JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2022, VOL 5, NO S12

AI-Driven Risk Assessment And Compliance Automation In Multi-Cloud Environments

Durga Bramarambika Sailaja Varri

Independent Researcher ORCID ID: 0009-0009-0437-605X

Abstract—This work explores how available AI techniques can be deployed to automatically assess risks and enforce compliance across multi-cloud environments. First, the unique nature of cloud environments suggests a revised risk taxonomy applied across all service providers, which provides the basis for an anomaly-detection architecture with cloud-specific feature engi- neering. Second, differences between provider compliance policies are analyzed for an automated on-the-fly translation that enables continuous monitoring across multi-cloud installations. The find- ings contribute to the establishment of an AI-driven foundation for governance, risk, and compliance that simultaneously satisfies needs for organization, third-party, data, and service governance. The analysis also initiates a discussion of support for business- governance and data-governance constituencies, areas where little attention has been paid to cloud risk and compliance techniques despite the sensitive nature of many of the stored resources.

Index Terms—Multi-Cloud Risk Taxonomy, Cloud-Specific Feature Engineering, Anomaly Detection Architecture, Auto- mated Compliance Translation, Continuous Compliance Moni- toring, Provider Policy Variability, AI-Driven Governance, Cloud Risk Assessment, Compliance Enforcement, Third-Party Gov- ernance, Service Governance, Data Governance, Organizational Governance, Cloud Security Posture, Real-Time Risk Analytics, Cross-Cloud Monitoring, Governance–Risk–Compliance Integra- tion, Sensitive Resource Protection, Policy Harmonization, Auto- mated Risk Intelligence.

I. INTRODUCTION

Organisations are increasingly moving to a multi-cloud strategy, relying on multiple – publicly and privately-operated – cloud infrastructure services to run their applications and services. Security and compliance risks do not reduce. On the contrary, operating in multi-cloud environments raises new risks that need to be addressed; the growing complexity of cloud services creates new challenges for other aspects of cybersecurity (training, forensics, incident response) and especially for compliance. In cloud environments, the eval- uation of security and compliance issues often tends to be too qualitative, rather than quantitative and objective; that is, the nature of cloud services requires that an objective governance, risk and compliance framework be continually monitored and updated. A tailored approach based on artificial intelligence is presented, aimed at helping solve some of the existing gaps in risk and compliance evaluation on multi-cloud environments and services, on the basis of a consolidated cloud risk taxonomy and of a comprehensive set of principles and requirements for an effective governance of the multi-cloud

Identify applicable funding agency here. If none, delete this.

environment. The proposed system enables the semi-automatic management of such topics in the context of multi-cloud environments, while relying on an explicit risk and governance model based on a dedicated ontology.

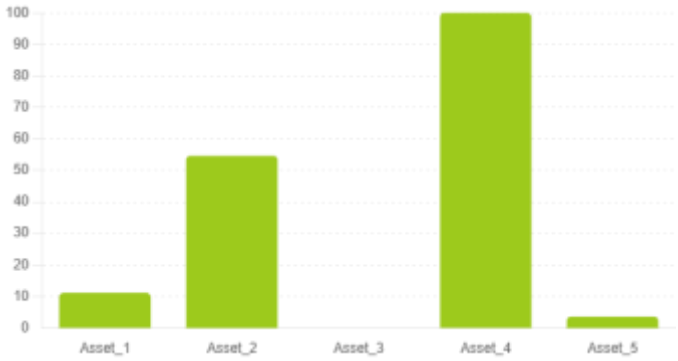
A. Overview and Objectives

Security and compliance are paramount in the cloud. Orga- nizations today depend on cloud instances delivered by third- party providers for applications and data storage. Nevertheless, multi-cloud deployments and utilizing IaaS, PaaS, and SaaS services entail risks that may lead to data loss and leakage, insecure interfaces and APIs, account and service hijacking, insider threats, abuse, and inadequate security. Although risk assessment frameworks and compliance guidelines exist, the need for continual verification is evident. Cloud providers typ- ically define security measures and security policies for their services; however, organizations are responsible for assessing the risks of combining different cloud services and monitoring the compliance of their implementations and usage. These risk aspects change dynamically, extending beyond the owner orga- nization's organizational borders and risk ownership. Although formal risk assessment processes can minimize information security risk using security controls, they often lack speed and operationalization. Existing methods are rarely capable of automating end-to-end risk assessment and assurance, or of automatically maintaining multi-cloud-compliance of all deployment stages, from design to runtime activity, through- out service usage and data lifecycles. Moreover, available risk-assessment and compliance-automation methods do not address the fundamental technical hurdles mentioned above, and associated research is scarce. For enormous, multi-cloud- compliance-assurance, executive-monitoring, public-service- provisioning systems, dynamic compliance violation and risk- state understanding, visibility, and acknowledgement is impor- tant.

Theoretical Foundations of AI-Driven Risk Assessment

The success of organizations in contemporary environments is inextricably linked to risk management and governance, which greatly influence their global competitiveness. Nevertheless, the increasing complexity of these organizations—particularly due to the growth of multicloud environments—and their processing technology makes risk assessment difficult and costly. Previous projects managing risk assessment in hybrid and multicloud contexts position the risk assessment within the classical risk assessment processes. Data analytics and AI methodologies are also introduced as means to automate risk assessment. While AI-related technologies are still being standardized and gaining maturity, topics such as data collection and feature engineering, as well as anomaly detection, user behavioral analysis, vulnerability scanning, and cyberthreat intelligence, are covered. Some of these approaches are SAR- (Security Automation and Response) based, while others are hybrid using statistical or machine-learning techniques. In terms of risk assessment within a multicloud environment, the focus is primarily

Fig. 1. Cloud Security and Compliance Challenges in Multi-Cloud Environ- ments.



