www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 6 June 2017, Page No. 21875-21879
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i6.54

An overview on Cloud Security and Proposed Solutions

Jamuna K M
Dept. of Computer Science and Engineering
PA College of Engineering, Manglore, Karnataka, India

Abstract

Cloud computing has revolutionized the world of computing in the last few years. The benefits such as reduced costs, rapid application deployment, and elastic resources, have made many organizations to utilize cloud resources or host much of their data in the cloud. Recent studies shown that more than 70 percent of the world's businesses now operate some of their operations in the cloud. But the security of the data stored in cloud is the major concern. This paper gives a vogue idea about the cloud security threads and its proposed solutions.

I Introductions

Cloud computing can be defined as a model for enabling ubiquitous, convenient and on demand network access to a shared pool of configurable computing resources that can be swiftly provisioned and released with least administration effort from the user side and least service provider interaction. The main objective of the cloud computing is that the customers can use and pay only for what they used. Cloud is not simply the latest term for the Internet, though the Internet is a necessary foundation for the cloud, the cloud is something more than the Internet. The cloud is where you go to use technology when you need it, for as long as you need it. You do not install anything on your desktop, and you do not pay for the technology when you are not using it. The cloud can be both software and infrastructure. It can be an application you access through the Web or a server like Gmail and it can be also an IT infrastructure that can be used as per user's request.

II Background

Cloud computing consist of three services, Software as a service (Saas), Platform as a Service (Paas) and Infrastructure as a service(Iaas).

Saas is a service model such that the consumer is allowed to use the cloud provider's application on cloud. For example Gmail is a Saas service provided by Google to use email application. To use this application there is no need to install application on the consumer's local machine. The complete control of the application is under the control of service provider so consumers, no need to worry about the management of server or data. This application is very cost effective.

Paas is a service where the user can run and also manage the program developed by them using the deployment and development tools provided by cloud. This service is useful for the developers or small scale enterprisers who are not financially fit to buy the platform by their own.

Iaas is a service that provides the end users access to large scale computing resources, such as servers, networking devices, storage. The major benefit for Iaas is the reduction in hardware costs.

Cloud deployment models

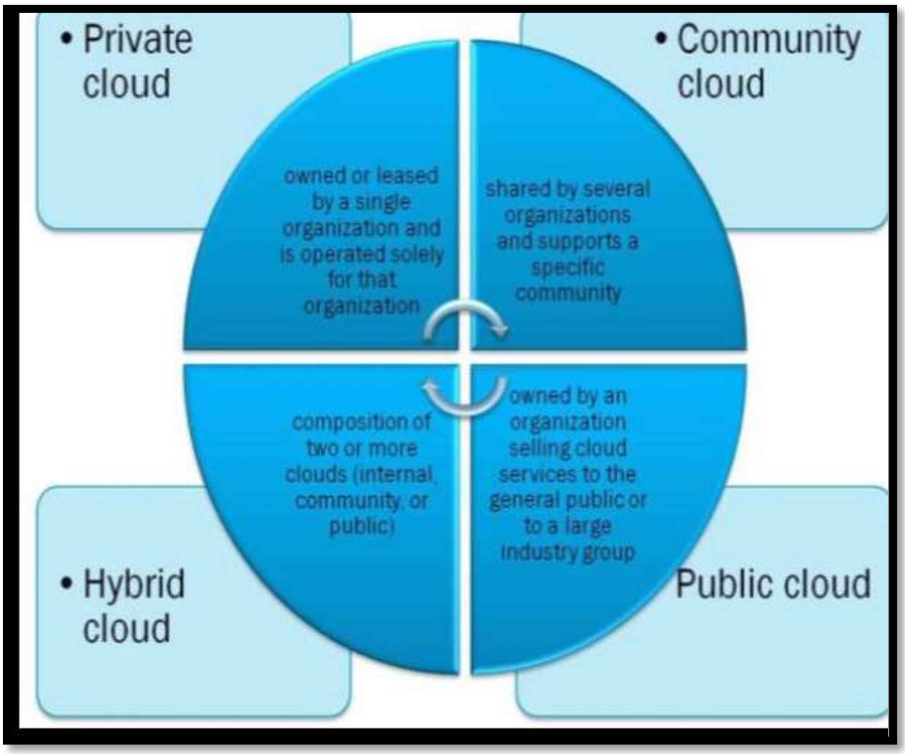
• Private cloud
• Community cloud
owned or leased by a single organization and is operated solely for that organization
shared by several organizations and supports a specific community
composition of two or more clouds (internal, community, or public)
owned by an organization selling cloud services to the general public or to a large industry group
• Hybrid cloud
Public cloud

Figure 1: Cloud deployment models

Public Cloud: These services are available to the clients from actually a third party service provider through the web. Public clouds are also secure and the data would be publically available. The vendors provide particular right of entry control mechanism for its users.

Private Cloud: This type of infrastructure is operated only for a single organization but it can be managed by some other organization or any third party.

Hybrid Cloud: It is a combination of public and private cloud. In this model the users mainly subcontract non-critical data and process towards the public cloud, whereas keep the critical information and the services in their private control.

Community Cloud: This cloud model is managed by a group of organizations which share the same interests. It can also be controlled by a third party.

