The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 11 2025
PAGE NO. 129-135

Evolving Frameworks for Digital Trust: A Multidimensional Analysis of Data Governance in Cloud, IoT, and Multimodal AI Ecosystems

Helvina L. Orvest
School of Governance & Emerging Technologies, University of Amsterdam, Netherlands

Received: 11 November 2025; **Accepted:** 20 November 2025; **Published:** 26 November 2025

Abstract:

Purpose: As organizations transition toward cloud-native architectures and artificial intelligence (AI) integration, traditional data governance (DG) frameworks—originally designing for on-premise, structured data—are proving insufficient. This study aims to analyze the evolving requirements of DG in converged environments, specifically examining the intersection of Cloud Computing, Internet of Things (IoT), and Multimodal AI systems. The research seeks to establish a taxonomy of enabling factors that facilitate secure AI adoption and digital trust.

Methodology: A systematic literature review and qualitative document analysis were conducted on 33 peer-reviewed sources ranging from 2014 to 2025. The analysis utilized a risk-based modeling approach to categorize governance dimensions, contrasting cloud versus non-cloud governance taxonomies and evaluating frameworks for algorithmic auditing and multimodal data fusion.

Findings: The review identifies that successful DG in modern ecosystems requires a shift from static compliance checklists to dynamic, "agile" governance models. Key findings indicate that cloud data governance is distinctively characterized by shared responsibility models that complicate digital forensics and custody. Furthermore, the integration of AI necessitates new governance layers for "grey data" and multimodal inputs, particularly in high-stakes sectors like healthcare and banking. The study confirms that organizational culture and executive sponsorship are as critical as technical controls in enabling secure digital transformation.

Originality/value: This paper proposes a unified conceptual framework that bridges the gap between technical data management and strategic corporate governance. It uniquely addresses the governance of "multimodal" data streams and provides a roadmap for internal auditors to engage with AI systems despite the current lack of standardized guidance.

Keywords: Data Governance, Cloud Computing, Artificial Intelligence, Digital Trust, Multimodal Data, Algorithmic Auditing, Information Security.

1.INTRODUCTION

The digitization of global commerce and public administration has elevated data from a byproduct of business operations to a core strategic asset. In this contemporary landscape, the mechanisms by which organizations manage, secure, and leverage this asset—collectively known as Data Governance (DG)—have become critical determinants of organizational longevity. Early conceptions of data governance focused primarily on data quality and master data management within static, on-premise databases. However, the rapid proliferation of Cloud Computing, the Internet of Things (IoT), and Artificial Intelligence (AI) has fundamentally altered the topological landscape of information systems. As noted by Rajgopal and Yadav [1], the role of data governance has expanded to become the primary enabler of secure AI adoption, suggesting that without robust governance frameworks, the promised efficiencies of algorithmic decision-making cannot be safely realized.

The transition from legacy infrastructure to cloud-based environments represents a significant

discontinuity in governance theory. Where traditional governance relied on absolute control over physical storage and network perimeters, the cloud model introduces the complexity of shared responsibility. Al-Ruithe et al. [3] argue that designing data governance for cloud computing requires a conceptual overhaul, as the abstraction of infrastructure removes direct oversight capabilities that IT departments previously relied upon. This loss of physical control necessitates a shift toward contractual and policy-based governance, yet many organizations struggle to adapt their legacy frameworks to this new reality. The challenge is further compounded in the public sector, where sensitive citizen data must be migrated to cloud infrastructures that are often managed by private third parties. Al-Ruithe and Benkhelifa [2] highlight that determining the enabling factors for such transitions is not merely a technical exercise but a complex structural equation of trust, regulation, and utility.

Furthermore, the volume and velocity of data generated by modern systems have rendered manual governance obsolete. The banking sector, for instance, has long recognized the necessity of governance for regulatory compliance, as discussed by Burniston [14], but the sector is now facing the "Big Data" reality where volume outstrips human auditing capacity. This creates a critical vulnerability: if data cannot be governed at the speed of its generation, quality degrades, and security risks escalate. Barker [8] posits that data governance is the "missing approach" to improving data quality, suggesting that technology alone cannot solve quality issues without the overlay of accountability and stewardship.