Asset	ResidualExpectedLossUSD	RiskScore 0to100
Asset 1	83697.85	11.17
Asset 2	126639.19	54.6
Asset 3	72650.57	0.0
Asset 4	171538.27	100.0
Asset 5	76190.42	3.58

Fig. 2. Risk Score per Asset

$I_{ip} > 0$: monetary impact if it occurs
$X_{ip} \in [0, 1]$: exposure share (blast radius / business criticality) $E_{ip} \in [0, 1]$: control effectiveness (fraction of risk mitigated) $w_p \geq 0$, $\sum_p w_p = 1$: business weights across providers Residual expected loss per provider: $E[\text{loss}]_{ip} = (L_{ip} I_{ip} X_{ip})(1 - E_{ip})$. (1)

Aggregate residual expected loss for asset i:

$$\text{REL}_i = \sum_p w_p E[\text{loss}]_{ip} \quad (2)$$

Scaled risk score (0–100 across assets):
on implementing governance, risk, and compliance (GRC) ontologies and on ensuring privacy through data protection policies. Both are key considerations when defining a data-

$$\text{Risk Score}_i = 100 \cdot \frac{\max_j \text{REL}_j - \min_j \text{REL}_j + \varepsilon}{\text{REL}_i - \min_j \text{REL}_j}$$

(small ε avoids di (3)
governance strategy. Multi-cloud architecture maximizes the benefits of cloud solutions, particularly through the appropriate choice of provider per service. However, it also increases the effort required for compliance and risk management, leading to activities being no longer valid in real time. Consequently, the management of risk assessment and audit compliance becomes a multicloud issue, thereby increasing the overall risk for the organization. The choice of cloud providers normally relies on service functionality, security level, and price per service. None of these elements centers on audit compliance for segregation of duties and the currency of organizational operations. Multi-cloud environments also present increased

process-change dynamics, either from internal process adjustments or external service provider changes. As a result, automatic policy translation between cloud providers is essential, as the original cloud-data policies change constantly.

Equation 1: Multi-Cloud Risk Scoring Model Definitions (for asset i on provider p):
Lip ∈ [0,1]: probability of adverse event

Risk by Asset (Residual Expected Loss & Scaled Risk)

A. **Definitions and Scope**

Compliance and risk are two distinct concepts. Compliance represents an obligation to fulfill a set of requirements, while the notion of risk carries an inherent uncertainty associated with the chance of incurring a loss. Nevertheless, compliance and risk management represent two closely connected ele- ments of an organizations governance, risk management, and compliance (GRC) stack, ultimately aiming at protecting the organizations assets. Organizations therefore take a risk-based approach to their compliance effort: they prioritize the imple- mentation of those controls, out of many possible candidates, that mitigate the impact of all identified and assessed risks, or at the very least the ones they consider the most important. Governance risks arise from nonconformity with regulations, policies, standards, or other expectations related to stakeholder behaviour, business conduct, or the evolution of socio-political dynamics. It refers to the effectiveness and adequacy of the governance framework defining the decision-making structure of an organization. Inadequate decision-making or a failure to prevent violations and misconduct or to take prompt corrective action may lead to civil or criminal liability, financial losses, reputational damage, or shareholder action. Such risks occur at the level of government, regulators, and other stakeholder organizations and apply to sectors, groups, or markets as a whole.

B. **Risk Taxonomies in Multi-Cloud Environments**

Apart from data and applications, other factors also affect the cloud risk landscape. Among others, the construction and operational context of a cloud service—i.e., the topology of the service and the connectivity to other services—are determinants of the risk exposure and manifestation. For example, in a modern enterprise, such as a bank or healthcare provider, cloud services are often part of an overall hybrid environment that also includes traditional data centers or on-premises installations. Their construction is more than merely hybrid; they are flanked by multiple cloud services (e.g., SaaS/third-party) and connected (inside or outside) to other cloud providers. The enterprise end-users or customers, and the rest of the organization, may unintentionally expose the cloud services to risks while accessing from anywhere and with any device.

The companies developing software and services to mitigate exposure to risks of external parties must realize that the same type of service can be constructed by a malicious actor. This can extend to risk analysis based on threat models of the attacker or scanner and even testing services that provide the same value without causing denial to an external user. The risk landscape is also changing dynamically during the life cycle of an enterprise. The identification of emerging risks, extrapolated from known incidents and threat vectors, is a formal part of a company's governance, risk, and compliance (GRC) program. Recognizing the need for a formal taxonomy of classic risks associated with multi-cloud environments is essential for operations teams. However, the taxonomy should be referred to a formal risk catalog that provides risk statements and rationale for customers to be able to analyze exposure (adversary risks) to that specific cloud service. The cloud service could be exposed not only to denial of service (DoS) platforms but also to malicious code evaluation, such as crypto-jacking or storage as service.

