International Journal of Engineering &Technology, 7 (1.7) (2018) 186-188

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Cloud – IAAS security threats and its possible mitigations

R Priyadarshini [1*], N.Malarvizhi [2]

[1]*Research Scholar, Dept of CSE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology*

[2]*Professor, Dept of CSE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology*

**Corresponding author E-mail: darshini.sr@gmail.com*

Abstract

Cloud IaaS, a virtual data center is an instant computing infrastructure provided and managed over the Internet. The provider owns the resource and maintains it in the level specified in the SLA. The user is permitted to use the resources as services like operating systems, security, networking, application developing servers, application deploying tools, databases, etc., on the basis of pay-per-use model. The providers and users both are concerned over integrity, privacy and security issues. This study distinguishes the issues identified with the cloud IaaS layer and strategies to overcome them to maximize the performance.

Keywords: *Infrastructure as a service (IaaS), Delivery models, SLA*

1. Introduction

Cloud computing is defined as "a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet"[9]. Infrastructure as a service (IaaS) is a virtualized service of cloud computing which is outsourced. Here a consumer can rent all provided resources such as storage, data center, band-widths, operating system, load balancers, firewalls etc., without considering the hardware support. Many organizations are readily adopting IaaS service, as they need not want to worry about the requirement or infrastructure available for the services. The consumers have to pay for the service they use and the providers are sole in charge for the infrastructure i.e., the consumer need not worry about the maintenance and management which will be taken care by the providers. In IaaS also we can find some security threats like, external network attacks: Man in the middle attack, flooding attack, data leakages, etc. which can affect the infrastructure. Though IaaS helps a consumer to avoid the complexity and expense of obtaining and managing their own servers, this kind of cloud environments are open for all kinds of phishing, exploits, scams and various other attempts to manipulate data.

1.1 Infrastructure as a Service

In this model a consumer pay for the resources provided by the provider. The provider is the one who maintains and owns the resources. A Service Level Agreement (SLA) will be made between the consumer and the provider regarding the level of the resources and billing details. The consumer will be paying for the part of the resources credited to their account, in which they can install OS, applications, libraries and other software within the Virtual Machine. But the consumers have limited control over networking and security.

1.2 Features of Infrastructure as a service

The following features are considered by the organizations for the adaption of Infra-structure as a service:

- Utility-style computing: The consumer will be utilizing the provider's infrastructure service with pay-per-use billing.
- Dynamic scalability: The service provider takes the responsibility to ensure that the service like memory, bandwidth, storage, servers etc. utilized by the user will be fulfilled dynamically.
- Service availability: The consumer should be provided with greater availability of the service through SLA; from business point of view it is very much important to maintain this.
- Automation of administrative tasks: Tasks including virtual servers, resource pool management and desktop management for different consumers should be made automated in the provider side.
- Technology upgrade: The service provider should update with latest technology, so that the consumer will get the latest hardware with lowest cost.

1.3 IaaS Advantages

The maintenance and upgrades of tools, database systems, etc. and the underlying infrastructure are the responsibility of the organization. The various billing models allows for paying for what is been used, for example, an individual or a small organization could not afford for a development software on a dedicated server. Multiple platforms are supported by some IaaS providers which can be utilized for similar application development. The new releases of technology will be updated by the provider themself. The management of the data center, backups, and software even the failover everything will be managed by the Cloud IaaS provider.

Copyright © 2018S Alex David, Almas Begum, S Ravikumar. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1.4 IaaS Disadvantages

The user is sole responsible for the developed software, its maintenance and upgrades of tools, database systems, etc. Sometimes the deployed software has to be modified when there is a software update by the IaaS provider. If a high speed interaction is required for the access between the clouds and data then relying on the internet will not provide the speed required. Sometimes, legal issues are faced when the data storage is out of country. The security provided by the provider may not adequate the consumer needs.

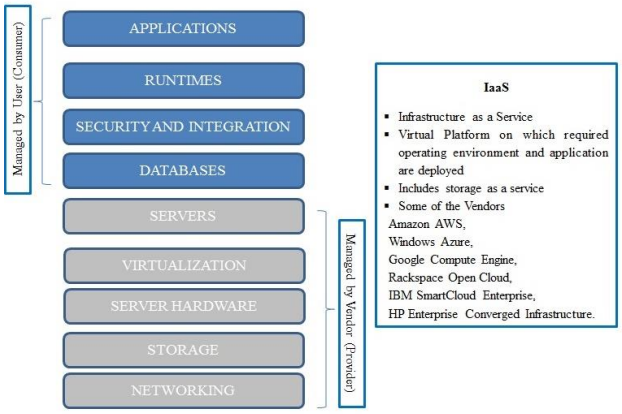


Figure 1: Structure of Infrastructure as a Service

2. Security concerns in Infrastructure as a service

Both users and providers are concerned about the privacy and security. Cloud Infrastructure is sole responsible for the Security of any service that run in the cloud. Cloud IaaS have some issues that needed to be resolved for their high performance.

