Deep Science Publishing
https://doi.org/10.70593/978-81-984306-5-6_8

Chapter 8

Security and compliance in hybrid cloud models

Ravi Kumar Vankayalapati

Cloud AI ML Engineer, Equinix, Dallas, USA.
ravikumar.vankayalapti.research@gmail.com

Abstract

Security and compliance are critical considerations in hybrid cloud models, where organizations must safeguard sensitive data across both public and private cloud environments. This abstract explores the challenges of ensuring data protection, regulatory compliance, and secure integration between cloud platforms. Key strategies include encryption, access controls, and identity management to protect data at rest and in transit. It also discusses the importance of continuous monitoring, compliance auditing, and maintaining clear governance frameworks to meet industry-specific regulations. By addressing these security and compliance needs, businesses can confidently leverage hybrid clouds while minimizing risks and ensuring regulatory adherence.

Keywords

Security, Compliance, Hybrid Cloud, Data Protection, Regulatory Compliance, Cloud Integration, Data Encryption, Access Control, Identity Management, Continuous Monitoring, Compliance Auditing, Governance Frameworks, Risk Management, Data Privacy, Cloud Security, Hybrid Cloud Models.

8.1. Introduction

Cloud computing is revolutionising IT economics and service models. Organisations are working towards a hybrid (private/public) cloud model that involves the transfer of data and workloads between such environments. The anticipated benefits are greater flexibility and the ability to reduce costs by offloading non-critical workloads to the public cloud. However, there are barriers to entry imposed by security and compliance risks. It would appear that these hybrid workloads are significantly more susceptible to security incidents than anticipated. Moreover, in such environments, achieving or indeed demonstrating

security and compliance can be difficult and expensive. Existing solutions to these issues are often narrowly focused or consider the problems in isolation (Danda, 2024).

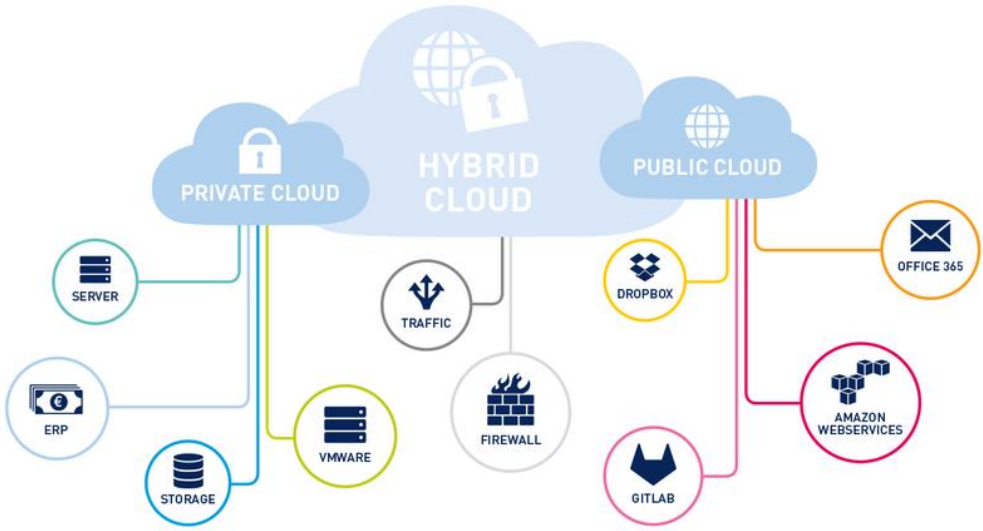

Fig 8.1: Compliance and Security in Hybrid Cloud Environments

8.2. Understanding Hybrid Cloud Models

It is obvious that cloud computing is a noticeable technology in today's world information society. As hardware, software, data maintenance and networking are delivered to user devices on-demand as utilities it is strategic and ambitious. Security is a major element in high quality of service delivery in the cloud environment and is one of the most dynamic areas of technology development and of the major interest in the cloud computing field. Hybrid cloud computing is a symbiosis of varied technical and financial service models and deployment implementation where some form of IT resources are made available to integrate the application services within the cloud. In the other case, the end-user can utilize the on-premises software that accesses applications on cloud computing outside the organization firewall (Syed, 2023).