Equation 2: Compliance Automation Efficiency (CAE)
Let:
T_0, T_a: manual engineering hours per period before/after automation

C0,Ca: cost before/after automation
Q_0, $Q_a \in [0, 1]$: audit quality/coverage proxy
weights $\alpha + \beta + \gamma = 1$ $(\alpha + \beta + \gamma = 1)$ (default $\alpha = 0.5, \beta = 0.3, \gamma = 0.2$)

$$CAE = \alpha(1 - T_0/T_a) + \beta(1 - C_0/C_a) + \gamma(Q_0/Q_a) \quad (4)$$

Residual Expected Loss by Cloud Provider

Provider	ResidualExpectedLoss USD
AWS	545668.62
Azure	745612.29
GCP	205938.2

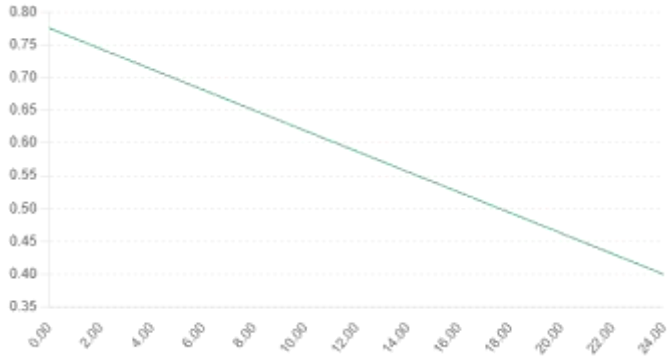


Fig. 3. Sensitivity to Automation Effort

III. Multi-Cloud Context: Architecture and Security Considerations

The growing adoption of multi-cloud topolo- gies—combining private clouds and on-premises infrastructure with one or more public cloud providers—supports the evolution of new, advanced services able to process massive amounts of data at high speed using low, variable costs. However, excessive reliance on multiple providers may introduce new dependencies that an organization is unable to manage. The loss or compromised integrity of sensitive data or access control credentials in any of the providers may impact workloads in other, apparently independent providers. These affects are especially relevant to cloud services processing data about natural or human-made disasters, where delays in information propagation or validation may have catastrophic consequences. Multi-cloud deployments introduce additional monitoring requirements for several reasons. Affected data objects are not limited to a single provider, and improper protection on any provider may expose sensitive information that risks are exfiltration or leakage, even if the other providers offer perfect confidentiality. Normalization and translation of policies expressed in different syntaxes are necessary across providers to verify the correct implementation of automated reactions. Finally, control observables, such as the audience of a shared object, may depend on two or more providers. Addressing these considerations constitutes a prerequisite for the extension of AI-Driven Risk Assessment and Compliance Automation in Multi-Cloud.

A. Hybrid and Multi-Cloud Topologies

Cloud systems with computational units and storage that are distributed and managed across multiple cloud providers can be organized in hybrid or multi-cloud topologies. Hybrid clouds have the ability to move data and application code across the boundaries of cloud services in a manner that enables the realization of

security and compliance controls. Multi-cloud refers to the use of multiple cloud computing services in a single architecture to minimize dependence on a single vendor (vendor lock-in). A cloud can be composed of different public IaaS (for example, Amazon EC2 and Microsoft Azure) in a multi-cloud Topology, with other com- ponents from a restricted cloud provider, for example an EU, Swiss, or US cloud, as a fallback for the personal data of people living in the corresponding jurisdiction. Multi-cloud systems may expose services to a larger set of authentication and authorization mechanisms and policies, and may therefore require additional monitoring regarding the violation of such controls, through either a verification or an attack-detection perspective. Multi-cloud services may also require additional checks regarding financial retributions, since their correct use should aggregate the costs of remote use of cloud services from different providers.

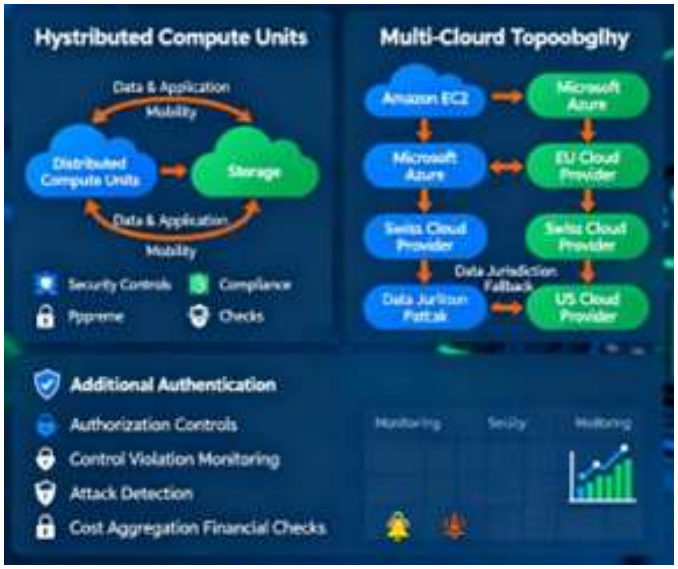


Fig. 4. Hybrid and Multi-Cloud Topologies with Security, Compliance, and Cost Monitoring.

B. Data-Flow and Observation Points

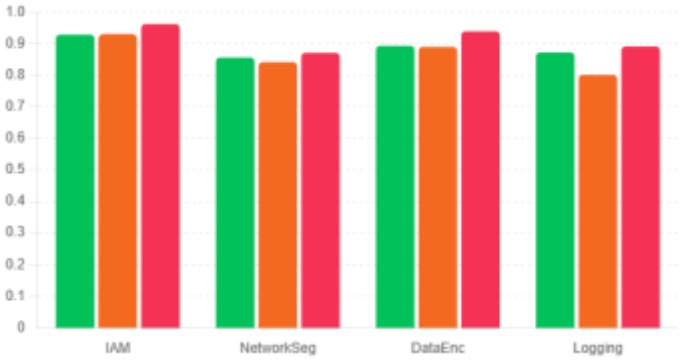


Fig. 5. Control Success by Provider

too popular a method or technique may consequently degrade the business ecosystem perceived risk exposure. Three vertical layers, namely topology definition, orchestration for batch or interactive service consumption, and logical composition of services, support the cloud-based digital business ecosystem architecture. The highest layer represents the overall digital business ecosystem, encompassing the Internet, actors, industry cloud ecosystems, and public cloud services in a world market. The middle layer refers to

the behavior of a specific actor within a digital ecosystem during a particular period and is capable of producing observable actions, while the bottom layer temporalizes the digital business ecosystem and its industry cloud ecosystems, thus enabling the logical composition of services provided by industry cloud ecosystem partners through the support of semantic data and service registries. Bandwidth and security constraints, and the dynamic character of actor resource usage in this environment, introduce new missing property characteristics in the traditional behavioral component.

