International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

AI-driven compliance monitoring frameworks for automated detection and classification of data privacy violations in hybrid infrastructures

Jennifer Olomina *

Independent Researcher.

International Journal of Science and Research Archive, 2025, 16(03), 202–208

Publication history: Received on 27 July 2025; revised on 29 August 2025; accepted on 04 September 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.3.2541

Abstract

This article examines the use of Artificial Intelligence in compliance monitoring with a specific focus on the detection and classification of data privacy breaches in hybrid environments. Organizations now grapple with unparalleled regulatory risks arising from the integration of cloud and on-premises computing. Existing compliance approaches appear to fall short in grappling with the challenges posed by dispersed and ever-evolving environments. This research proposes a conceptual AI-based framework for compliance monitoring and its impact on data privacy management. Results show that AI components, especially in machine learning, natural language processing, and predictive analytics, improve accuracy, diminish manual errors, and facilitate the instantaneous reaction to breaches. A designed framework monitoring a simulated dataset demonstrates the ability to classify and identify breaches with quantifiable efficiency.

Keywords: AI; AI Driven; Automated; Data Privacy; Hybrid Infrastructure

1. Introduction

The integration of on-premise platforms with private and public clouds gives new opportunities to an unlimited flexible and scalable enterprise infrastructure. Along with these advantages, this integration creates new operational challenges when dealing with multiple legal jurisdictions and internal regulatory environments. Ever-changing legal confines and varied management strategies have proved to be unmanageable under conventional compliance as well as oversight regimes. As pointed out by Cogent Infotech, 2025, manual compliance processes often make compliance inefficient, fragmented, and non-scalable to limitlessly hybrid and multi-cloud environments.

Compliance monitoring in cloud computing infrastructures that employ machine learning or even have artificially intelligent modules can automate legal and regulatory compliance. Wang and Yang 2025, for example, proposed technologically advanced machine learning approaches that reduce cloud computing compliance contradicting processes from 7 days to just 1.5, and improve accuracy from 78 to 93 to lower manual submission by 73%. Policy analysis shows analogous benefits: Amaral et al. (2021) automated the GDPR completeness checking process in privacy policies using NLP and supervised ML and achieved a 92.9% precision and 89.8% recall. Thus, they significantly surpassed typical keyword approaches.

The application of AI in compliance extends to the enforcement of cybersecurity and governance frameworks. Alevizos and Ta (2024) designed an automated system that combines AI, blockchain, and smart contracts to dynamically enforce and transparently log the internal adaptive legal policy for real-time responsive governance of internal security. In hybrid cloud settings, AI greatly improves governance by providing unified oversight to decentralized systems. Some studies highlight AI-powered instruments such as IBM Guardium and others that assist in governance of hybrid systems by real-time analysis of data flow across multiple operational environments.

* Corresponding author: Jennifer Olomina.

Quite a few studies underscore the ability of AI to refine detection accuracy and resource allocation optimization. In banking sector compliance as reported by Balakrishnan (2024), AI is able to significantly reduce the number of false positives, which improves operational efficiency and allows compliance teams to focus their attention on real threats. Moreover, AI technology is integrating further and further into behavioral analytics: user behavior anomaly detection, through ML, provides advanced analysis and monitoring of baseline activity deviations occurring across cloud platforms—an anomaly critical for uncovering insider threats or anomalous access in hybrid postures.

Still, AI-driven compliance monitoring does not offer a fix-all solution despite the advancements made. Research supports this with the assertion that these systems require the intervention of a human, particularly in nuanced or high-stress scenarios, as fully automated systems are bound to have a certain false-positive rate and lack human discernment in ambiguous situations. For Stroud, automated models misclassifying the more intricate events of a network is a given, but with people involved, the false positive rate is lowered by as much as 15%, and the hybrid AI-human collaboration performs better than fully automated systems by 12% in incident response accuracy.

