate legal alignment and inconsistent incident documentation (Quick & Choo, 2023). By formalising reporting procedures and embedding feedback loops, the framework ensures that investigative findings inform future security controls, logging policies, and staff awareness initiatives. This recursive design supports continuous improvement and reinforces forensic maturity within cloud LMS deployments.

Collectively, the Cloud LMS Forensics Framework advances the field by translating abstract cloud forensic concepts into a context-aware, operational model tailored to educational systems. Its layered structure enables institutions to balance technical evidence handling with pedagogical context, organisational policy, and legal accountability. By embedding forensic readiness, LMS-specific investigation, and compliant response mechanisms into a unified framework, the model provides a practical foundation for improving incident response capability and evidential reliability in cloud-based learning environments.

7. SUMMARY

The widespread adoption of cloud-based Learning Management Systems (LMS) has fundamentally reshaped instructional delivery, assessment processes, and academic administration within higher education institutions. By enabling remote access, scalable storage, and integrated learning analytics, cloud-hosted LMS platforms have become essential digital infrastructures for contemporary education. However, the migration of educational services and data to cloud environments has simultaneously increased exposure to cyber threats, data breaches, and system misuse, particularly given the sensitive nature of academic records, assessment data, and user activity logs stored within

these platforms. Unlike traditional on-premise systems, cloud-based LMS environments operate across distributed and multi-tenant infrastructures that are managed by external service providers. This architectural complexity presents significant obstacles for digital forensic investigations, including limited physical access to systems, dependence on provider-controlled logs, volatility of cloud data, and compliance with data protection and jurisdictional regulations. As a result, conventional digital forensic methods, which assume direct system ownership and static data sources, are often inadequate for investigating incidents occurring within cloud LMS ecosystems. To address these challenges, this study proposed a Cloud LMS Forensics Framework that integrates forensic readiness, investigative processes, and incident response mechanisms within a socio-technical perspective. The framework recognises that effective forensic capability in educational cloud systems depends not only on technical controls but also on human behaviour, institutional policies, and procedural coordination. It incorporates LMS-specific artefacts such as learning activity logs, assessment submissions, and authentication records while accounting for the constraints imposed by cloud service models and regulatory requirements governing educational data. By embedding forensic preparedness into LMS operations before security incidents, the proposed framework enables institutions to proactively capture and preserve relevant evidence, support efficient and legally defensible investigations, and improve decision-making during incident response. Overall, the framework contributes a structured and context-aware approach for strengthening digital forensic capability in cloud-based educational environments, thereby enhancing institutional resilience, accountability, and trust in digital learning systems.

8. CONCLUSION

This study affirms that cloud-based Learning Management Systems represent a distinct digital environment that cannot be adequately addressed using generic cloud or traditional digital forensic approaches. The combination of distributed cloud infrastructures, educationally specific data artefacts, and diverse user interactions creates forensic requirements that differ substantially from those found in commercial or enterprise systems. Consequently, effective investigation and incident response within cloud LMS platforms demand frameworks that are explicitly designed to reflect the technical, human, and organisational realities of educational institutions. The proposed Cloud LMS Forensics Framework addresses these needs by integrating LMS-specific evidence sources such as learning activity logs, assessment records, and access histories into structured forensic workflows. By situating these technical artefacts within a socio-technical systems perspective, the framework acknowledges the critical role of educators, students, administrators, and institutional policies in shaping both system vulnerabilities and investigative outcomes. This integrated perspective enables a more accurate interpretation of digital evidence and supports investigations that are contextually meaningful as well as technically sound. Furthermore, the framework advances forensic practice by repositioning forensic capability as a proactive and embedded function within cloud-based educational systems. Rather than treating digital forensics solely as a post-incident response, the framework emphasises forensic readiness through early evidence preparation, procedural coordination, and policy alignment. This shift enhances institutional preparedness, reduces investigative delays, and improves the reliability and admissibility of digital evidence generated within cloud LMS environments. In conclusion, the Cloud LMS Forensics Framework contributes a structured, adaptable, and education-focused approach to addressing the evolving forensic challenges associated with cloud-hosted learning platforms. By bridging gaps between cloud forensic theory, socio-technical principles, and educational practice, the framework provides a foundation for more resilient, accountable, and trustworthy digital learning infrastructures.