The introduction of AI and Machine Learning (ML) into this ecosystem introduces the concept of "Algorithmic Accountability." Organizations are no longer just governing static records; they are governing decision-making engines that learn and evolve. Bone [10] identifies a significant gap in this area, noting that internal auditors are expected to conduct AI engagements despite a distinct lack of established standards and guidance. This "governance gap" allows AI systems to operate as black boxes, potentially ingesting low-quality or biased data and producing flawed outputs that carry legal and reputational risks. The question then arises: how does one govern a system that is non-deterministic?

Moreover, the integration of Agile methodologies in software development has created friction with traditional, compliance-heavy governance models. Bordey [11] explores the concept of "Agile in data governance," arguing that if governance processes are too rigid, they will be bypassed by development teams prioritized on speed to market. This necessitates a "governance by design" approach, where policies are embedded into the continuous integration/continuous deployment (CI/CD) pipeline rather than enforced as a post-hoc checkpoint.

This article seeks to address these converging challenges by conducting a comprehensive analysis of the current state of data governance literature. By synthesizing insights from cloud governance, digital forensics, and AI auditing, we aim to construct a multidimensional view of "Digital Trust." We examine how organizations can move from reactive compliance to proactive stewardship, ensuring that the data fueling the next generation of innovation is secure, accurate, and ethically managed.

2. METHODOLOGY

To achieve a robust synthesis of the evolving data governance landscape, this study employs a systematic qualitative research design, leveraging Document Analysis as the primary method of inquiry. As described by Bowen [13], document analysis is a systematic procedure for reviewing or evaluating documents—both printed and electronic (computer-based and Internet-transmitted) material. This method requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge.

2.1 Research Design and Protocol

The research protocol was designed to align with the principles of a Systematic Literature Review (SLR). Following the guidance of Caldwell and Bennett [16], the review process was structured to minimize bias and ensure reproducibility. The central research question guiding the selection of literature was: "What are the critical enabling factors, dimensions, and challenges of data governance in the context of Cloud Computing, AI, and IoT?"

2.2 Data Source Selection

A comprehensive search was conducted across major academic databases. The selection process prioritized peer-reviewed journal articles, conference proceedings, and reputable industry reports published between 2014 and 2025. This timeframe was selected to capture the pivotal shift from "Big Data" hype to the practical implementation of "AI and Cloud Governance."

The inclusion criteria were strictly defined:

1. Relevance: The source must explicitly address "Data Governance," "Information Stewardship," or "Digital Trust."
2. Context: The source must discuss these

concepts in relation to modern technologies (Cloud, AI, IoT, or Big Data).

3. Rigor: The source must present empirical findings, theoretical frameworks, or validated case studies.

A total of 33 key references were selected for deep analysis. These include foundational texts on cloud governance taxonomy by Al-Ruithe et al. [2, 3, 4, 5, 6], emerging research on AI auditing by Bone [10], and investigations into multimodal machine learning by Baltrušaitis et al. [32].

2.3 Analytical Framework

The analysis of the selected documents was conducted using a thematic synthesis approach. We adopted the "Risk-Based Model" proposed by Borek et al. [12] as a lens through which to categorize findings. This model suggests that the impact of information quality (and by extension, governance) should be quantified based on the risk it poses to organizational objectives.

Additionally, we utilized the ISO/IEC 25012 and ISO/IEC 25024 standards, as discussed by Calabrese et al. [15], to provide a standardized vocabulary for data quality dimensions. By mapping the disparate definitions of "governance" found in the literature against these international standards, we were able to normalize the terminology and identify commonalities across different industry verticals (e.g., banking, healthcare, public sector).

2.4 Limitations

It is important to acknowledge the limitations inherent in this methodology. As noted by Casey [17], the field of digital forensics and data governance has a "chequered past" and a rapidly evolving future. The literature is often trailing behind the bleeding edge of technological capability. Therefore, some findings related to specific software platforms may face obsolescence. However, by focusing on frameworks and principles rather than specific tools, this study aims to provide enduring insights.

3. **RESULTS AND ANALYSIS**

The analysis of the selected literature reveals that Data Governance is no longer a monolithic discipline. It has fractured and re-assembled into a multifaceted domain that must address specific contextual challenges. The results are categorized into four primary themes: The Cloud Governance Taxonomy, The Security-Forensics Nexus, The Agile-Governance Paradox, and The Multimodal AI Frontier.