Equation 3: Cross-Cloud Security Integrity (CSI)

For each control c on provider p, let $scp \in [0, 1]$ be the success probability (control "holds" in a given interval). A control is satisfied if any provider enforces it successfully

The data-flow and security-oriented observation points for risk and compliance assessment in multi-cloud environments are critical for the effective deployment of AI-based risk assessment and compliance automation mechanisms. For a sound risk analysis, the threat surface must be clearly mapped, allowing attackers to identify all possible points of attack, understand system behavior during attacks, and even prevent unexpected detection. Strong digital business ecosystems, such as industry cloud ecosystems, nevertheless remain highly vulnerable to external threats and attacks involving affected organizational trust dependencies. The contribution of trust in a cloud service provider needs to be carefully addressed, since cloud services are inherently less trustworthy than, for example, on-premises solutions because of the public nature of the services. Framework damage in a trust-oriented business ecosystem is therefore of major importance. Any risk exposure analysis process that adopts

(series of parallel components):

Per-control success across providers: $1 - \prod_{p}(1 - scp_p)$

Overall integrity across all required controls (series composition):

$$CSI = \prod_{c}[1 - \prod_{p}(1 - scp)] \qquad (5)$$

IV. AI Techniques for Risk Assessment

Applicable AI techniques can address the data collection, risk assessment, and compliance automation steps in the GRC process. Procedural and unstructured data from IT environ- ments can be identified, collected, and pre-processed to sup- port GRC's risk-aware automation objectives. AI methods for risk management combine anomaly detection and behavioral analytics to derive a risk taxonomy and assess risk exposure. The procedure calculates risk at runtime rather than as a standalone step, permitting fast, scalable updates supplemented by periodic threat hunting. Continuous monitoring eases op- erational burden and keeps teams focused on the most salient risks. Surveys discuss detecting deviations from baseline behavior, but the innovation lies in combining these tech- niques within a broader risk-analysis framework. Behavioral analytics—making inferences about users or services based on their actions—examines runtime behaviors of entities in attacks while using historical data or external reports to build an attestation layer. Separation of concerns, illustrated with user accounts and authentication, supports detecting account compromise, incorrect implementation of the principle of least privilege, and vertical privilege escalation. Further innovation lies in applying statistical techniques within the context of risk assessment versus pure detection, filtering out false positives by expressing risk exposure and impact in the context of the application landscape.

A. Data Collection and Feature Engineering

Data collection for AI model training requires abundant labeled data for all considered risk types. It follows the situation-action paradigm, which uses behavioral models to characterize the usual operations of cloud providers. During normal operations, data such as logs, network flows, and resource configurations are collected through Paul, a multi-cloud observability architecture. Events from the cloud providers record logs and status information that reflect the state of resources. The different templates yield a multitude of fields. Processing such logs also requires feature-engineering capabilities that create a common view of resources, activities, and flows. Redundant and unimportant fields are identified and removed based on the possible risk types, generating event records with a description of risk activities detected. When a risk occurs that causes at least one confirmed event, the blacklist of the GRC agent is checked. If the event is not considered accepted, it is tagged as labeled data for the ML model. The labeled data is then fed into the builds of the statistical ML preventive models to detect the presence of that risk type. Feature engineering is further applied to describe a risk-related situation, and these features are made available to the models for these risk types.

Equation 4: Automated Incident Response Score (AIRS) With industry-minimum reference values MTTA⋆, MTTR⋆, MTTA⋆•, MTTR⋆• and containment rate r ∈ [0, 1], define:

$$\text{AIRS} = 100[w1MT\,T\,AMT\,T\,A\star \qquad (6)$$

with $w_1 + w_2 + w_3 = 1$ (default 0.4, 0.4, 0.2). Cap to [0,100].

B. Anomaly Detection and Behavioral Analytics

Anomaly detection aims at modelling a behaviour in a system and then identifying behaviours that deviate from the model. Although there are many techniques for anomaly detection, statistical techniques and artificial neural networks (ANNs) are among the most usual choices. Anomalous be- haviour detection can also be regarded as unsupervised ma- chine learning, with similar characteristics and difficulties tied to unlabelled data. A characteristic of anomaly detection techniques is that they usually do not require the data to have labelled examples of anomalies, although the availability of labelled data is a way to measure how difficult is the problem of anomaly detection. The applicability of anomaly detection techniques depends on the data set used and its distribution. The identified anomalies do not necessarily correspond to an attack; they can also represent normal behaviour. For example, in a cloud environment, under certain scenarios where the proactive scaling is in effect, the number of instances of a service can increase, and so it would not be an anomaly. Hence, labelled data sets can help to measure the performance of anomaly detection techniques. Examples include ISOT, KDD Cup 1999, NLS-KDD, CSE-CIC-IDS-2018, AILDS, and MINN. While labelled data sets assist in evaluating the accuracy of the technique, nonlabelled data sets are the main type used for implementation.

V. Compliance Automation across Cloud Providers

Security expert Wolfgang E. S. Fuchs describes compre- hensive data-structure cover-to-cover. Enforcement, Decision, Action, and Notification are the four main processes in Com- pliance as a Service solution. Policy translation and normal- ization allow heterogeneous cloud policies to be merged and checked easily for compliance; Cloud-Hybr, a Cloud Service Provider, provides an API to perform automatic translation into its policies for its clients. Compliance is maintained by continuously monitoring the three processes and addressing any compliance violation. Current violations are presented to users, and past violations are monitored to ensure that evidence is generated, stored, and delivered according to the policy schedule. The main threat is price changes for any Achilles heel of the deployed Cloud(s) used by the members of the federation. An AI service continuously scans the contracts and prices of all Cloud Providers available in the region for possible replacements to improve or return to compliance.