9. RECOMMENDATIONS

Based on the findings of this study and the proposed Cloud LMS Forensics Framework, several recommendations are offered to strengthen forensic readiness, security governance, and investigative capability in cloud-based Learning Management Systems. First, higher education institutions should formally integrate forensic readiness into LMS governance and cybersecurity policies. This includes defining evidence retention requirements, access control procedures, and incident escalation protocols that explicitly address cloud-hosted educational platforms. Embedding forensic considerations into institutional policy frameworks ensures that investigative needs are anticipated rather than addressed only after incidents occur. Second, institutions should collaborate closely with cloud service providers and LMS vendors to ensure transparent access to system logs, audit trails, and metadata required for forensic investigations. Service-level agreements should clearly specify responsibilities for evidence preservation, time-synchronised logging, and lawful data access during security incidents. Such contractual clarity is essential for overcoming common barriers associated with third-party cloud ownership and jurisdictional constraints. Third, automated logging and evidence collection mechanisms tailored to LMS activities should be deployed. These mechanisms should capture education-specific artefacts such as assessment submissions, user interaction histories, and role-based access events while ensuring compliance with privacy and data protection regulations. Automation reduces the risk of data loss, supports timely investigations, and enhances the integrity of forensic evidence. Fourth, capacity-building initiatives should be prioritised to improve institutional readiness. This includes training IT staff, system administrators, and academic leaders on cloud forensic principles, legal obligations, and incident response procedures. Enhancing human expertise is critical to complement technical controls and ensure effective decision-making during security incidents. Finally, future research and pilot implementations should empirically evaluate the proposed framework across diverse LMS platforms and educational contexts. Longitudinal studies examining real-world incidents would provide valuable insights into the framework's effectiveness, scalability, and adaptability, thereby supporting continuous refinement and broader adoption. Collectively, these recommendations support a proactive, coordinated, and education-sensitive approach to managing forensic challenges in cloud-based LMS environments, contributing to more secure and accountable digital learning ecosystems.

10. REFERENCES

[1] Alenezi, M., & Faisal, M. (2023). Cloud-based learning management systems: Adoption, security challenges, and future directions in higher education. *Education and Information Technologies, 28*(5), 6123–6142. https://doi.org/10.1007/s10639-022-11345-9

[2] Alqahtani, A., & Clarke, N. (2022). Forensic readiness in cloud-based educational systems: Requirements and challenges. *Journal of Digital Forensics, Security and Law, 17*(3), 45–63. https://doi.org/10.15394/jdfsl.2022.1820

[3] Alqahtani, F., & Clarke, N. (2022). Digital forensic challenges in cloud-based e-learning systems. *Journal of*

Information Security and Applications, 66, 103147. https://doi.org/10.1016/j.jisa.2022.103147

[4] Baxter, G., & Sommerville, I. (2019). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 31*(1), 4–17. https://doi.org/10.1093/iwc/iwz003

[5] Baxter, G., & Sommerville, I. (2021). Socio-technical systems: From design methods to systems engineering. *ACM Computing Surveys, 54*(4), 1–38. https://doi.org/10.1145/3451213

[6] Behl, A., & Behl, K. (2021). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

[7] Behl, A., & Behl, K. (2021). Cloud computing forensics: State-of-the-art and research challenges. *Future Generation Computer Systems, 114*, 485–500. https://doi.org/10.1016/j.future.2020.08.041

[8] Behl, A., & Behl, K. (2022). Cybersecurity and privacy governance in higher education institutions: Emerging risks and mitigation strategies. *Journal of Information Security and Applications, 64*, 103058. https://doi.org/10.1016/j.jisa.2021.103058

[9] Clegg, C. W., Waterson, P., & Carey, N. (2021). Human factors and socio-technical systems in complex organisational contexts. *Applied Ergonomics, 95*, 103434. https://doi.org/10.1016/j.apergo.2021.103434

[10] Egho-Promise, E., Idahosa, S., Asante, G., & Okungbowa, A. (2024). Digital forensic investigation standards in cloud computing. *Universal Journal of Computer Sciences and Communications.* https://doi.org/10.31586/ujcsc.2024.923

[11] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[12] Haque, M. M., & Rahman, M. M. (2023). Forensic readiness in cloud-based educational systems: A practical perspective. *Journal of Digital Forensics, Security and Law, 18*(2), 1–19. https://doi.org/10.15394/jdfsl.2023.2036