8.2.1. Definition and Characteristics

With the rise and increasing acceptance of business processes being uploaded onto remote, public Clouds, security and regulatory actions are still around to prevent the common threats such as Data loss, spread of malware, physical break ins, denial of service, and can also malfunction of the systems. They are also complicating the way of

a rapid acceptance of a widespread usage of public Cloud for a traditional financial data, health reporting system, or legal tribunal case data mart, owing to the feared possibility of regulatory noncompliance. One possible approach to alleviate these fears is to deploy private cloud and virtual private cloud security controls. However, in recent times another increasingly popular interest is in public Cloud ensures the most cost effective and easily manageable computational assets, especially if they are placed in entirely external service provider's Cloud, farther away from the user site. And their viewpoint they are unable to either design or force any other parties to adopt and be subjected compliantly to, such security controls that could mitigate risks of the current regulatory framework violation (Nampalli, 2023).

Equation 1: Cost of Reserved Instances vs. On-Demand Pricing

$$C_{\text{on-demand}} = \sum_{i=1}^{n} P_i \times t_i \times R_{\text{on-demand}}$$

$$C_{\text{reserved}} = \sum_{i=1}^{n} P_i \times t_i \times R_{\text{reserved}}$$

Where:

- $C_{\text{on-demand}}$ = Total cost of using on-demand instances
- C_{reserved} = Total cost of using reserved instances
- $R_{\text{on-demand}}$ = Rate for on-demand instances
- R_{reserved} = Rate for reserved instances (usually lower)

Fig : Optimize and refine your hybrid cloud strategy

8.2.2. Benefits and Challenges

Since the very beginning of the cloud computing era, one of the most significant and difficult barriers was the trust in the cloud. Certain issues like security and on a larger scale compliance were naturally becoming the dominant discussion points in the prospect of enterprise interests. The promise of the cloud was, and still is, abstracting the crust of IT operations while opening up the possibility to use practically unlimited computing power. Despite having some initial biases against cloud, a lot of cloud adoption and success stories were occurring - but they were mostly at mundane, generic services, eventually resulting in mega cloud providers' locked-in potentially jeopardizing the future adaptability. Also, the initial promises of completely moving to the cloud turned out to be erroneous. In a direct consequence, enterprises started moving towards a middle ground: hybrid clouds.

Hybrid cloud is a composition of two or more distinct cloud infrastructures that remain unique entities, but are bound together by standardized technology that enables data and application portability (Ramanakar et al., 2024).

8.3. Importance of Security and Compliance in Hybrid Clouds

Cloud computing has rapidly emerged as the major technology within information technology (IT) for both users and commercial providers. Businesses or users can appeal to varied cloud service models such as infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS), for provisioning storage, networking interfaces and computational resources. Data and software are stored and executed in a large number of different shared data centers, which are often located at dispersed global sites. This distributed feature of services puts increased pressure on achieving and maintaining proper governance of security and regulatory compliance in cloudy architectures. The academic domain has been overwhelmed by a vast amount of new theoretical and technological works to evolve service-oriented systems. These service architectures are designed to function seamlessly over multiple domains and expand the communication capabilities to a global scale in a loosely coupled network. Such systems are generally large-scale, communication-based, network-connection computing entities. Each entity is operated by dissimilar units through the cooperation and competition across cables, optical fibers, air space, and digital networks, embodying social and business interests and implementations. Governance of security and compliance issues is an important requirement for the endorsement of commercial platforms and exchange of data-sensitive applications. Increasingly large and significant efforts have been made within both industry and academia to stabilize cloud service level agreements (SLAs) based on satisfactory quality of service (QoS) guarantees. However, the QoS is not able to guarantee the trade priceoff between indemnity levels and the several regulatory

factors. Furthermore, from the analysis of the business viewpoint, the guarantees of QoS on cloud services could not directly interpret the regulatory and execution model of the cloud technologies. It is significant to close the gap between such diverse stakeholders concerning the exchange of data-sensitive computations on distributed cloudy systems (Syed, 2022).