2.1 Security issues concerned

I. Issues related to SLA:
Service Level Agreement is the understanding made between the service provider and the consumer to make and maintain the trust for quality of services. The important challenges concerned are how to monitor the SLA and how to put into effect the SLA in the system used, so as to maintain the agreement made between the providers and consumers.
II. Issues related to utility computing:
Utility computing, where the users are charged according to their usage of services. Here, the problem is its complexity in metering the use, i.e., when the service provided to one user is carried on to another user, and it becomes difficult in metering the services for charging. Also this system becomes an easy target to the attackers.
III. Issues related to cloud software:
Cloud software is the software which joins the cloud components together as a single component. The XML services security standards can be attacked by the attacker and even against the web services which can break the service communications, literally creating disturbance in cloud process.
IV. Issues related to Networks:
When connected in internet the issues like: Man, in the middle attack where a hacker hacks between two systems and gets access to their private details or flooding attack, where a hacker sends huge amount of unwanted request to attack the information in the network.
V. Data leakage:
Data in the cloud when exposed to the unauthorized user creates data leaks; it means only the recognized users must access the data. This may affect both the consumers and IaaS providers.
VI. Logging and reporting records:
It is must to have proper logging and reporting modules, so as to keep track of details about of the information, user, machines handling information, storage area details etc.
vii. Authentication and authorization:
The most common security measures, that has to be maintained in any system. The high secure authentication mechanism is always required for authorized user for the service usage.

2.2 Protection Methodology

Protection methods at each level have to be applied in order to reduce risks associated with information security. The infrastructure security zones should have monitoring and audit tools, the regular software update scheduling and regular testing and vulnerability analysis.
The following protections are suggested by different authors to the issues concerned:
I. WSLA framework
The solution to the SLA maintenance is Web Service Level Agreement (WSLA) framework, which is used to define and monitor SLAs for web services. WSLA framework consists of a flexibility based on XML schema and runtime architecture, provides SLA trust by allowing the third parties outsourcing with task of maintaining the SLA provisions in cloud computing. [5]

II. Amazon Devpay
Amazon Devpay like application can be used for metering the levels of service used. It meters the customer usage and bills them accordingly. Even it keeps track the customer levels and pipeline their order for which billing is done. From consumer point of view they should also maintain their authentication keys secured and authorized users. [7]
III. XML Signature and Encryption
XML signature is used as a solution to avoid XML service types of attack by authentication and integrity security. XML Encryption can also be used as another solution. In this the original data has to be encrypted and again decryption has to be performed to get the information. [4]
IV. Traffic Encryption and Network Monitoring
Traffic encryption can be used as a solution to sidestep the externals attacks. By monitoring services in the network, all the parameters concerned are ensured in working condition. In this measure, the outlined activities are hided from the user, protects the sensitive information like password, personal details etc. to the attacker. Firewalls are also used for the protection from the outside attackers. [3]
V. Usage monitoring:
The issues concerned with data leaks can be resolved by restricting the data usages i.e. continuous monitoring of the data usage has to be performed. The usage has to be monitored continuously for the performance improvement. [3][11]
vi. Data Encryption
Data protection is popularly done by encryption, where the original data is converted to another form, using an algorithm. Where the encryption key storage has to be maintained and secured.
VII. Vulnerability Control
Vulnerability control has to be used and implemented together with regular software updates. This will reduce the risks associated with information security for both the IaaS provider and its clients.

3. Conclusion

The fundamental concentration in this paper is to examine distinctive sorts of security threats to cloud IaaS and strategies to relieve them. These are few issues that must be settled before sending any administration in cloud. Legitimate nature of administrations and superior exhibitions of the providers require appropriate observing of their sources in successful approaches to accomplish. On the off chance that these security threats of IaaS are

not fathomed, it might lead to failure of entire infra-structure. As part of future work, we can analyze few security issues and mechanism to mitigate them.

Reference

[1] Bineet Kumar Joshi, Mohit Kumar Shrivastava, Bansidhar Joshi, 2016, Security threats and their mitigation in infrastructure as a service, Perspectives in Science, ISSN: 2213-0209, Vol: 8, Page: 462-464

[2] Arora, P., Wadhawan, R.C., Ahuja, E.S.P., 2012. Cloud computing security issues in infrastructure as a service. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2 (January (1)).

[3] Bhardwaj, Y., Kaushik, M., 2014. A review paper on virtualization and security in cloud computing. Int. J. Adv. Res. Comput. Sci.Softw. Eng. 4 (March (3)).

[4] Dawoud, W., Takouna, I., Meinel, C., 2004. Infrastructure as a service security: challenges and solution. IEEE.

[5] Jaiswal, P.R., Rohankar, A.W., 2014. Infrastructure as a service: security issues in cloud computing. IJCSMC 3, 707—711.

[6] Jenson, M., Schwenk, J., Gruschka, N., Lo Iacono, L., 2009. On technical security issues in cloud computing. IEEE.

[7] Padhy, R.P., Patra, M.R., Satapathy, S.C., 2011. Cloud computing: security issues and research challenges. Int. J. Comput. Sci. Inf.Technol. Secur. 1 (December (2)).

[8] Rumale, A.S., Chaudhari, D.N., 2013. Cloud computing: infrastructure as a service. Int. J. Invent. Eng. Sci. 1 (3).,

[9] Nikos Antonopoulos, Lee Gillam,2010, Cloud Computing: Principles, Systems and Applications Springer Science & Business Media.

[10] Kailash Jayaswal, Jagannath Kallakurchi, Donald J. Houde, Deven Shah, 2014, Cloud Computing Black Book, Dreamtech Press.

[11] Krutz, R.L., Vines, R.D., 2014. Cloud Security. Wiley Publication.