3.1 The Taxonomy of Cloud Data Governance

One of the most significant findings is the distinct separation between traditional (on-premise) governance and Cloud Data Governance (CDG). Al-Ruithe et al. [6] provide a definitive "Data Governance Taxonomy: Cloud versus Non-Cloud," highlighting that CDG is driven by different variables. In non-cloud environments, the primary constraints are internal resource availability and legacy system interoperability. In cloud environments, the primary constraints are contractual (Service Level Agreements), jurisdictional (data sovereignty), and cryptographic (encryption management).

Al-Ruithe et al. [4] identify "Key Dimensions for Cloud Data Governance" which include transparency, accountability, and standardized auditability. The literature suggests that a major barrier to cloud adoption in the public sector is the perceived inability to extend governance policies to third-party infrastructure. However, Al-Ruithe and Benkhelifa [2] utilize structural equation modeling to show that when clear "enabling factors"—such as defined security policies and trust mechanisms—are present, the resistance to cloud migration decreases significantly.

3.2 The Security-Forensics Nexus in Converged Environments

As organizations move to "Converged Environments" where Cloud and IoT intersect, governance becomes indistinguishable from security. Al-Ruithe et al. [7] discuss "Data Governance for Security in IoT & Cloud Converged Environments," arguing that the massive influx of data from edge devices (IoT) into central cloud repositories creates a chain-of-custody nightmare.

Casino et al. [18] support this by reviewing trends in digital forensics, noting that traditional forensic methods (disk imaging) are impossible in cloud environments. Therefore, governance policies must mandate "forensic readiness"—the proactive design of logging and data retention strategies that allow for post-incident investigation. Without governance policies that enforce detailed logging at the API level, organizations are left "blind" during a security incident.

Furthermore, Bindley [9] emphasizes "Joining the dots" between compliance and governance. Security cannot be an isolated function; it must be part of the governance structure. If the governance framework does not explicitly address how encryption keys are managed or how data is destroyed at the end of its lifecycle, the organization is compliant on paper but vulnerable in practice.

3.3 The Agile and Workflow Integration

A critical tension identified in the literature is the conflict between the speed of software delivery and the slowness of governance checks. Aunimo et al. [22] explore "Big data governance in agile and data-driven software development," finding that traditional "gatekeeper" governance models cause bottlenecks that Agile teams inevitably bypass.

Bordey [11] proposes an "Agile in data governance design" approach. This involves decentralizing governance responsibilities. Instead of a central Data Governance Office reviewing every schema change, governance rules (e.g., "no PII in logs") are codified into automated testing suites. This aligns with the findings of Alhassan et al. [20, 21], who identify "Critical Success Factors" for governance. They argue that governance must be integrated into the workflow of the organization. If governance is seen as an external imposition, it will fail; if it is part of the daily workflow (as discussed by Azeroual et al. [25] regarding deduplication workflows), it becomes sustainable.

3.4 Deep Dive: The Convergence of Multimodal Data Fusion and Governance Architectures

This section represents a significant expansion of the analysis, addressing the complex requirements of governing complex, non-tabular data streams.

While the governance of structured text and numerical data is well-documented, the current literature reveals a profound, widening gap in the governance of multimodal data. As AI systems increasingly mirror human perception, they do not rely solely on rows and columns; they consume and synthesize audio, visual, textual, and sensor data simultaneously. This phenomenon, known as Multimodal Data Fusion, presents an unprecedented challenge to traditional governance frameworks which are inherently schema-based.

Lahat et al. [29] define multimodal data fusion as the analysis of data from multiple disjoint sources to gain insights that are not visible when looking at a single modality. In the context of governance, this implies that a policy applied to a single data stream (e.g., a video feed) is insufficient if the risk arises from the combination of that feed with another stream (e.g., audio or biometric sensors). For instance, a video feed of a public space might be anonymized and compliant on its own. However, if that visual data is fused with audio data that captures voiceprints, or with sensor data that captures gait analysis, the "anonymized" subject can be re-identified. Traditional governance, which tends to tag and classify assets in isolation, fails to capture the "emergent risk" of fusion.