Fig 8.2: Importance of Security and Compliance in Hybrid Clouds

8.4. Security Measures in Hybrid Cloud Models

Security and compliance are two important topics that all cloud service providers, regardless of model type, must address. But what security measures must be implemented by cloud service providers to ensure that infrastructure and data are secure? How can consumers of cloud feel confident that the provider will not employ their data or service illegally? In addition, widespread adoption of public cloud services is further prevented by the inability of systems in domains subject to regulation and international legal agreements to de-risk ensuring that a cloud's provision of data processing or storage resources does not cause liabilities of non-compliance with the regulation of domains. This section addresses these issues through the analysis of cloud security requirements and the methods for the compliant design and use of Cloud services (Tulasi et al., 2022).

Physical threats are frequently noted as the greatest dangers to the cloud. Most CSPs are aware of threats to their IT infrastructure from natural disasters, terrorist threats, fire, sabotage, and other extreme phenomena. Nevertheless, a distributed denial-of-service attack on a DNS provider paralyzed large parts of the Internet in 2016. As fallout of the

shut down, many popular Cloud services were non-available mainly in the North American and West European regions. This event brought public attention to the risks of cyber-attacks to the Cloud. However, the risks do not concentrate exclusively on public clouds; they grow proportionally to the increase in providers of data and service processing. Consequently, third parties are targeted during contract negotiation, as abuse of customer accounts can bring criminal gains. Thus, hacking operations try at large to steal credit card numbers, or run commands for fulfillments of a useful but possibly illicit task.

Equation 2: Cost of Data Transfer between On-premises and Cloud

$$C_{\text{transfer}} = \sum_{j=1}^{m} (D_j \times C_{\text{transfer-rate}})$$

Where:

- D_j = Amount of data transferred (e.g., GB or TB)
- $C_{\text{transfer-rate}}$ = Cost per unit of data transferred (e.g., $/GB)

8.4.1. Data Encryption

Within a hybrid cloud model, organizations adopt a combination of private and public cloud. All or a portion of the data, applications, and services reside in both. This configuration supports organizations in shifting workloads to and from the cloud, addressing privacy concerns, reducing costs, and meeting a variety of business and technical needs. At the same time, hybrid cloud presents complex, unique challenges in maintaining privacy, security, and compliance (Venkata et al., 2022). These chiefly arise from the distributed and mixed nature of the cloud resources, from the potentially different cloud providers whose services must be used, and from the different levels of control the organization has over these services.