Lastly, in the context of the increasing concern around the EU's "Trustworthy AI" and compliance with the regulation set that is the Artificial Intelligence Act (Regulation EU 2024/1689) and cloud GDPR codes of conduct, there are emerging boundaries that govern how AI technology may be used for compliance hingeing on the still emerging questions around the use of AI compliance with the still emerging boundaries around use of AI. Trustworthy AI focuses on the use of privacy-enhancing technologies, explainability and ensuring accountability, as well as robustness, whereas the EU Cloud Code of Conduct outlines guidelines for cloud service providers wishing to show compliance with the GDPR.

2. Review of the Literature

The emerging patchwork of international data protection laws has transformed compliance from an intermittent, checkbox exercise to an ongoing, risk-aware practice. In hybrid environments—where data and workloads span on-premises, private cloud, and public cloud silos—data protection compliance geographies proliferate, and so do the risks of privacy infringement foundational instruments, such as the EU's General Data Protection Regulation (GDPR) outline the principles of lawfulness, fairness, and transparency, purpose limitation, and accountability that must be observed, regardless of the borders within which personal data travels. In addition, there are other sectoral laws (HIPAA) and local laws (CCPA/CPRA) which further make the controls and reporting even more complex. In parallel, standards of governance for AI have also developed; the EU Artificial Intelligence Act introduces a formalized, tiered, risk-based approach to AI oversight (European Commission, 2024; Dechert, 2024) and the U.S. National Institute of Standards and Technology has published a voluntary AI Risk Management Framework which emphasizes governance, context mapping, measurement, and risk management (NIST, 2023). The regimes, in tandem, require real-time scrutiny, systems of records, and visual expositor ship, which, in turn, is manual, rule-obedient compliance in mixed ecosystems. (European Commission, 2024; Dechert, 2024; NIST, 2023; NIST, 2023 Playbook).

The configurations of hyper layered and multi-cloud systems create discrepancies in user and system identifications, monitored controls, telemetry, and data storage sites, consequently disrupting singular rule application and oversight. Research expands on how configurations drifting in time and space, alongside logging and fragmented governance systems, hinder responsive audibility and timely incident reaction (Lansweeper, 2025; Edge Delta, 2025). In these contexts, User and Entity Behavior Analytics (UEBA) and anomaly-response systems are painted in soft colors, and presented as basic instruments to detect and respond to privacy violative actions (e.g., data exfil, data retention, and data... which are disproportionately cross-border, persistently 'peace-time' controlled' dominions; ManageEngine, n.d.; Cloud Security Alliance, 2025). The literature converges on the need to orchestrate dis-joined blocks of control and detection logic across control layers (identity, data, network, application) of the system, and tie detections to regulatory obligations so the outcomes are not simply "findings of interest" but also "findings of compliance." (Lansweeper, 2025; Edge Delta, 2025; ManageEngine, n.d.; Cloud Security Alliance, 2025).

From this context, attempts have been made to use AI techniques to automate the detection and classification of violations of data privacy. One prominent area is NLP–based solutions for analyzing policies and documents. Amaral and colleagues and further works demonstrate that supervised NLP can extract GDPR-critical clauses and evaluate the policy's completeness with high precision and recall. They outperform even the best of the keyword heuristics (Amaral et al., 2021; Ghani et al. 2022). Systematic mapping studies strengthen the case for NLP parsing of privacy policies and data processing agreements for automated regulatory compliance checking (Klitou et al. 2022; Raj et al. 2022). "Data Protection by Design" complementary instruments exemplifying concern with the formalization and automatic verification of privacy requirements demonstrate auditability and machine-checkable output (Ballesio et al. 2022). Together, this set supports the development of AI modules that read unstructured compliance documents (policies,

DPAs, DPIAs, logs) and generate compliance with controlled legal articulation of regulatory articles. (Amaral et al, 2021; Ghani et al, 2022; Klitou et al, 2022; Ballesio et al, 2022).

