Perspectives in Science (2016) xxx, xxx–xxx

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/pisc

Security threats and their mitigation in infrastructure as a service☆

Bineet Kumar Joshi[a,*], **Mohit Kumar Shrivastava**[a], **Bansidhar Joshi**[b]

[a] *Faculty of Science & Technology, ICFAI University, Dehradun 248197, India*
[b] *Department of Computer Science, JIIT University, Noida 201306, India*

Received 9 December 2015; accepted 5 May 2016
Available online xxx

KEYWORDS
Infrastructure as a service (IaaS);
Delivery models;
Virtualization;
Service level agreement;
Data leakage

Summary Cloud computing is a hot technology in the market. It permits user to use all IT resources as computing services on the basis of pay per use manner and access the applications remotely. Infrastructure as a service (IaaS) is the basic requirement for all delivery models. Infrastructure as a service delivers all possible it resources (Network Components, Operating System, etc.) as a service to users. From both users and providers point of view: integrity, privacy and other security issues in IaaS are the important concern. In this paper we studied in detail about the different types of security related issues in IaaS layer and methods to resolve them to maximize the performance and to maintain the highest level of security in IaaS.

Introduction

Infrastructure as a service delivers a virtualized outsourced service in cloud computing. In IaaS consumer can rent all possible IT resources as storage, data center, bandwidths, OS, firewalls, load balancers, etc., without worrying about the hardware requirements and the infrastructure. Many organizations are adopting IaaS services, because the organizations need not to worry about the hardware or infrastructures for services, they only have to pay for that service and the providers are responsible for providing the whole infrastructure.

In IaaS there are some security threats which can affect the infrastructure like, external network attacks: Man in the middle attack, flooding attack; Data leakages, etc. This paper tried to identify some of the threats in IaaS and provides an abstract solution for that threat.

The rest of the paper is organized as follows. 2nd section discusses features of IaaS and lists some of the companies providing IaaS services. In 3rd we discuss various security issues in IaaS. Conclusion and future works are discussed in final section.

☆ This article belongs to the special issue on Engineering and Material Sciences.

* Corresponding author. Tel.: +91 9410581742.
E-mail address: bineetjoshi@gmail.com (B.K. Joshi).

http://dx.doi.org/10.1016/j.pisc.2016.05.001

Please cite this article in press as: Joshi, B.K., et al., Security threats and their mitigation in infrastructure as a service. Perspectives in Science (2016), http://dx.doi.org/10.1016/j.pisc.2016.05.001

Table 1 International and national companies (Rumale and Chaudhari, 2013).

Name of company	Data hosting	Network hosting	Virtual machines	Database services	International/Indian	Popular products
Amazon	√	√	√	√	International	Amazon EC2
Rackspace	√		√	√	International	Cloud files
Google	√		√	√	International	Google Storage
Netmagic Solutions	√	√		√	Indian	CloudNet
Zenith InfoTech	√			√	Indian	PROUD
Cynapse India	√	√		√	Indian	Cyn.in

Infrastructure as a service

In IaaS, the service user can concentrate to run their operations. The consumer needs not to worry about other housekeeping work like purchasing, managing and maintaining the hardware.

Features of infrastructure as a service

IaaS has following features that lead to adaption of Infrastructure as a service within the organizations:

A. **Dynamic infrastructure scaling:** It will be the responsibility of service provider to ensure that the service user requirements of infrastructure will always be full filled without dynamically.
B. **Guaranteed uptime:** The service providers should guarantee 99.94% or greater availability with 100% guaranteed uptime through service level agreement, as it is very crucial for business point of view (cDW).
C. **Administrative tasks automation:** The service providers should deploy such a system that tasks such as virtual servers and desktop management for different entities (employees and guest), virtual server pools management become automated (cDW).
D. **Availability of the latest technology:** It is responsibility of the service provider to be always equipped with latest technology. Due to this a consumer will get upgraded hardware and other equipments with lowest cost.

List of companies providing infrastructure as a service

Some of the companies and their product are shown in Table 1.

Security issues in infrastructure as a service

Privacy and security are the important concern from both users and providers point of views. Infrastructure as a service has also some issues that needed to resolve for proper high performance. These issues can be divided in two categories.

Component wise security issues

Service providers visualize the services into some components that help them to recover the respective issues with that component. There are some threats like billing issues of services, network related attacks in IaaS that can affect the infrastructure. So it is the best practice to resolving the security issues with each and every component of IaaS. Some of these issues are discussed below.