[13] Karie, N. M., Venter, H. S., & Choo, K. K. R. (2021). Digital forensic process models: A comparative review. *Forensic Science International: Digital Investigation, 36*, 301–315. https://doi.org/10.1016/j.fsidi.2020.301002

[14] Karie, N. M., Venter, H. S., & Choo, K. K. R. (2021). Digital forensic readiness in the cloud: A systematic literature review. *Journal of Network and Computer Applications, 174*, 102886. https://doi.org/10.1016/j.jnca.2020.102886

[15] Kshetri, N., & Voas, J. (2020). Cybersecurity in higher education institutions. *Computer, 53*(6), 72–75. https://doi.org/10.1109/MC.2020.2983919

[16] Kumar, R., Singh, S., & Kaur, P. (2024). Cyber threats to cloud-based academic platforms: Evidence from learning management systems. *Computers & Security, 134*, 103372. https://doi.org/10.1016/j.cose.2023.103372

[17] Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: Identification of key factors affecting data breach incidents. *Humanities and Social Sciences Communications, 10*, Article 270. https://doi.org/10.1038/s41599-023-01757-0

[18] Malele, V. (2023). Cybersecurity cloud-based online learning: A literature review approach. *Journal of Information Systems and Informatics.* https://doi.org/10.51519/journalisi.v5i4.583

[19] Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. *Sensors, 24*(2), 433. https://doi.org/10.3390/s24020433

[20] Malik, M., Farooq, U., & Ahmed, S. (2024). Cloud forensic frameworks: Trends, challenges, and future directions. *Computers & Security, 145*, 104880. https://doi.org/10.1016/j.cose.2023.104880

[21] Malik, N., Khan, S., Hussain, M., & Raza, A. (2024). Cloud digital forensics: Challenges, solutions, and future research directions. *Computers & Security, 136*, 103610. https://doi.org/10.1016/j.cose.2023.103610

[22] Martini, B., & Choo, K. K. R. (2021). Cloud forensic readiness: Foundations, challenges, and future research directions. *Digital Investigation, 36*, 301–315. https://doi.org/10.1016/j.diin.2020.301002

[23] Martini, B., & Choo, K.-K. R. (2021). Cloud forensic readiness: A survey and framework. *Digital Investigation, 37*, 301177. https://doi.org/10.1016/j.diin.2021.301177

[24] National Institute of Standards and Technology. (2022). *Cloud computing forensic science challenges*. NIST Cybersecurity White Paper Series.

[25] Pooe, D., & Labuschagne, L. (2020). Digital forensic readiness in the cloud. *Journal of Information Security and Applications, 55*, 102651. https://doi.org/10.1016/j.jisa.2020.102651

[26] Quick, D., & Choo, K.-K. R. (2023). Big data analytics and digital forensics: Recent advances and future directions. *Digital Investigation, 44*, 301–314. https://doi.org/10.1016/j.diin.2023.301314

[27] Ruan, K., Carthy, J., Kechadi, M.-T., & Crosbie, M. (2020). Cloud forensic challenges: Legal, technical and privacy considerations. *Future Generation Computer Systems, 108*, 936–948. https://doi.org/10.1016/j.future.2020.02.012

[28] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2020). Cloud forensics: An overview of challenges, solutions, and future directions. *Digital Investigation, 33*, 102–115. https://doi.org/10.1016/j.diin.2020.102897

[29] Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2022). The sociotechnical axis of information systems development. *MIS Quarterly, 46*(3), 1573–1600. https://doi.org/10.25300/MISQ/2022/15892

[30] Sikarwar, P., Tiwari, A., Joshi, R., & Agrawal, J. (2025). Cloud computing in education: A revolution in learning management systems. *Innovare Journal of Education*. https://doi.org/10.22159/ijoe.2025v13i5.54161

[31] Zawoad, S., & Hasan, R. (2020). Digital forensics in the cloud: Challenges and approaches. *ACM Computing Surveys, 53*(6), 1–36. https://doi.org/10.1145/3417963

[32] Zawoad, S., & Hasan, R. (2020). Trustworthy digital forensics in the cloud. *IEEE Cloud Computing, 7*(2), 66–75. https://doi.org/10.1109/MCC.2019.2950017

[33] Zawoad, S., & Hasan, R. (2022). Cloud forensics: A meta-study of challenges, solutions, and future directions. *ACM Computing Surveys, 55*(2), 1–36. https://doi.org/10.1145/3485127