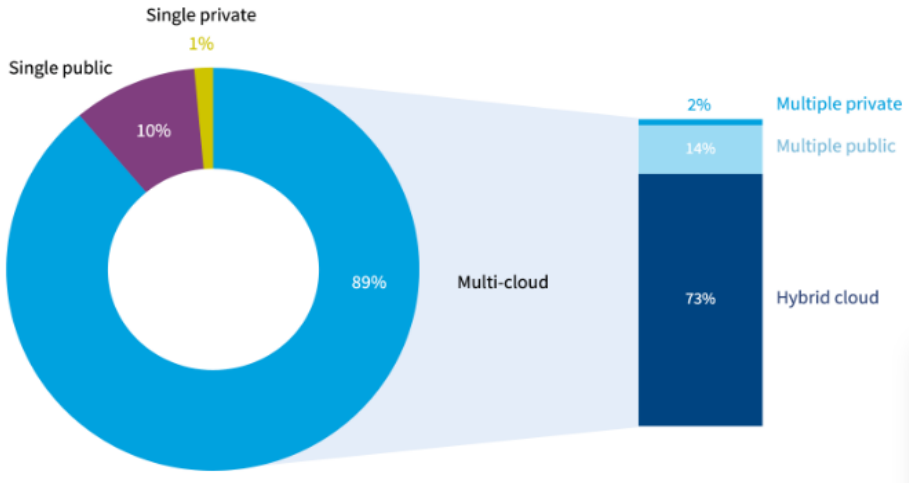

Fig: State of the Cloud Report

8.4.2. Network Security

This section will discuss four different pillars that are essential in ensuring the runtime security & compliance in the hybrid cloud models. They are discussed under separate sections comprising their current solutions followed by the targeted policy changes.

This chapter is the positioning of a secure cloud posture in a hybrid cloud infrastructure composed of the different alternatives for data center instances. It extends and generalizes the security posture for the new data center instances to the entire big data platform and is applied to a commercial case study of securing a commercial petabyte-scale Hadoop as a Service offering. It shows why exporting the data center model to the big data platform fails, and it discusses alternative modeling methods and the associated trade-offs.

8.5. Compliance Requirements in Hybrid Cloud Models

For years now, cloud computing has been proven to be the go-to-market strategy for enterprises to reduce capital expenditures and make enterprise-level applications accessible to every user, regardless of their location. Studies state that in 2022, more than 91% of enterprises worldwide will adopt cloud computing as the medium of their businesses. However, as of today, it's observed that only about 20% of the enterprise's mission-critical workloads and sensitive data are deployed in clouds, with the rest being on-premises. This remaining 80% of the applications are expected to move to the cloud in the future, and among those applications, 30% will be hybrid or multi-cloud. However, one of the significant challenges for enterprises to adopt public cloud is the need to

constantly comply with the changing regulations. In order to stay in business, enterprises engaged in financial, health-care, defense, etc., industries must meet stringent compliance requirements (Pandugula et al., 2024). To further elaborate, banks must be compliant with the Payment Card Industry Data Security Standard; health-care companies must meet the Health Insurance Portability and Accountability Act; data handling companies must comply with the General Data Protection Regulation. However, the shared responsibility model that cloud providers follow has a wide array of security compliance checks by default, whereas only a narrow set of them can be manually tailored by the tenant.

8.5.1. Regulatory Frameworks and Standards

The mostly cost-cutting benefits of Cloud computing and the accelerated time-to-market of Cloud-based services have been realized for retail and commercial sectors. However, the productive non-technical benefits of this fast-evolving technology, particularly those in sectors as conservative as the water industry, have yet to be significantly explored. Current Cloud providers have not paid special attention to security and compliance needs of the water domain, which involves protecting critical SCADA data from breaches and ensuring strict adherence to national and EU data protection laws. Since Clouds-particularly public ones-are usually deployed across wide geographical/frontier domains, they introduce a multitude of further regulatory obligations and challenges (Kalisetty et al., 2023).

Thus, to tackle a proper regulatory control strategy towards meeting security/compliance obligations within a chosen Cloud infrastructure, one needs to answer a number of questions the water companies would pose. Automated Compliance Design for Cloud Computing is a solution that, when given inputs including a list of security & compliance requirements (S&C), a Cloud service model reference and a detailed low-level specification of the Cloud infrastructure, can generate the Cloud infrastructure deployment blueprint that satisfies the security & compliance requirements as well as the Cloud service model reference. Common cloud configurations include hybrid clouds, where companies employ cloud-based applications to perform ensemble-based analytics that interact with on-premise resources. A set of control tactics are presented that aim to move a cross-platform workflow from on-premise, to Tier 3 (medium-/low-usage, non-HSE) to Tier 2 – the former 2 exploiting cloud-based services while the latter constitutes a fully cloud-based one. The tactics are detailed in the context of a chronic lymphocytic leukaemia (CLL) radiomics study, with ensemble models built through a previously developed security and performance benchmarked analytic engine. The cloud performance, security approach, the security of patient data transmission from local NHS Trusts is simulated over a high-bandwidth, secure pipeline (Sondinti et al., 2023).

