Security in Hybrid Cloud Services

Jeff Miller

Graduate Student

School of Information Systems and Applied Technology

Southern Illinois University

Carbondale, IL

Southern Illinois University

November 15th, 2020

Security in Hybrid Cloud Services

Although the Hybrid Deployment model of cloud computing is not without a fair amount of security challenges; recent trends illustrate the popularity of the hybrid model and its advantages are very clear to customers. Hybrid cloud is gaining popularity, as indicated by a recent Denodo survey. Hybrid cloud is the most popular form of cloud deployment, indicating that it has become the 'de-facto' standard for enterprises. The 2020 Denodo Global Cloud Study polled 250 enterprise organizations across Asia Pacific, Europe, Middle East & Africa, and North America. The study found that hybrid cloud deployments account for 42% of configurations, followed by public could (18%) and private cloud (17%). [1] According to the study, as much as 78% of the companies indicated that they run some kind of workload in the cloud. How many of those institutions also have an existing store of on-premise, private data that they would love to tap into, and still get all of the benefits offered through the public and community deployment models of cloud service?

This research paper is intended to support this movement by defining and highlighting some of these benefits, and also address basic security concerns that can arise in a hybrid cloud environment. A simple outline of the foundations of cloud security will be provided as well. In order to analyze security in the hybrid environment, it is important to define the Hybrid Cloud deployment method, considering this definition pretty obviously points out some of the benefits of using one. Going by the NIST definition of cloud computing, it explains that it is usually a combination of two of the three types of cloud deployment. [2] Furthermore, as others have explained, "this type of cloud consists of different deployment cloud models (community, private, or public). The combination of models leads to having unique entities needed by users/organization to be used for multiple purposes in compliance with the standards technology [3]. The hybrid model is the most common design among the others. However, it is more secure and organized than public cloud when it comes to access the structure online. In addition, the Hybrid offers multiple benefits from the other types of cloud deployment models." [4]

Security in the hybrid cloud is usually broken down into four areas. Infrastructure, Applications & Programs, Administration, and Compliance. Within each category the security concerns listed represent a further breakdown into layers. Infrastructure is managed by the provider, and is not accessible to the client; whereas Applications, Administration and compliance are client facing.

- **Infrastructure:** Physical security, Host, Virtualization, Network
- **Applications & Platforms:** Data Security, Application Security, Platform Security, Security as a Service
- **Administration:** Phases of Service Use, Audit, Identity & Rights Management, Interoperability & Portability
- **Compliance:** Data Privacy, Risk Management, Legal Framework, Governance

"That territory interest around the security danger or issue that may happen on foundations layers. Those layers are isolated toward four territories System, Host, Virtualizations, and Physical Security. The particular territories develop a center segment of the Cloud Foundation. By and large, clients don't have any effect on these center parts. It is exceptionally troublesome for clients to assess their security because of many-sided quality of cloud framework." [5]

Although many companies are moving to hybrid cloud out of necessity and convenience, governments are also moving to hybrid cloud, as offerings from major cloud providers have included government cloud products for many years. Without delving too far into vendors, one example would be Amazon AWS GovCloud, A secure platform for government agencies to access the benefits of public and private clouds to further increase agility and security. [6]

The situation where hybrid cloud will be used will be one where a company has its own physical servers, infrastructure, possibly hosted applications and legacy applications being maintained or the SDLC. They might have their own datacenters and mail services, although in this day and age they have likely moved toa mail provider in the cloud. In this usage, the company could simply move to reduce its usage of on premise infrastructure, and move certain services such as mail, contact, management, vendor specific applications and even office productivity software to online solutions. Federations can solve user authentication, even with SSO single-sign-on. In this hybrid scenario. Companies can also move selected servers to the public cloud and move away from physical servers.

According to a 2016 SLR (systematic literature review) study on issues in hybrid cloud [7], the greatest perceived concerns found in the review were:

1.) Public Cloud Security Concerns

2.) Effective Management Use

3.) Integration Complexity

4.) Components Partitioning

5.) Achieving QoS / Task Scheduling & Execution (tie)

It is interesting that the bulk of all security concerns were related to the public cloud and security, where the main risk is exposing private data to the public. Various mechanisms are able to help with this, and have been defined in various publications, such as the Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. “Protecting data through encryption as it moves to the cloud requires more than just ensuring that a secure transfer channel (i.e. TLS) is used. Encrypting the transfer of data to the cloud does not ensure the data is protected in the cloud. Once data arrives in the cloud, it should remain protected both at rest and in use.” [8] Encryption is essential for any organization that stores data. The use of encryption usually brings up the subject of key management, this is also increases the complexity of encryption when you have to manage all of those keys . Alternative approaches to encryption include tokenization, data anonymization, and utilizing built in access controls within a database. Utilizing cryptography in cloud deployments, content aware encryption, and format preserving encryption where formats and numbers of digits are retained further expand alternatives to encrypting everything. Regardless of the complexity, “encrypting data has little value if both providers as well as users of cloud services do not vigorously enforce the processes around key management.” [8] Key management will be very important when considering public and private keys and management. It is important for vendors, not just clients, as the multi-tenancy nature from their perspective complicates their own administration of the keys. Authentication and identity management will also be very important in the hybrid cloud scenario, as new ways of sign on are constantly evolving, with 3rd factor identification utilizing mobile phones and possibly biometrics.

While the cost saving benefits of hybrid cloud are apparent when you reduce any number of servers or physical infrastructure, you may also find that human resources are also spared when your model will not require as many administrators or programmers. Reducing servers by virtualization in your infrastructure is also the same premise that will protect the clients from each other in multi-tenancy, client VM’s are isolated from each other.

References

[1] Datacenter News, 2020, https://datacenternews.us/story/hybrid-cloud-the-most-popular-deployment-path-studypath-study https://datacenternews.us

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Sep-2011

[3] Marwa, S., Abdelmgeid, A., Fatma, O., 2016," Data Security using Cryptography and Steganography techniques ", International Journal of Advanced Computer Science and Applications.

[4] Darwish, M., Yafi, E., Almasri A., Zuhairi, M. (2018) Privacy and Security of Cloud Computing: A Comprehensive Review of Techniques and Challenges, International Journal of Engineering and Technology 7 (4.29) (2018) 239-246

[5] Meena, P., Payal, M., Mathur, D., Choudary, M. (2018) Hybrid Cloud Computing with Security Aspect, Global Journal of Internet inventions and IT Fusion Volume 1, Issue 3, 2018

[6] Amazon Web Services, "AWS GovCloud (US) Region Overview – Government Cloud Computing," Amazon Web Services, Inc., 2015. [Online]. Available: http://aws.amazon.com/govcloud-us/. [Accessed: 14-Oct-2020]

[7] Khan, S., Ullah, N. (2016) Challenges in the Adoption of Hybrid Cloud and Exploratory Study Using Systematic Literature Review, Journal of Engineering, April 15th 2016

[8] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0." Cloud Security Alliance, 2009.