A. Policy Translation and Normalization

Natural-language processing (NLP) techniques enable au- tomatic translation and normalization of policy

decisions and declarative statements across public cloud providers, improv- ing the effectiveness of compliance monitoring and assur- ing continuous compliance. Cloud services have proliferated rapidly, bringing new opportunities and business benefits while also introducing additional vulnerabilities and risks. Orga- nizations need to reduce these risks while efficiently using new cloud services and feature offerings. Multi-cloud provider configurations are increasingly common, often for expertise, best-of-breed products, geographic coverage, pricing, and ven- dor lock-in avoidance. NLP techniques for automatic trans- lation are available for various domains. Organizations want to enforce similar governance, risk, and compliance (GRC) policies, including data retention, member and role configura- tions, data-use and access restrictions, category-classification requirements, and SLA fulfillment, across multiple providers.

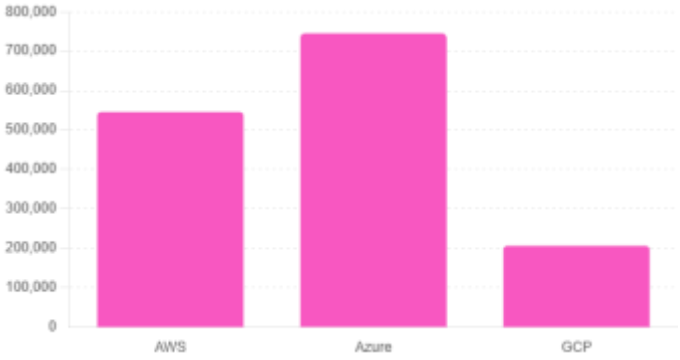


Fig. 6. Compliance as a Service: Policy Translation, Monitoring, and AI- Driven Price Scanning.

Operators want to quickly ensure that these GRC policies are being enforced across all clouds. When cloud usage is minimal and simple, operators can check data operator procedures manually; however, as cloud usage broadens and intensifies, manual full-operational reviews are no longer practical. Sta- tistical measures of textual similarity provide the basis for mutation detection. Users express GRC policies as declarative statements, which NLP services can translate into a common representation. Existing problems in semantic policy trans- lation, evaluation, and verification may emerge. Continuous monitoring relies on automatic policy translation for cloud sys- tems into a common operational data representation. Dynamic security-compliance management enforces policies across a federation of cloud services. Normalization eases compliance- execution failure detection and corrective responses by service consumers.

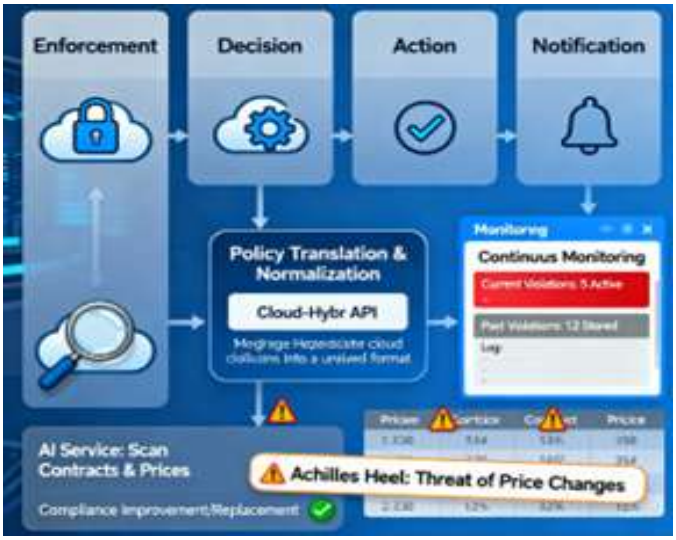


Fig. 7. Residual Expected Loss by Provider

have been issued by only a few cloud-computing providers. Thus, Gap provides a framework that automatically checks for compliance to policies expressed in a third-party language, Enforced Compliance Policy Language (ECPL), which is richer and more expressive than cloud providers' languages and that plays an intermediary role between business processes realized in Business Process Model and Notation (BPMN) and the different cloud providers' languages. Gap combines an analysis of service-choreography definitions with process testing and formal verification and can check service choreography definitions against a given policy or test a proper service-choreography instance against a trust-and-security policy provided as a finite state automaton. Test cases (test data) are generated according to two different approaches: a direct solution based on a path-generation algorithm and a stochastic solution based on a strategy using a Markov chain. However, the framework is on-line, and automatic run-time monitoring of a multi-cloud-computing scenario is currently a work in progress.