III Literature survey

Modi et.al [1] in his a review paper tells about the security issues on higher levels in cloud and also he projected some solutions for those problems. Xiao and Chen[2] in their paper describes about the the main security issues and also about the techniques to counter the vulnerabalities present in it. Neng Hai et.al[3] also describes about the recent security issues. Mell and Grance [4] made a survey on popular security models such as cube model, multi tenancy model, risk assessment model. Srinivas, J.., et al. [5] in this paper proposed various concepts involved in cloud computing. Cloud is discussed from technical and service aspects and some of the opportunities in cloud computing have been highlighted. Sabahi, F [6] talked about the cloud deployment strategies, delievery models and Cloud RAS (Reliability- Availability- Security) Issues. Shaikh, F. B. and S. Haider [7] described all the security and privacy issues, tools and models proposed against security threats and analyzed the diverse security models and tools.

Security in cloud computing

Moving critical and sensitive data to cloud makes the organizations a major concern. The data moved to cloud is under the control of cloud provider. The user is unaware of the data location or the security of the data. The major factor that needs to exist between a user and the cloud provider is trust. A threat is major attack that leads to misuse of data or resources that lead to undesirable result. Table 1 shows the list of cloud security threads. Table 1 shows the different security threads and its description.

Threat	Threat Describtion
Data Breaches	Release of protected data in an untrusted environment
Data Loss	Information is lost due to improper storage, transmission or processing
Traffic Hijacking	Account or Service Attack methods such as fraud and exploitation of services
Insecure APIs	Attack on code-signing keys used by web and cloud for identification
Denial of Service	Refusing user access to their data or applications
Malicious Insider	Any insider misusing their authority to harm the cloud system
Abuse of cloud services	Using the cloud servers and services for malicious activities
Insufficient Due Diligence	Risk due to incomplete understanding of the cloud infrastructure

Shared Technology	Attacks due to multi-tenant architecture, re-deployable platforms and shared resources services

Table 1: Describtion about cloud security threads

Security threads and proposed solutions

A. *Data breach*

A data breach occurs when an unauthorized individual or organization gains access to sensitive, protected, or confidential data. Encryption and key management techniques are used to protect against data breaches. The concept is that the once the data is encrypted using the secret key, unauthorized users will not be able capture the encrypted data. But man in the middle attack is possible in cloud. So the cloud providers started using Data Loss Prevention (DLP) tools. The use of DLP tools has made reduction of data breaches possible, but end user action is also required to enable these tools.

B. *Account Hijacking/ Maintenance*

Many users have access to data which they do not need access to in case of carelessness. In fact, many companies fail to remove file access rights to users that have been fired or moved to other areas in the company. Another general mistake which leads to account vulnerability is unsecure code. Another cause of account hijacking is weak passwords. Most end users continue to use passwords that are easy to guess or brute force using tools freely available in the Internet. Multi-factor authentication is the preferred way to securely authenticate users on the cloud. Authentication methods used are mutual authentication, password and smart card, biometric authentication. A cloud adoption risk report from the fourth quarter of 2015 revealed that only 18.1 percent of end users take advantage of multi-factor authentication.

C. *Multitenancy Threats*

Most security concerns in multitenancy occurs when multiple organizations accessing the same virtual infrastructure that houses the services. This is known as co-residency. Co-residency has many threats since machines can be placed in a honored position relative to one another. Threats which have elevated risks due to co-residency are; unauthorized connection monitoring, unmonitored application login attempts, malware propagation, and man in the middle attacks. Many regulatory acts require that businesses can only access information on need to know basis. In order to ensure these protections, segmentation is enabled.

Current Segmentation – Many cloud providers offer segmentation at all levels, but in most cases securing the data is the responsibility of the the end user. APIs have been created to introduce proper segmentation, isolation, and protection for tenant resources

VM Introspection – Newer products utilize VM introspection to fill in the gap and provide those missing details about the hypervisor. Segmentation and VM Introspection show promise to protect users against multitenancy threats.

Conclusion

Cloud computing is technology which provide the customers the facility to store data, execute data or to provide the infrastures required. The cloud data security is the responsibility of cloud providers which they should keep the confidential data secure and keep the users trust on them. This paper provided an over view about cloud services and its deployment models along with the security threats and proposed solutions.

References

[1] C. Modi, D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing. " *The journal of super computing*" volume 63 ,no 2 ,pp 561- 592, 2013.

[2] Z. Xiao and J Chen, "cloud computing security issues and countermeasures" in proceeding of 4th international Conference on Computer Engineering and Networks, Springer *International Publishing*, 2015.

[3] Y. Neng-Hai, Z. Hao, J. Xu, W. Zhang and C. Zhang, "Review of cloud computing security," *Acta Electron Sinica*, vol. 41, no. 2, pp. 371-381, 2013.

[4] P. Mell and T. Grance, "The NIST definition of cloud computing," Computer Security, 2011.

[5] Srinivas, J., et al. (2012). "Cloud Computing Basics." International Journal of Advanced Research in Computer and Communication Engineering, 1 (5).

[6] Sabahi, F. (2011). Cloud computing security threats and responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, IEEE.

[7] Shaikh, F. B. and S. Haider (2011). Security threats in cloud computing. Internet technology and secured transactions (ICITST), 2011 international conference for, IEEE.

[8] Kumar, P. "Security Threats to Cloud Computing."

[9] Silva, C. M. R. d., et al. (2013). Security Threats in Cloud Computing Models: Domains and Proposals. Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on, IEEE.