Threats to Hybrid Cloud Security

Agbaje Michael, Adegbie Foladoyin, Alowosile Oluyemi

Abstract-Hybrid cloud environments are complex and complicated, having to deal with issues from multiple users accessing different environments from different places. As developments across cloud approach evolve, companies are adopting hybrid systems to build additional layers to their security infrastructure. Since some services are better handled in the cloud so as to help navigate attacks, this paper takes a descriptive study of problems associated with hybrid cloud and their probable solutions.

Keywords: Cloud, security, Hybrid, Data, off- premise, private, public

1 INTRODUCTION

Hybrid cloud is a formulation of two or more clouds. The cloud could be private or public that maintain distinct operations but are bound together, offering the benefits of multiple deployment models. Gartner defines Cloud Computing as being scalable, delivering IT- enabled services using the Internet (Gartner, 2012). For example, an organization may store delicate client data in- house on a private cloud application, but interconnect that application to a security department like the state security department provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services.

Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications a company uses. Another example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity needs that cannot be met by the private cloud. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds. Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization pays for extra compute resources only when they are needed. Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during usage spikes, in processing demands.

Types of cloud computing are considered and issues affecting public and private clouds, and when a hybrid is applied, problems that can be encountered individually, probable solutions based on their examination are explored. Even though cloud computing effectively reduces the cost and maintenance of IT industry

security issues plays a very important role. More and more IT companies are shifting to cloud based service like Private, Public and Hybrid cloud computing. But at the same time they are concerned about security issues. According to a recent research by (Coppolino et al,2016), the three major vectors of attack are network, hypervisor, and hardware. These vectors are mapped to attacks such as external, internal, and cloud provider or insider attack respectively. This paper is to do a descriptive study of hybrid cloud security, check threats to it and proffers probable solutions.

2 Literature Review

2.1 Types of Clouds

Private Cloud

It is a cloud computing platform built on a user's own hardware and software P. Mell, Grance,(2011), Hamrén(2012). It is also known as internal cloud or corporate cloud. It provides hosted services to a limited number of people behind a firewall. A Private Cloud is implemented using a dedicated data center infrastructure of hardware and software that is used privately by an organization. It is not shared with another organization. If the data center is shared, that is a Virtual Private Cloud. A Private Cloud may participate in a Hybrid Cloud.

Public Cloud

Here the service provider makes resources like application, infrastructure and storage, available to the customers and businesses over the internet. P. Mell, Grance,(2011), Hamrén(2012). The service providers like Microsoft Azure, Google App engine, Amazon web Server etc. A Public Cloud is implemented using a shared data center infrastructure of hardware and software that is shared by multiple organizations(Veruscorp,2013).

Hybrid Cloud

When an organization wants to maintain different business applications with different levels of security, hybrid cloud is most viable for this(W. Jansen(2013) ,T. Grance(2011)).A Hybrid Cloud is any combination of Clouds. It could be a Private Cloud and one or more Public Clouds. Similarly, it could be a Virtual Private Cloud and one or more Public Clouds. It is, however, more than just multiple Clouds. There needs to be resources shared among the Clouds. An example is Cloud Bursting.

2.2 Advantages of Cloud

According to Avram(2014) , there are some unique advantages to cloud computing. Some of the key advantages are:

- Minimized costs for new entrants
- Limited time constraints on access to resources
- Reduction in IT barriers to innovation
- Easy scalability

3 Threats to Hybrid Computing

Cloud computing, like other areas of IT, suffers from a number of security issues,

which need to be addressed (Coppolino, L., D'Antonio, S., Mazzeo(2016) G., & Romano, Ramachandran,(2015)

Lack of encryption: Data stored in the cloud is often not within an organization's control. Instead, it may rely entirely on best security practices by third parties Goyal(2014). When a company provides services via the cloud, customers only know they can access their applications and data when they want but customers do not know where their data is stored

Inadequate security risk assessment: Information security risk assessment is an on-going process of discovering, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information system

Poor data redundancy: Data redundancy is a condition created within a database in which the same piece of data is held in two separate places.

Data leakage: with data protection moving from cloud consumer to cloud service provider, the risk of accidental, malicious, and intentional data breach is high.

Lack of data ownership:

Cross platform tools: Cross-platform tools refer to the development of tools that can be used on multiple mobile platforms.

Unprotected API's:

Authentication: Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server.[Goyal(2014)

Poor security management:

Denial of service: any denial of service attack on the cloud provider can affect all tenets

Distributed denial of service attacks (DDOS):certain features of cloud computing can be used for malicious attack purposes such as the use of trail period of use to launch zombie or DDoS attacks.

Poor IP protection: many vulnerabilities inherent in IP such as IP spoofing, ARP spoofing, DNS poisoning are real threats.

4 PROBABLE SOLUTION

Lack of encryption: Shielding transmissions from random attacks with cryptographic protocols that include endpoint authentication. Encrypting all transmissions using Secure sockets layer and Transport layer security (SSL/TLS) to manage server authentication and prevent interception of data off the wire, cryptographic protocols that provide communication over a network. Also, employing a reliable VPN and using a reliable proxy server and Using Secure Shell (SSH) network protocols to send unencrypted traffic over a network.

Inadequate security risk assessment: A holistic approach is the best way to handle network organization security using a reliable Security Information and event management (SIEM) system. This way all enterprise security data can be viewed and easily trended. Intrusion detection system and Intrusion prevention system (ID/IPS)

systems should always scan for any malicious traffic.