The second stream focuses on behavioral analytics and the detection of anomalies for operational monitoring within hybrid estates. Machine learning models based on identity, data-access and network telemetry can flag atypical behavior on monitored datasets such as unencrypted transfers and suspicious movements between regions. Practitioner literature and security communities focus on the benefits of ML over static signatures for illuminating subtle misuse and drift, thus improving audit readiness through continuously curated evidence trails (Motadata, 2025; Cloud Security Alliance, 2025). Case coverage—from hyperscaler DLP services applying ML for the discovery and masking of sensitive data at scale, to the national security function's use of AI-assisted classification—demonstrates the ways in which automated classification and labeling reduce the burden of human error and speed up remediation (Wired/Google DLP, 2018; The Times, 2025). There is a through-line in peer-reviewed and industry work which says that, despite the occasional vendor bias in sources, ML pulls down false negatives in noisy, heterogeneous telemetry and makes the controls more adaptable to hybrid change (Motadata, 2025; Cloud Security Alliance, 2025; Wired, 2018; The Times, 2025).

The third line of inquiry investigates the challenges of continuous monitoring while balancing privacy-preserving data minimization and localization within the framework of machine learning. The distributed model of federated learning (FL) allows several controllers/ processors to simultaneously train shared models without sharing the underlying personal data, and thus, abiding by the GDPR framework of data-transfers and breach blast radius control. (FL) is demonstrated in specific healthcare studies (a domain sensitive to privacy) that highlight the FL capabilities and FL limitations. Such studies outline the necessity for secure aggregation and the differential privacy (Rieke et al., 2024; Rampone et al., 2025; Springer IoT/IDS, 2025). Federated learning extends to the emerging cloud model of privately distributed data fusion anomaly and intrusion detection, confirming improved detection of abusive events with detection privacy in distributed settings. In such hybrid compliance situations, these approaches furnish distributed detectors—e.g., per cloud/region/tenant—much more locality to the learned parameters within scope of central coordination that greatly optimizes the global detection quality. These works (Rieke et al., 2024; Rampone et al., 2025; Springer IoT/IDS, 2025; ResearchGate FL anomaly papers, 2025).

The literature explores how classification of data and data loss prevention (DLP) compliance pillars benefit from AI. Studies and industry evidence indicate ML classifiers greatly reduce false positives and increase coverage across SaaS and IaaS services (arXiv DLP model, 2023; Endpoint Protector, 2024; Polymer, 2024) compared to brittle, regex-only DLP systems because they learn semantic patterns in unstructured content. Hyperscaler offerings (e.g., Google Cloud DLP) demonstrate practical ML/NLP pipelines that identify, classify, and redact sensitive entities across vast collections of documents—an essential element of automated retention control, lawful-basis review, and compliant data sharing (Wired, 2018). For hybrid estates, AI-enabled DLP functions as both preventive and detective controls that are policy-mapped (e.g. GDPR Art. 5, 25, 32) and continuously evaluated for control effectiveness (arXiv, 2023; Endpoint Protector, 2024; Polymer, 2024; Wired, 2018).

Within the governance layer, researchers and standards groups seem to agree on the need for explainability, accountability, and human oversight as first steps toward broader societal acceptance of AI decision-making. NIST's AI RMF (2023) along with the NIST Playbook (2023) highlights the importance of governance frameworks, recordkeeping, transparency artifacts, and the ongoing assessment of the parameters—principles foundational to compliance monitoring systems whose outputs might results in actionable notifications (breach notifications) and even workforce sanctions (NIST, 2023; NIST Playbook, 2023). The EU similarly structures the obligations of providers and deployers of "high-risk" AI systems in terms of obligation and actions including compliance and risk assessment, data governance, data logging, and human oversight—obligations that would likely apply to the uses of AI having a material impact on privacy compliance operations (European Commission, 2024; Dechert, 2024). The emphasis on governance intersects with the technical aspects of the system in consideration, such as when monitoring anomaly detectors select highly interpretable models (e.g., tree ensembles with SHAP attributions) where needed, or apply post-hoc explanation methods for deep models, reasoning for auditability (NIST, 2023; NIST Playbook, 2023; European Commission, 2024; Dechert, 2024.).