A. **Service level agreement related issues:** SLA is the contract between the service provider and the client to make the trust for quality of services and guaranty uptime. The challenges are how to proper monitoring in SLA and how to enforce the SLA in environment to keep the trust between providers and clients. The solution is Web Service Level Agreement (WSLA) framework, which is designed for SLA monitoring and enforcement in Service Oriented Architecture. WSLA manages SLA trust by allowing the third parties innovation with task of maintaining the SLA provisions in cloud computing (Jaiswal and Rohankar, 2014).
B. **Utility computing related issues:** Utility computing is the commercial face of grid and cluster computing where users are charges according to usage of services. First challenge in utility computing is the complexity, i.e., the 1st service providers provides services to 2nd, which also provides services to other, then it is difficult to metered the services for the charges. The other challenging issue is that this whole system will became an easy target for any attackers, who want to access services without paying any money. The solution for first challenge is like Amazon Devpay. It allows provider at 2nd level to meter the service usage at this level and accordingly bill the consumer of the service. The solution for second challenge is that service provider should keep the system clean and attack free. Client's practice also affects the system, so the client also need to keep secure their authentication keys (Padhy et al., 2011; Arora et al., 2012).
C. **Cloud software related issues:** Cloud software is that key which joins the cloud components together that they can act as single component. An attacker can attack against the XML services security standards and attack against the web services that can lead to break the communication of services. The solution to avoid these types of attacks is XML signature for authentication

Please cite this article in press as: Joshi, B.K., et al., Security threats and their mitigation in infrastructure as a service. Perspectives in Science (2016), http://dx.doi.org/10.1016/j.pisc.2016.05.001

and integrity protection. The other solution is the XML Encryption. It wraps the data in a encrypted manner and decrypted that data to get the original data (Dawoud et al., 2004; Jenson et al., 2009).

D. **Networks related issues:** Networking services and internet connectivity plays an important role in delivering a service over the internet (Cloudscalling). There are some issues in networks and internet connectivity likes: Man in the middle attack where a hacker manipulates the network connectivity by creating middle man addressing, from where the attacker can access all the confidential data and permissions. Another type of attack is flooding attack, in which an unauthorized user sends a huge amount of request that lead more chances to attack on that demand. The possible solutions are traffic encryption by using point to point protocols that encrypt the connectivity to avoid the externals attacks. Another solution is, by proper network monitoring on services that whether all networking parameters are working properly or not, the externals attacks can also avoided by implementing the firewalls we can protect the connectivity from outer attacks (Cloudscalling; Bhardwaj and Kaushik, 2014).

Overall security issues

Overall security issue is the view on the basis of overall services provided by an IaaS provider. Some of the overall security issues are:

A. **Data leakage and usage monitoring:** Data stored in the cloud should be kept confidential. It means it should be known that only authorized user should access data and the manner the in which data is going to be accessed. These issues can be resolved by up to date right data managing services by restricting the data usages. The usage should be monitored continuously (Bhardwaj and Kaushik, 2014; Krutz and Vines, 2014).

B. **Logging and reporting:** To make deployment of IaaS more efficient proper logging and reporting modules should be used effectively. A good logging and reporting solutions should always keep track of where about of the information, its user, information about machines handling it and which storage area are keeping it.

C. **Authentication and authorization:** It is one of the most common security measures a system has to maintain. It is well known fact that only a user name and password is not enough for a high secure authentication mechanism. A service provider should use multi-factor authentication.

Conclusion

These are the some issues that must be resolved before deploying any service in cloud. Proper monitoring of the resources must be done in an effective ways to achieve proper quality of services and high performances from the providers.

Our main focus in this paper is to study different types of security threats to IaaS and methods to mitigate these threats. These threats can be detected by two approaches: first one is component wise threats and second is overall service related threats. These security threats of IaaS must be solved otherwise they will lead to failure of whole infrastructure. As a part of future work we can focus on one or two security issues and analyzes the different mechanism followed by big companies to mitigate these concerns and the effectiveness of this mechanism to make IaaS more reliable and robust.

References

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)).

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)).

cDW. http://www.800.800.4239|cDW.com.

Cloudscalling. http://www.cloudscalling.com.

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

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

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

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

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)).

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

Please cite this article in press as: Joshi, B.K., et al., Security threats and their mitigation in infrastructure as a service. Perspectives in Science (2016), http://dx.doi.org/10.1016/j.pisc.2016.05.001