Equation 5: Cloud Compliance Consistency Index (CCCI)
Let S_p be the set of normalized controls after NLP translation for provider p and λ_p the enforcement latency (minutes). Compute:

B. Continuous Compliance Monitoring
Average pairwise Jaccard similarity: J = avg
$\underline{|S_a \cap S_b|}$
$a<b\ |S_a \cup S_b|$

As long as cloud services can augment only parts of business processes, complexity in distributing business processes across heterogeneous cloud infrastructures can easily be managed. However, once crucial components in business processes rely on multi-cloud services, complex interactions between the services and potential inconsistencies across the clouds can threaten business operations. These are not merely theoretical considerations, as many organizations have already experienced serious service outages that negatively affected their businesses. Moreover, the problem of interaction between different services is exacerbated by the lack of a unified cloud policy across the various cloud providers. Indeed, business policies defining the constraints under which services reside in the public cloud and which controls are required in order to use cloud services safely
Coefficient of variation of latency: $CV=\sigma(\lambda)/\mu(\lambda)$

$$CCCI = 100(0.6J + 0.4(1 - CV)) \qquad (7)$$

VI. Operationalizing AI-Driven Compliance in Practice

Governance, risk, and compliance (GRC) embrace an or- ganization's structures and processes for establishing objec- tives, determining risks, and ensuring that all activities are in accordance with applicable laws and regulations. In practice, however, the interrelation of the mentioned aspects is rarely addressed. As such, an ontology model is proposed to formal- ize the relationships and enable practical GRC implementation. Moreover, a support profile to govern AI operationalization covers national regulations, sectoral rules, and corporate guide- lines, and points out related data governance and privacy issues. Typical comprehensive GRC systems comprise busi- ness rules and operating procedures within governance, risks addressed within risk management, internal and external regu- lations in compliance. Several discrete point solutions address GRC areas, such as risk assessment and audit management, yet barely any integrate those.

This interrelation is important because without rules (compliance), there is no assessment of whether the desired objectives (governance) are achieved or not, and without knowing the level of risk (risk management), it is not possible to evaluate whether the compliance achieved is acceptable under that particular risk. Separable for oper- ationalization, these areas must interconnected for practical implementation.

A. Governance, Risk, and Compliance (GRC) Ontology

An ontology that captures the Governance, Risk and Compliance (GRC) requirements for multi-cloud environments is introduced. The ontology formalizes the GRC domain knowledge in GRC policies by leveraging the resources offered by GRC service providers, such as analysis engines and data management services, to alleviate the effort of supporting risk management tasks. With the growing adoption of multi-cloud environments composed by services from several cloud infrastructure providers (CSPs), risk management and compliance assessment constitute pressing challenges. Despite the effort devoted by academic researchers, solution providers, and the community at large, the state of the art is still far from providing operational solutions that can be used by practitioners to efficiently and effectively support these important tasks. Risk assessment and compliance evaluation of multi-cloud environments concern non-trivial activities that require several experts with different areas of competence. Due to the complexity and specialization, GRC service providers have emerged to offer solutions capable of assisting several organizations in GRC tasks, such as compliance checking, compliance monitoring, risk evaluation, risk treatment, and security evaluation. These service providers deploy engines that are able to support specific analysis. For instance, Web application vulnerability scanners are GRC services having as purpose the evaluation of Web applications against security threats in the context of the OWASP Top 10 Risks. However, even possessing access to risk management services does not make the GRC tasks trivial. On the contrary, the existence of such services demands extra care because services relying on multiple policy definitions need to translate and normalize policies among the GRC domains, providers, and services. In addition, the organization using the service must provide the data required by the service to support its execution. Failure to fulfill such data requirements of the GRC service may lead to no result or even mislead the organization to take the wrong decision, as when an organization does not grant the proper access to a Web application scanning service.

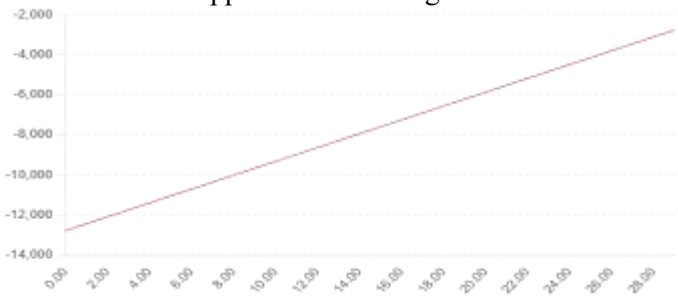


Fig. 8. Predictive Risk Mitigation Value vs TPR

Equation 6: Predictive Risk Mitigation Value (PRMV)
Let:
π: incident prevalence per period, L: loss per incident, TPR,FPRTPR,FPR: model performance,
p: fraction of loss preventable if detected in time,
Cfp: cost per false positive, Cops: operating cost per period Baseline expected loss: πL
With detection: residual incident loss = $(1 - p\ TPR)\pi L$ plus false-positive and ops costs.

$$PRMV = \pi L - ((1 - pT\ PR)\pi L + FPR(1 - \pi)C_{fp} + C_{ops})$$

(8)

B. Data Governance and Privacy Considerations

Privacy and data protection considerations should guide the design of a custom-designed Governance, Risk, and Com- pliance (GRC) ontology. Risk assessment and compliance- monitoring engine requirements must be explicitly stated. Sim- ilarly, feature engineering should encompass suitable trans- formations of the observation data based on the domain knowledge, emphasized by multilingual support. The ontology must be populated during both training and operation. A proper design that accounts for non-repudiation and data protection issues would ensure compliance with new e-Privacy and General Data Protection Regulation (GDPR) requirements, beyond supporting the GDPR by design statement. Auto- matic data processing via natural language processing (NLP) models processing source data in natural language and/or in an organization-specific and compliant language would ease adoption. A policy normalization/substitution engine in the compliance monitoring-enforcing engine should detect and accommodate multi-cloud differences, promoting a multi- cloud-ready design. A dedicated GRC model governing the policies and procedures supporting dataflows would further ease guaranteeing compliance when investing in additional infrastructure.