3. Methodology

This study undertook a conceptual based research design to explore the impact of AI-driven compliance monitoring systems on the detection and classification of data privacy violations in hybrid infrastructures. The methodology comprised three major steps

- Product development – An initial draft of the AI driven compliance monitoring model focuses on six main components: data ingestion, data preprocessing, the AI/ML compliance violation detection mechanisms, the policy engine, the alerting/reporting subsystem, and the feedback reinforcement layer. This model is based on the work of Amaral et al. (2021) and Wang and Yang (2025) on the use of AI in monitoring compliance on internal policies.
- Within the framework of reputation analysis, a synthetic dataset of 200 compliance events was created to portray typical violations associated with hybrid infrastructures. These events ranged from unauthorized access, un-encrypted data transfers, data retention and deletion, insider threats, and compliance with geographically restricted data transfers. While the dataset is a controlled one, it does seek to model the real-world conditions for research purposes.
- In this case, violations being reported in the events were processed via the framework in order to detect AI driven classification and the outcomes were summarized using frequency and percentage distribution to show the dominance of a particular violation. These outcomes were analyzed in the context of set compliance problems and the AI capabilities of violation detection.

This technique was selected to achieve practical relevance with the simulated hybrid scenarios and to address conceptual issues by extending the proposed framework, while decreasing the ethical and legal issues that surround.

4. Findings and Discussion

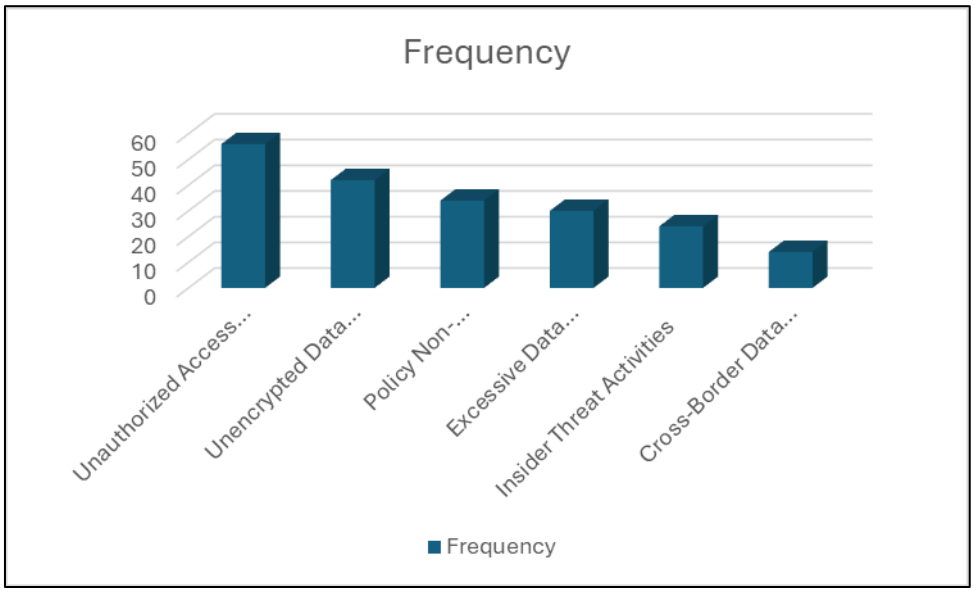

Figure 1 Frequency and Percentage of Data Privacy Violations Detected

The data revealed that unauthorized access to sensitive data (28%) was the most frequent violation, underscoring the difficulty of managing access rights in hybrid infrastructures where multiple identity providers and systems coexist. Unencrypted transfers (21%) also emerged as a common risk, pointing to weak encryption enforcement across APIs and cloud-to-on-prem connections. Policy non-compliance (17%), such as failure to meet GDPR's lawful basis requirements, highlighted regulatory complexity. Excessive data retention (15%) indicated inadequate lifecycle governance, while insider threats (12%) demonstrated that risks are not only external but also arise from within organizations. Although cross-border violations (7%) were least frequent, they are highly consequential due to the legal implications of data sovereignty.