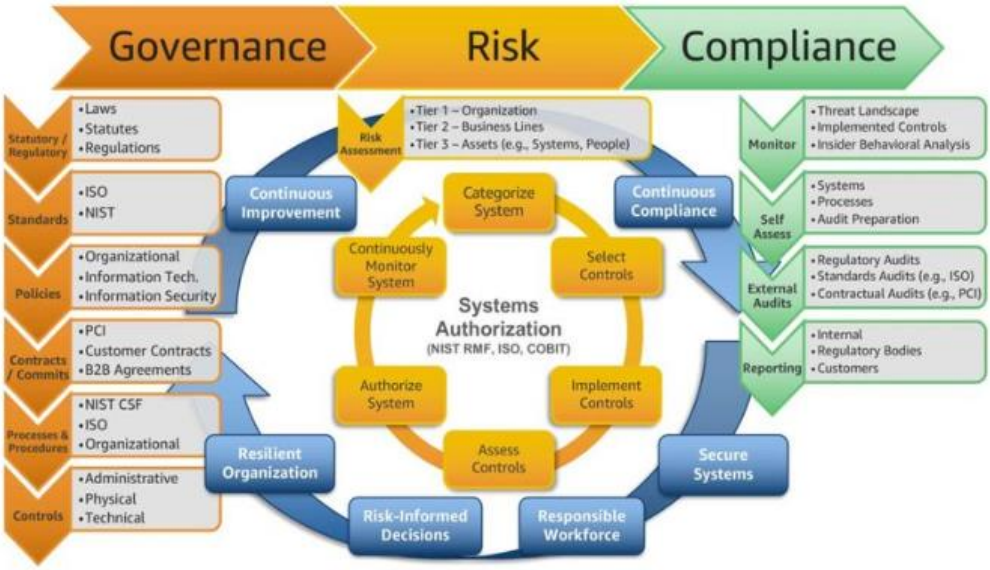

Fig 8.3: Compliance and Regulatory in Cloud Computing

8.5.2. Auditing and Reporting

The migration of data and services has brought various advantages to an entity through the use of cloud computing. The prominent gains are measured in terms of the time and resources saved from acquiring the dedicated infrastructure and propelled particular services. These resources or services may be allocated later on, allowing the user's system to become scalable. The purpose of an organization's activities in the cloud may be to increase profits or earn money in some online business, while on the other hand, a governmental organization may expand its services institutions. Due to the use of different services or computing resources in the cloud, security properties associated with the services or virtual instances and compliance may become concerns. Intentionally or unintentionally, the services are running in the cloud limitations that could lead to security breaches or regulatory non-compliance. An entity's activities in the cloud may bring conformance requirements arising by law, rules, contracts, policies, or a combination of these sources.

8.6. Case Studies and Best Practices

Investigations are mainly focused on Security and Compliance in the hybrid cloud models, their case studies and best practices. Table 1, below, summarizes the tools utilized in case studies and the best practices. These metrics are intended to showcase the current

state of Hybrid cloud models, the security risks they present, and the tool or technique that could be used to eliminate that risk along with the benefits of doing so.

There is widespread agreement that Cloud computing has proven cost cutting and agility benefits. However, security and regulatory compliance issues are continuing to challenge the wide acceptance of such technology. Clouds, and Public Clouds in particular, are operated and owned by various entities and often involve physical infrastructure deployed within different legal domains. In the Cloud environment, applications and data are distributed across different legal environments around the globe. The exchange of data is generally regulated and governed by laws and organizational policies, describing the parties allowed to share the data, modes of exchange, access conditions, etc.