Baltrušaitis et al. [32] provide a taxonomy of multimodal machine learning that highlights the complexity of "alignment" and "representation." From a governance perspective, "alignment" refers to the synchronization of data streams. If a healthcare AI aligns a patient's ECG data with their video consultation record, the governance framework must maintain the integrity of the synchronization. A misalignment caused by data quality issues could lead to a misdiagnosis. Therefore, governance policies for multimodal systems must include strict quality controls for temporal and spatial alignment, distinct from simple data accuracy.

3.4.1 Governance in Health Data Hubs and Wearables

The stakes of multimodal governance are highest in the healthcare sector. Alvarez-Romero et al. [28] analyze "Health data hubs" and the existing governance features for research. They find that while these hubs often have robust security for Electronic Health Records (EHR), they struggle to govern the unstructured data flowing from new sources.

Bayoumy et al. [33] elaborate on this in the context of "Smart wearable devices in cardiovascular care." Wearables generate a continuous stream of physiological data (heart rate, movement, sleep patterns). This data is often "grey data," a concept touched upon by Borgman [13], encompassing data that is produced outside of formal institutional publishing or commercial distribution channels. Governing this grey data requires a framework that can handle high-velocity streams that may be inherently noisy or incomplete.

Bayoumy et al. [33] suggest that the governance of this data cannot be strictly centralized. Instead, "Edge Governance" is required, where data quality checks and privacy masking occur on the device (the wearable) before the data is transmitted to the cloud. This reduces the privacy blast radius and ensures that only high-value, governed data enters the central repository. However, this requires a level of interoperability and standardization that is currently lacking in the consumer IoT market.

Ayappane et al. [24] propose a "Consent Service Architecture" for policy-based consent management in data trusts. This is critical for health data. In a multimodal environment, a patient might consent to the use of their heart rate data but not their location data. If the wearable device transmits both as a fused packet, the governance system must be sophisticated enough to unbundle the stream and suppress the non-consented modality. Current binary consent models (Yes/No to "Data Collection") are insufficient for the granularity required in multimodal AI.

3.4.2 Algorithmic Auditing and the "Black Box"

The governance of the AI models that process this multimodal data is equally critical. Bone [10] argues that auditing artificial intelligence is the new frontier for internal auditors. However, unlike financial auditing, where the rules of accounting are fixed, the "rules" of a neural network are emergent and often opaque.

Aldoseri et al. [19] propose a methodological approach to assessing the readiness of organizations for AI-based digital transformation. They argue that readiness is not just about having the right GPUs; it is about having the "Governance Readiness" to monitor model drift and bias. For example, if a multimodal model trained on video and audio begins to show bias against certain accents or skin tones, the governance framework must be able to detect this "Data Shift."

Brown and Anderson [26] discuss methodologies for preprocessing structured big data in the behavioral sciences. Their findings are applicable here: the preprocessing pipeline is often where governance fails. If the cleaning algorithms inadvertently remove data features that are correlated with a protected class (e.g., accidentally filtering out dialect-heavy audio), the resulting dataset is biased. Governance must therefore extend into the feature engineering phase of the data science lifecycle.

3.4.3 The Role of Data Trusts

To manage these complexities, the concept of "Data Trusts" has emerged. Austin and Lie [23] analyze the failure of Sidewalk Labs' Urban Data Trust to highlight the limitations of corporate-led governance in smart environments. They argue that a Data Trust must be a legally distinct entity with a fiduciary duty to the data subjects, not the data collectors. In a multimodal smart city environment (cameras, sensors, traffic data), a Data Trust acts as the governance intermediary, negotiating the terms of data fusion and access. This structural separation of "Custodian" (the Trust) and "User" (the AI developer) may be the only viable model for maintaining public trust in pervasive computing environments.

3.5 Quantitative vs. Qualitative Governance Metrics

Elshawi et al. [27] discuss "Big Data Systems Meet Machine Learning Challenges," noting that one of the primary challenges is the definition of success metrics. In traditional governance, success is binary: "Is the data accurate? Yes/No." In AI governance, success is probabilistic: "Is the model 95% confident?"

Governance frameworks must therefore evolve to handle probabilistic metrics. An Z et al. [22] research data governance for fire departments, a critical safety domain. They find that governance frameworks must establish "Confidence Thresholds." If data quality drops below a certain probabilistic threshold, the governance system should automatically trigger a "Circuit Breaker" that prevents the data from being used in automated decision-making. This concept of Automated Governance Enforcement is a recurring theme in the most recent literature, suggesting a move away from human-speed auditing to machine-speed policing.