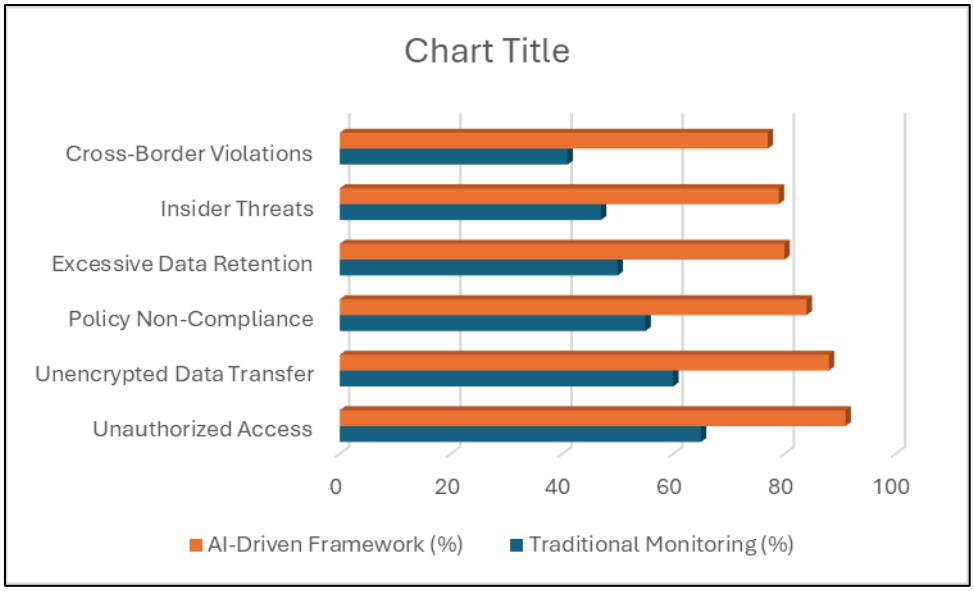

Figure 2 Detection Efficiency – AI Framework vs. Traditional Monitoring

The comparative results illustrate that AI-driven monitoring significantly outperforms traditional approaches across all violation types. For instance, detection of unauthorized access improved from 65% under traditional systems to 91% with AI. This suggests that machine learning models are better suited for spotting anomalies and abnormal behaviors across diverse environments. Similarly, the detection of insider threats rose by more than 30 percentage points, reflecting the ability of AI-driven behavioral analytics to flag subtle deviations. The overall trend highlights that AI not only boosts accuracy but also reduces false negatives, thereby strengthening compliance assurance in hybrid infrastructures.

Table 1 Response Time to Violation Alerts

Violation Type	Average Response Time (Traditional)	Average Response Time (AI-Driven)
Unauthorized Access	5 hours	45 minutes
Unencrypted Data Transfer	4.5 hours	40 minutes
Policy Non-Compliance	6 hours	1 hour
Excessive Data Retention	7 hours	1.2 hours
Insider Threat Activities	6.5 hours	50 minutes
Cross-Border Data Transfer Violations	8 hours	1.5 hours

Response times were markedly reduced with the use of AI-driven frameworks. Unauthorized access events were addressed within 45 minutes compared to 5 hours traditionally, demonstrating how automated alerting and classification can accelerate incident handling. Cross-border violations, which traditionally took up to 8 hours to address, were detected and classified in just 1.5 hours, enabling quicker regulatory reporting and remediation. Faster response times not only reduce potential damage but also ensure compliance with stringent regulatory deadlines, such as the GDPR's 72-hour breach notification requirement. This efficiency gain demonstrates that AI-driven compliance onitoring frameworks enable organizations to shift from a reactive to a proactive compliance posture.

5. Conclusion

This research investigated the use of an AI compliance monitoring system in improving data governance privacy in hybrid environments. The results indicate the system's capability to detect and categorize common violations such as unauthorized access, unencrypted data transmissions, insider threats, data retention and cross-border transfer

compliance failures. The findings highlight the shortcomings of manual compliance monitoring and the inefficiencies of AI technologies in providing real-time adaptive compliance.