Poor data redundancy: This can be accomplished three ways by utilizing:

- multiple data centers from one cloud provider
- from many public cloud providers,
- and from a hybrid cloud

Poor compliance: The two clouds must be coordinated. The public cloud provider and private cloud must be in compliance, and demonstrate the compliance of the two clouds as they work together. The two cloud should also meet industry standards for data security when handling sensitive data.

Data leakage: Since the enterprise customer owns customer data, security is the customer's responsibility. Security measures must be able to counter infrastructure malfunctions, security breaches, and software errors.

Lack of data ownership: Data ownership and security must be verified. Avoiding vendors who cannot provide reasonable ownership expectations. Getting everything defined from the provider in a well-constructed Service Level Agreement (SLA) that covers a hybrid IT enterprise. Also, knowing exactly who has access to data, what the provider does with access logs, and the geographic location of all stored data.

Cross platform tools: Developing Cloud application migration tools for interoperability and moving apps between private and public clouds. Cloud monitoring tools that accommodate a virtualized environment should be used. Cloud automation tools to maintain access and security needed for dynamic cloud provisioning and VM movement.

Unprotected API's: API keys must be handled in the same manner as encryption and code-signing keys. Third- party developers must be sure to handle keys securely. Always verifying a third-party before releasing API keys to avoid a security breach.

Authentication : Monitoring and verifying all access permissions and Synchronizing data security by using an IP Multimedia Core Network Subsystem (IMS).

Poor security management: Replicating controls for either clouds, synchronizing security data or using an identity management service that works with systems run in either cloud. Maintaining in-house data storage for sensitive data not appropriate for the public cloud.

DOS attacks: Denial of Service attacks on cloud management APIs are often caused by sending bad Simple object access protocol (SOAP) or Representative state transfer (REST) requests from the enterprise. Flow analytics can fend off DOS attacks by reacting to the incursion and redirecting traffic to a mitigation device. The flow analytics tool must be scalable for the amount of traffic it gathers and analyzes. Because it is a slower method, it is not as effective in combating volumetric (DDoS) attacks.

Distributed denial of service attacks (DDOS): Fending off a DDoS attack requires robust in-path deployment of a DDoS mitigation device that continuously

processes all incoming and outgoing traffic. The device must be able to act immediately and scale and perform when there are multi-vector attacks.

Poor IP protection: Completely automated systems are inadequate in classifying IP and quantifying risk. These tasks must be done manually. Risks associated with IP can only be identified once that data is classified. Also, conducting extensive third-party audits.

5 Conclusion

The fast development of Internet-based computing allows several technologies to be developed to meet increasing demand. However, the importance of security is still emerging. Security needs to be built at every layer in a cloud-computing platform by incorporating best practices and emerging technologies to effectively mitigate the risk.

References

[1] Gartner(2012) Cloud Computing . Retrived April 15,2012 from http://www.gartner.com/technology/it-glossary/cloud omputing.jsp

[2] Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2016). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2016.03.004

[3]Ramachandran, M. (2015). Software security requirements management as an emerging cloud computing service. International Journal of Information Management, Vol. 36, Issue 4, pp. 580-590.

[4] Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. Procedia Technology, Vol. 12, pp. 529-534.

[5] International Journal of Computer Applications (0975 – 8887) Volume 55– No.13, October 2012 , Security Issues: Public vs Private vs Hybrid Cloud Computing

[6]. Roundup of Cloud Computing Forecasts and Market Estimates, 2015. (2015). http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/#56c0b0f0740c (Retrieved 2 May 2016)

[7] Wang, C. (2009). Cloud Computing Checklist: How Secure Is Your Cloud? (2009). Forrester Research. https://www.forrester.com/report/Cloud+Computing+Checklist+How+Secure+Is+Your+Cloud/-/E-RES55453

[8] R. Buyya, C. S. Yeo, and S. Venugopal, ―Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities,‖ In: Proceedings of 10th IEEE International Conference on High Performance Computing and Communication, Dalian, China, Sep. 2008, pp. 5–13.

[9] S. Ostermann, A. Iosup, N. Yigitbasi, R. Prodan, T. Fahringer and D. Epema, ―A performance analysis of EC2 cloud computing services for scientific computing, In: Cloud Computing (pp. 115-131). Springer Berlin Heidelberg, 2010.

[10] Sumit Goyal - I.J. Computer Network and Information Security, 2014, 3, 20-29 Published Online February 2014 in MECS MECS I.J. Computer Network and Information Security, 2014, 3, 20-29 , Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review

[11] P. Mell and T. Grance, ―The NIST definition of cloud computing (draft), NIST special publication, 800(145), 7, 2011.

[12] O. Hamrén. (2012). M.S. Thesis. ―Mobile phones and cloud computing.

[13] Veruscorp Website. (2013) .Available: http://www.veruscorp.com/public-cloud-networks.aspx.

[14] Search cloud computing Tec target Website. [Online] (2013) . Available: http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud

[15] W. Jansen and T. Grance, ―Guidelines on security and privacy in public cloud computing, NIST special publication 800-144, 2011.

[16] Khalil H. A. Al-Shqeerat et al(2017): Cloud Computing Security Challenges in Higher Educational Institutions – A survey,International Journal of Computer Applications (0975 – 8887) Volume 161 – No 6.