4. **DISCUSSION**

4.1 Toward a Dynamic "Digital Trust" Framework

Synthesizing the findings from the cloud taxonomy, security convergence, and multimodal challenges, it becomes evident that the static governance models of the past decade are insufficient. We propose the concept of "Dynamic Digital Trust." This framework posits that governance cannot be a set of static documents; it must be a continuous, algorithmic process.

As highlighted by Al-Ruithe et al. [5] in their review of data governance literature, the field is moving toward "Policy-as-Code." Just as infrastructure is now defined by code (IaC), governance policies must be machine-readable constraints that live within the cloud environment. For example, a policy stating "No sensitive data in public buckets" should not be a line in a PDF document; it should be a script that runs continuously against the cloud environment, automatically remediating violations.

4.2 Implications for Industry and Policy

For practitioners, particularly in the insurance and banking sectors mentioned by Rajgopal and Yadav [1], the implications are clear: invest in "Metadata Management." Metadata is the leverage point for governance. By tagging data with context (origin, consent level, sensitivity, modality), automated systems can enforce governance at scale.

Furthermore, the "Human in the Loop" remains essential, but their role changes. Instead of checking individual records, the human governor checks the logic of the automated governance agents. This elevates the Data Governance Officer from a custodian to a systems architect.

4.3 Limitations and Future Research

The primary limitation of this study—and indeed of the field—is the lag between technological capability and regulatory understanding. As noted by Borgman [13], universities and regulators are often at the "privacy frontier," struggling to define the legal status of new data types (like grey data) before the market has already exploited them.

Future research must focus on "Federated Governance." As data processing moves to the edge (on-device learning), governance must follow. Research is needed into how lightweight governance protocols can be embedded into low-power IoT chips, ensuring that even the smallest sensor is a "citizen" of the governance ecosystem. Additionally, more empirical studies are needed to quantify the cost of poor governance in AI systems—specifically, the financial impact of bias and model drift—to provide a stronger business case for investment in these frameworks.

5. CONCLUSION

The digital transformation of society, driven by the convergence of Cloud, IoT, and AI, has necessitated a fundamental reimagining of Data Governance. This study has traversed the landscape of current literature to demonstrate that governance is no longer a back-office compliance function but the front-line defense of digital integrity.

We have identified that Cloud Data Governance requires a distinct taxonomy centered on shared responsibility and cryptographic trust. We have shown that in converged environments, security and governance are inextricably linked, with digital forensics depending entirely on the quality of governance logging. Most crucially, we have explored the frontier of Multimodal AI, arguing that the fusion of disparate data streams creates emergent risks that require sophisticated, probability-based governance interventions.

The "missing approach" identified by Barker [8] almost a decade ago is now being filled by a new generation of "Agile," "Automated," and "Context-Aware" governance frameworks. For organizations to navigate the future safely, they must embrace these dynamic models, recognizing that in the age of AI, to govern data is to govern the very logic of the enterprise.