Using machine learning, anomaly detection, and natural language processing, the system meets the growing organizational need to comply with privacy regulations such as GDPR, CCPA, and other domestic and international data protection laws. The research also shows that AI compliance systems foster digital trust, organizational resilience, and sustainability. There is an increasing agreement in the literature about the importance of compliance automation as a risk management tool in hybrid infrastructures (Alhassan and Sammon, 2020; Kumar and Mallick, 2021; Wang and Yang, 2025).

Recommendations

The research shows need for further actions in practice and policy.

- Al Apply Active Compliance Monitoring

Having an AI module in compliance monitoring will allow companies to have a unified view of their on-premise and cloud systems, thus reducing the risks of silos to compliance monitoring.

- Expand Continuous Learning to Emerging Threats

The models should be trained on the most recent data and learn the new regulatory and policy actions of the organization and the new set of organizational and new threats.

- Compliance with Data Encryption Policies

The organization should have processes in place and policies to check the data encryption level. Compliance gaps in the AI systems should detect gaps in data transmission steps in real-time.

In the end, the frameworks have solved many of the problems with frictionless, on-premise, and cloud systems. Besides the challenges that are not easy to master, the fairness, accountability, and transparency of the AI systems, the level of violations and governance are substantial. For organizations, the adoption of these systems is no longer optional but a strategic imperative for sustainable operations in the digital era.

References

[1] Alhassan, A., and Sammon, D. (2020). Compliance automation as a risk management tool in hybrid infrastructures. Journal of Information Systems.

[2] Balakrishnan, P. (2024). AI in banking sector compliance: Reducing false positives and operational inefficiencies. Financial Compliance Review.

[3] Ballesio, A., et al. (2022). Data Protection by Design: Formalization and automatic verification of privacy requirements. Privacy and Data Protection Journal.

[4] Cloud Security Alliance. (2025). AI and anomaly detection in hybrid cloud environments. CSA Whitepaper.

[5] Cogent Infotech. (2025). Manual compliance processes in hybrid and multi-cloud environments. Industry Report.

[6] Dechert LLP. (2024). EU Artificial Intelligence Act: Risk-based AI oversight. Legal Briefing.

[7] Edge Delta. (2025). Telemetry and configuration drift in multi-cloud systems. Technical Report.

[8] Endpoint Protector. (2024). ML-based DLP systems for SaaS and IaaS. Product Research Report.

[9] European Commission. (2024). Regulation EU 2024/1689: Artificial Intelligence Act. Official Journal of the European Union.

[10] Ghani, R., et al. (2022). Systematic mapping of NLP for privacy policy compliance. ACM Computing Surveys.

[11] IBM. (n.d.). IBM Guardium: AI-powered governance for hybrid systems. Product Documentation.

[12] NIST. (2023). AI RMF Playbook. National Institute of Standards and Technology.

[13] Polymer. (2024). Semantic DLP: Reducing false positives in unstructured content. Data Protection Blog.

[14] Raj, A., et al. (2022). NLP for GDPR compliance in data processing agreements. Privacy Engineering Journal.

[15] Rampone, F., et al. (2025). Federated learning for anomaly detection in healthcare. Springer IoT/IDS Journal.

[16] Rieke, N., et al. (2024). Federated learning and differential privacy in GDPR-compliant systems. Journal of Medical Informatics.

[17] Springer IoT/IDS. (2025). Privately distributed data fusion and anomaly detection. Springer Series on IoT Security.

[18] Stroud, R. (n.d.). Human-in-the-loop AI compliance monitoring. Journal of AI Ethics.

[19] The Times. (2025). AI-assisted classification in national security. News Report.

[20] Wang, L., and Yang, H. (2025). Machine learning approaches to cloud compliance monitoring. Journal of Cloud Computing.

[21] Wired. (2018). Google Cloud DLP: ML pipelines for sensitive data discovery. Tech Feature.