8.7. Conclusion

Since global data privacy rules such as GDPR, information loss and information security have become paramount for public and commercial enterprises and are a major necessity when operating in the cloud. To address and solve these constraints, commercial organizations migrate to construct their own private clouds. However, operational cloud-based architectures and applications can extend elegantly out-of-the-box and on-premises private cloud deployments. Consequently, in concert or by design, combinations of on-premises and cloud-hosted infrastructures are used. This paper suggests an engineered approach to comprehending, evaluating, and perhaps fixing the combined security and conformity difficulties in these composite deployment configurations.

8.7.1. Future Trends

As Cloud systems are a shared infrastructure where enterprises rent, borrow, and even own services, there is (yet another) shared pool of responsibility between the user of the Cloud and the provider of the Cloud. The provider commits to protect access to its infrastructure and the physical systems. The user promises to secure the virtual machines and applications they run on the shared infrastructure. Solutions are designed to solve current and future security threats. Today, many of these solutions can be purchased as an appliance from your favorite vendor partner or as a managed service.

To properly protect the rapidly changing threat landscape, solutions ought to be erected on an extensible platform with a programmatic API consumption capability such as the JavaScript Object Notation (JSON), Representational State Transfer (REST), and Python. There will always be some security that can never be addressed; thus, it is important to pick the threats that can have the most impact and figure out what the appropriate response should be. Broadly, the types of threats that enterprises face for an IT security

environment are influenced from the state of the Cloud industry and the provider, and from the kind of threats common in a data center network environment.

In this context, a focus has been placed on preventing and detecting the privilege account compromises, and minimally securing the baseline monthly security statistics. Common methods to control and secure access to privileged account have been consolidated.

References

Danda, R. R. (2024). Generative AI for Enhanced Engagement in Digital Wellness Programs: A Predictive Approach to Health Outcomes. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 788-798.

Kalisetty, S., Pandugula, C., & Mallesham, G. (2023). Leveraging Artificial Intelligence to Enhance Supply Chain Resilience: A Study of Predictive Analytics and Risk Mitigation Strategies. In Journal of Artificial Intelligence and Big Data (Vol. 3, Issue 1, pp. 29–45). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2023.1202

Nampalli, R. C. R. (2022). Machine Learning Applications in Fleet Electrification: Optimizing Vehicle Maintenance and Energy Consumption. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.8258

Pandugula, C., Kalisetty, S., & Polineni, T. N. S. (2024). Omni-channel Retail: Leveraging Machine Learning for Personalized Customer Experiences and Transaction Optimization. Utilitas Mathematica, 121, 389-401.

Ramanakar Reddy Danda, Z. Y., Mandala, G., & Maguluri, K. K. Smart Medicine: The Role of Artificial Intelligence and Machine Learning in Next-Generation Healthcare Innovation.

Sondinti, L. R. K., Kalisetty, S., Polineni, T. N. S., & abhireddy, N. (2023). Towards Quantum-Enhanced Cloud Platforms: Bridging Classical and Quantum Computing for Future Workloads. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3347

Syed, S. (2022). Towards Autonomous Analytics: The Evolution of Self-Service BI Platforms with Machine Learning Integration. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 84–96). Science Publications (SCIPUB).https://doi.org/10.31586/jaibd.2022.1157

Syed, S. Advanced Manufacturing Analytics: Optimizing Engine Performance through Real-Time Data and Predictive Maintenance.

Tulasi Naga Subhash Polineni , Kiran Kumar Maguluri , Zakera Yasmeen , Andrew Edward. (2022). AI-Driven Insights In to End-Of-Life Decision-Making: Ethical, Legal, And Clinical Perspectives On Leveraging Machine Learning To Improve Patient Autonomy And Palliative Care Outcomes. Migration Letters, 19(6), 1159–1172. Retrieved from https://migrationletters.com/index.php/ml/article/view/11497

Venkata Obula Reddy Puli, & Kiran Kumar Maguluri. (2022). Deep Learning Applications In Materials Management For Pharmaceutical Supply Chains. Migration Letters, 19(6), 1144–1158. Retrieved from https://migrationletters.com/index.php/ml/article/view/11459