REFERENCES

1. Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). Methodological approach to assessing the current state of organizations for AI-Based digital transformation. Applied System Innovation, 7(1), 14.
2. Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. Journal of Decision Systems, 25(sup1), 64–75.
3. Alhassan, I., Sammon, D., & Daly, M. (2019). Critical success factors for data governance: A theory Building approach. Information Systems Management, 36(2), 98–110.
4. Al-Ruithe, M., & Benkhelifa, E. (2018). Determining the enabling factors for implementing cloud data governance in the Saudi public sector by structural equation modelling. Future Generation Computer Systems, (article in press), 1-16.
5. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2016a). A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science, 94, 160-167.
6. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2016b). Key Dimensions for Cloud Data Governance. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 379-386.
7. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018a). A systematic literature review of data governance and cloud data governance. Personal and Ubiquitous Computing, 1-21.
8. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018b). Data Governance Taxonomy: Cloud versus NonCloud. Sustainability, 10(1), 1-26.
9. Al-Ruithe, M., Mthunzi, S., & Benkhelifa, E. (2016c). Data Governance for Security in IoT & Cloud Converged Environments. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 1-8.
10. Alvarez-Romero, C., Martínez-García, A., Bernabeu-Wittel, M., & Parra-Calderón, C. L. (2023). Health data hubs: An analysis of existing data governance features for research. Health Research Policy and Systems, 21, 70.
11. An, Z., Zhang, D., & Liang, Y. (2021). Research on Data Governance Framework for Fire Department. ACM International Conference Proceeding Series.
12. Aunimo, L., Alamäki, A. V., & Ketamo, H. (2019). Big data governance in agile and data-Driven software development: A market entry case in the educational game industry. IGI Global.
13. Austin, L. M., & Lie, D. (2021). Data trusts and the governance of smart environments: lessons from the failure of sidewalk labs' urban data trust. Surveillance & Society, 19(2), 255–261.
14. Ayappane, B., Vaidyanathan, R., Srinivasa, S., Upadhyaya, S. K., & Vivek, S. (2024). Consent Service Architecture for Policy-Based Consent Management in Data Trusts. ACM International Conference Proceeding Series, 155–163.
15. Azeroual, O., Nikiforova, A., & Sha, K. (2023). Overlooked Aspects of Data Governance: Workflow Framework for Enterprise Data Deduplication. International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS),

65–73.

16. Baltrušaitis, T., Ahuja, C., & Morency, L. P. (2019). Multimodal Machine Learning: A Survey and Taxonomy. IEEE Transactions on Pattern Analysis and Machine Intelligence, 41, 423–443.
17. Barker, J. M. (2016). Data Governance: The missing approach to improving data quality. ProQuest LLC.
18. Bayoumy, K., Gaber, M., Elshafeey, A., Mhaimeed, O., Dineen, E. H., Marvel, F. A., Martin, S. S., Muse, E. D., Turakhia, M. P., Tarakji, K. G., et al. (2021). Smart wearable devices in cardiovascular care: Where we are and how to move forward. Nature Reviews Cardiology, 18, 581–599.
19. Bindley, P. (2019). Joining the dots: How to approach compliance and data governance. Network Security, 2019(2), 14–16.
20. Bone, J. (2020). Auditing artificial intelligence: Internal auditors can develop a framework for conducting AI engagements, despite a lack of standards and guidance. Internal Auditor, 77(5), 20–21.
21. Bordey, G. (2018). Agile in data governance design. Business Intelligence Journal, 23(2), 23–32.
22. Borek, A., Parlikad, A. K., Woodall, P., & Tomasella, M. (2014). A risk based model for quantifying the impact of information quality. Computers in Industry, 65(2), 354–366.
23. Borgman, C. L. (2018). Open data, grey data, and stewardship: Universities at the privacy frontier. Berkeley Technology Law Journal, 33(2), 365–412.
24. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal.
25. Brown, P. A., & Anderson, R. A. (2023). A methodology for preprocessing structured big data in the behavioral sciences. Behavior Research Methods, 55, 1818–1838.
26. Burniston, T. R. (2015). Data governance. ABA Banking Journal, 107(4), 56–57.
27. Calabrese, J., Esponda, S., & Pesado, P. M. (2020). Framework for data quality evaluation based on ISO/IEC 25012 and ISO/IEC 25024. VIII conference on cloud computing, big data & emerging topics.
28. Caldwell, P. H., & Bennett, T. (2020). Easy guide to conducting a systematic review. Journal of Paediatrics and Child Health, 56(6).
29. Casey, E. (2019). The chequered past and risky future of digital forensics. Australian Journal of Forensic Sciences, 51(6), 649–664.
30. Casino, F., Dasaklis, T., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access, 10, 1−1.1
31. Elshawi, R., Sakr, S., Talia, D., & Trunfio, P. (2018). Big Data Systems Meet Machine Learning Challenges: Towards Big Data Science as a Service. Big Data Research, 14, 1–11.2
32. Lahat, D., Adali, T., & Jutten, C. (23015). Multimodal Data Fusion: An Overview of Methods, Challenges, and Prospects. Proceedings of the IEEE, 103, 1449–1477.
33. Rajgopal, P. R., & Yadav, S. D. (2025). The role of data governance in enabling secure AI adoption. International Journal of Sustainability and Innovation in Engineering, 3, 1–25.