VII. Conclusion

AI techniques can be successfully leveraged to reduce risk exposure and achieve compliance in multi-cloud environments. Risk assessment and support for cloud governance can be aided through anomaly detection based on data flows, while issues for the AI-based automated compliance architecture. AI techniques represent a breakthrough in the automatic translation and normalization of cloud provider policy re- quirements and facilitate continuous compliance monitoring in multi-cloud environments. A complete Governance, Risk, and Compliance ontology for top-level policy definition enables a clear understanding of the trade-offs among security, risk, privacy, and compliance metrics in the continuous risk-and-compliance-driven multi-cloud data governance strategy. The work represents only the initial steps for a GRC-driven data governance strategy in multi-cloud systems. Future extensions include the generalization and specialization of risk assess- ment techniques for regular, irregular, and targeted threats; the automation of the remaining Risk-and-Compliance and Privacy modules; the consolidation of the GRC ontology through collaboration with Cloud Governance Experts; and the operationalization of the Data Privacy module within GDPR constraints.

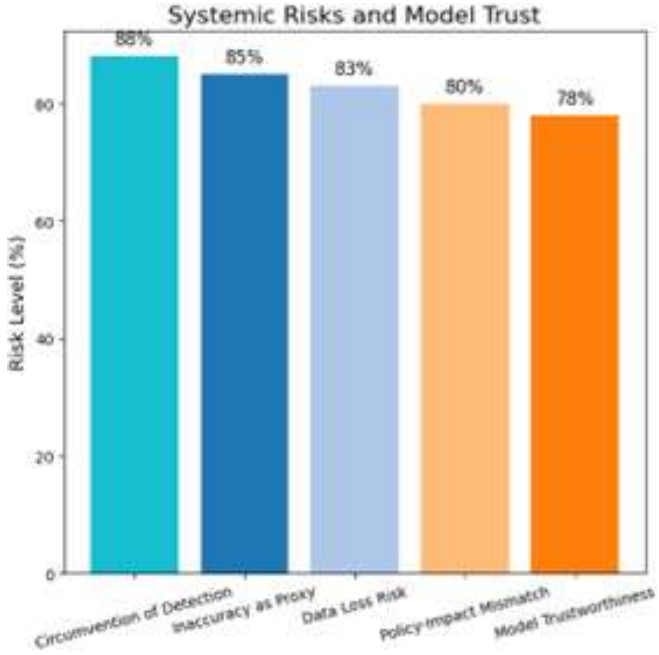


Fig. 9. Systemic Risks and Model Trust

behavioral monitoring can detect deviations from established baselines. Within the context of hybrid and multi-cloud topolo- gies, the illicit use of public cloud services by enterprise employees can be actively monitored. Continuous policy val- idation across cloud service providers, based on GRC policy and cloud provider ontology translation and normalization, serves to ensure that platform-specific regulatory compliance requirements are met. Future work will focus on operationaliz- ing the integration of AI-driven compliance monitoring within a technology and process stack based on the Decentralized Monitoring system and underlying technologies. The Decen- tralized Monitoring concept offers a union of monitoring, enforcement, and correction capabilities needed to retain a compliant state. Data governance considerations ensure that corporate data remains protected for its entire lifecycle, while special attention to privacy helps to preserve the integrity and confidentiality of private identity informationwithin the dynamic and hybrid multi-cloud ecosystem, where anonymiza- tion of detected data must be preserved.

A. Summary and Future Directions

This research explored how advanced Artificial Intelligence techniques can underpin risk assessment and compliance au- tomation in the multi-cloud ecosystem. The theoretical foun- dations of risk assessment were articulated, culminating in a risk taxonomy for multi-cloud environments. Three classes of risk were identified and deconstructed. A particular focus was the operationalization of AI techniques specifically for risk assessment; the technical processes for data collection, feature engineering, and risk quantification using Anomaly and Behavioral Analysis methods were elaborated. Multi-cloud compliance was also treated, with special emphasis on design

REFERENCES

[1] Alenezi, A., Abomhara, M. (2022). AI-based risk prediction models for multi-cloud security management. Computers Security, 118, 102734.

[2] Dwaraka Nath Kummari,. (2022). Machine Learning Approaches to Real-Time Quality Control in Automotive Assembly Lines. Mathe- matical Statistician and Engineering Applications, 71(4), 16801–16820.
Retrieved from https://philstat.org/index.php/MSEA/article/view/2972

[3] Alshamrani, A., Myneni, S. (2022). Automated compliance assessment for hybrid and multi-cloud infrastructures. Journal of Information Secu- rity and Applications, 67, 103160.

[4] Fakotakis, N. D., Nousias, S., Arvanitis, G., Zacharaki, E. I., Moustakas, K. (2022). AI-enabled sound pattern recognition on asthma medica- tion adherence: Evaluation with the RDA Benchmark Suite. arXiv. https://arxiv.org/abs/2205.15360

[5] Amazon Web Services. (2022). AWS cloud security and compliance handbook 2022. AWS Whitepaper. https://aws.amazon.com

[6] Bharath Somu,. (2022). Modernizing Core Banking Infrastructure: The Role of AI/ML in Transforming IT Services. Mathematical Statistician and Engineering Applications, 71(4), 16928–16960. Retrieved from https://philstat.org/index.php/MSEA/article/view/2990

[7] Arp, D., Spreitzenbarth, M., Rieck, K. (2022). AI-enabled detection of cloud configuration risks. IEEE Access, 10, 78211–78225.

[8] Bhatia, K., Singh, P. (2022). Machine learning–driven vulnerability scoring for cloud-native ecosystems. Journal of Network and Computer Applications, 207, 103503.

[9] Lakarasu, P. (2022). MLOps at Scale: Bridging Cloud Infrastructure and AI Lifecycle Management. Available at SSRN 5272259.

[10] Cisco Systems. (2022). Zero-trust and automated compliance in dis- tributed cloud environments. Cisco Security Research. https://cisco.com

[11] Nagabhyru, K. C. (2022). Bridging Traditional ETL Pipelines with AI Enhanced

Data Workflows: Foundations of Intelligent Automation in Data Engineering. Online Journal of Engineering Sciences, 1(1), 82–96. Retrieved from https://www.scipublications.com/journal/index.php/ojes/article/view/1345

[12] Das, S., Ray, P. (2022). AI-integrated cloud governance frameworks for regulated industries. Information Systems Frontiers, 24(6), 1789–1805.

[13] Taimoor, N., Rehman, S. (2022). Reliable and resilient AI and IoT-based personalised healthcare services: A survey. arXiv. https://arxiv.org/abs/2209.05457

[14] Zakeri, M., et al. (2022). Application of machine learning in predicting medication adherence. Journal of Medical Artificial Intelligence, ?(?). https://jmai.amegroups.org/article/view/6666/html

[15] Deloitte. (2022). AI-enabled compliance automation and digital risk intelligence. Deloitte Insights. https://www2.deloitte.com

[16] Stoner, M. C. D., et al. (2022). Digital directly ob- served therapy to monitor adherence: A study on syn- chronous DOT. Journal Name, Volume(Issue), pages. https://www.tandfonline.com/doi/full/10.1080/25787489.2022.2103512

[17] ENISA. (2022). Cloud security and compliance landscape 2022. Euro- pean Union Agency for Cybersecurity. https://www.enisa.europa.eu

[18] Pandiri, L., Chitta, S. (2022). Leveraging AI and Big Data for Real- Time Risk Profiling and Claims Processing: A Case Study on Usage- Based Auto Insurance. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3760.

[19] Inala, R. Advancing Group Insurance Solutions Through Ai-Enhanced Technology Architectures And Big Data Insights.

[20] Google Cloud. (2022). Risk and compliance in multi-cloud AI deploy- ments. Google Cloud Security Whitepaper. https://cloud.google.com

[21] Srinivas Kalyan Yellanki. (2022). Enhancing Operational Efficiency through Integrated Service Models: A Framework for Digital Transformation. Mathematical Statistician and Engineering Applications, 71(4), 16961–16986. Retrieved from https://www.philstat.org/index.php/MSEA/article/view/2991

[22] Gupta, R., Sharma, V. (2022). Risk quantification for cloud workloads using AI-enhanced scoring models. IEEE Transactions on Cloud Com- puting, 10(4), 2301–2315.

[23] Aitha, A. R. (2022). Cloud Native ETL Pipelines for Real Time Claims Processing in Large Scale Insurers. Universal Journal of Business and Management, 2(1), 50–63. Retrieved from https://www.scipublications.com/journal/index.php/ujbm/article/view/1347

[24] IBM Security. (2022). Automating cloud compliance with AI and policy analytics. IBM Research Papers. https://ibm.com/security

[25] Kulkarni, M., Golechha, S., Raj, R., Sreedharan, J., Bhardwaj, A., Rathod, S., Vadera, B., Joshi, R., Kurada, J., Raval, A. (2022). Predicting treatment adherence of tuberculosis patients at scale. arXiv. https://arxiv.org/abs/2211.02943

[26] Kandasamy, V., Srinivasan, A. (2022). Compliance-aware AI pipelines for multi-cloud environments. Journal of Cloud Computing, 11(1), 1–22.

[27] Meda, R. Enabling Sustainable Manufacturing Through AI-Optimized Supply Chains.

[28] Khan, M. A., Javaid, N. (2022). AI-assisted audit trails and governance models in cloud platforms. Future Generation Computer Systems, 129, 208–221.

[29] Kim, S., Park, H. (2022). Predictive analytics for cloud compliance vio- lations using machine learning. Expert Systems with Applications, 204, 117606. Goutham Kumar Sheelam, ”Power-Efficient Semiconductors for AI at the Edge: Enabling Scalable Intelligence in Wireless Systems,” International Journal of Innovative Research in

[30] KPMG. (2022). Cloud compliance and AI automation: Regulatory challenges and best practices. KPMG Research. https://kpmg.com

[31] Botlagunta Preethish Nandan. (2022). AI-Powered Fault Detection In Semiconductor Fabrication: A Data-Centric Perspective. Kurdish Stud- ies, 10(2), 917–933. https://doi.org/10.53555/ks.v10i2.3854

[32] Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), DOI 10.17148/IJIREEICE.2022.101220
[33] Li, X., Zhang, Y., Chen, Z. (2022). AI-based evaluation of multi-cloud drift and compliance misalignment. Computers Security, 121, 102832.
[34] Singireddy, J. (2022). Leveraging Artificial Intelligence and Machine Learning for Enhancing Automated Financial Advisory Systems: A Study on AIDriven Personalized Financial Planning and Credit Mon- itoring. Mathematical Statistician and Engineering Applications, 71 (4), 16711–16728.
[35] Microsoft. (2022). AI for cloud governance: Automating compliance workflows. Microsoft Defender Research. https://learn.microsoft.com/security
[36] Koppolu, H. K. R., Recharla, M., Chakilam, C. Revolutionizing Patient Care with AI and Cloud Computing: A Framework for Scalable and Predictive Healthcare Solutions.
[37] Mukherjee, D., Alam, S. (2022). Machine learning for cloud risk modeling: A survey and taxonomy. ACM Computing Surveys, 54(12), 1–35.
[38] Oguine, O. C., Oguine, K. J. (2022). AI in telemedicine: An appraisal on deep learning-based approaches to virtual diagnostic solutions (VDS). arXiv. https://arxiv.org/abs/2208.04690
[39] NIST. (2022). Automation of cloud security compliance using AI and policy engines. National Institute of Standards and Technology. https://nist.gov
[40] Gadi, A. L. (2022). Cloud-Native Data Governance for Next-Generation Automotive Manufacturing: Securing, Managing, and Optimizing Big Data in AI-Driven Production Systems. Kurdish Studies.