Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 1, January 2017, pg.178 – 181

A Review- Cloud and Cloud Security

Ashima Narang

Computer Science Department, Amity University, India

ashimanarang04@gmail.com

Abstract— The distribution of computing resources is done using a new technology called Cloud Computing. The efficient computing and storage can be achieved in an adaptable manner with the services offered by Cloud. The industry has welcomed this technology for achieving the change in information technology but there are risks associated with this technology. The work is in process to avoid such risks and to overcome them.

Keywords— Cloud Computing, PaaS, IaaS, SaaS

I. INTRODUCTION

Cloud Computing can be classified as a new paradigm for dynamic provisioning computer services supported by data centres that usually employ virtual machine (VM) technology for consolidation[1]. Cloud computing provides infrastructure, platform and software as services that is available to the consumer under the pay as you use model. The customers using a particular cloud, can access the resources provided by a cloud provider, according to the Service Level Agreement (SLA) given by the same cloud provider. In distributed data centres, the technology named virtualization is being used by the clouds to provide the resources to the customer whenever required. Clouds are provided to the customers for giving them three models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).

Cloud Computing has widely been adopted by the industry or organization though there are many existing issues like Load Balancing, Virtual Machine Consolidation, Energy Management, etc. which have not been fully implemented. Central to these issues is the issue of load balancing, that is required to distribute the excess dynamic local workload equally to all the nodes in the whole Cloud to achieve a high user satisfaction [2].

II. CLOUD ARCHITECTURE

Layers:

Cloud Computing architecture has the below given abstract layers which begins from bottom and works upwards. Figure 1 can be referred for the five layers that are constituted in cloud computing. The bottom most layer is known as the physical hardware (HaaS). The customers using the cloud for this particular layer are mostly the big corporations whose requirements are extremely large amount of Hardware as a Service. As a result, the cloud-provider runs, oversees, and upgrades its subleased hardware for its customers [4,2].

The next layer coincides of the cloud's software kernel. The layer acts as a path between the data being processed in the layer of Hardware and software infrastructure layer which is operating the hardware. It is the lowest level of abstraction implemented by the cloud's software and its main job is to manage the server's hardware resources while at the same time allowing other programs to run and utilize these same resources. [5]

The layer above the software kernel is the abstraction layer called the software infrastructure. This layer provides basic network resources to the two layers above it so that it can facilitate a new environment in a cloud that can be delivered to end users as an IT services. The services offered in the software infrastructure layer can be divided into three different categories: Computational resources (IaaS), data storage, and communication [5].

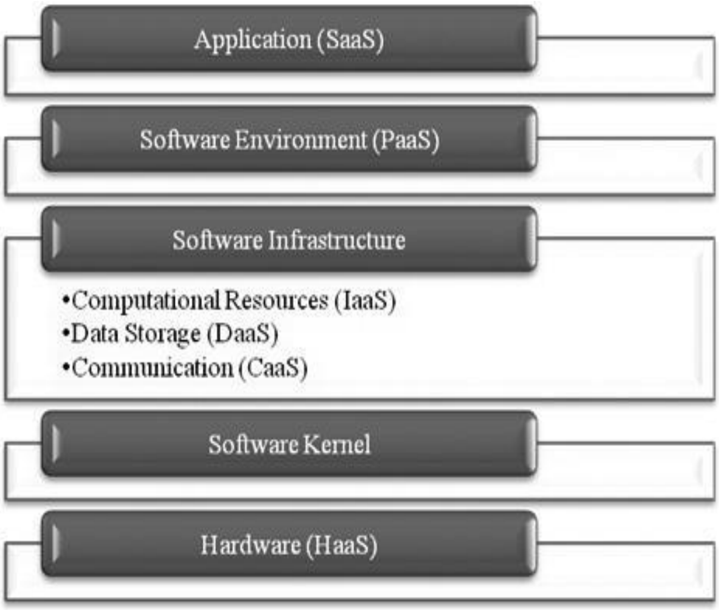

Figure: 1 Cloud Computing Architecture

III. SERVICES PROVIDED BY CLOUD

The services provided by Cloud also divide it into different types of Cloud. For understanding more about cloud, the services provided by cloud may be given as follows:

Platform as a service (PaaS): This provides environment for applications, development of various preparation tools etc. It provides the runtime environment that controls the applications. This type of Cloud, primarily aims to manage the storage, servers and information systems. It aims to facilitate the management problems related to the application development and also helps the customers.

Infrastructure as a Service (IaaS): This provides the elementary resources access such as virtual machinery, storage, physical machinery etc. The manageable things can be the operating system, application, chosen network elements, application. It actually provides the processing, networks, storage and essential resources for the user.

Software as a service (SaaS): This model provides one o use the application as a service to the users. The network, operating system, servers, storage or applications are not managed by the user. The environment is provided for the software distribution.

IV. CLOUD DEPLOYMENT MODELS

There are four different types of cloud deployment models which can be named as Public Cloud, Private Cloud, hybrid cloud and community cloud. The details of these types may be given as follows:

Public Cloud: A cloud infrastructure is managed by a third party and is provided to many customers and which is beyond the firewall of the company. The infrastructure provided, can be used by more than one enterprise at the same time and the resources can be provisioned by users dynamically. The cloud providers are responsible for the management, provisioning, installation and maintenance of the cloud. The cloud providers solely manage and host these clouds. The under usage of the resources are eliminated and the Customers only pay for the resources they use. As the consumers have very less control over the infrastructure, processes requiring powerful security and regulatory compliance which are always not a good fit for public clouds. In this model, there are no restrictions applied on the access and authorization and authentication techniques cannot be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud include Microsoft Azure, Google App Engine.

Private cloud: This type of cloud can be owned or rented and managed by the organization itself or somebody not from the organisation that is the third party and exist at on-premises or off-premises. When compared to the public cloud, It is more expensive and secure than it. There are no additional security regulations, legal requirements or bandwidth limitations are there in private cloud that can be present in a public cloud environment also but by using a private cloud, there is control of the infrastructure and improved security at the end of cloud service providers and the clients have optimized, since the user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems.

Hybrid Cloud: It is a combination of two or more cloud deployment models, linked in such a way that data transferred, takes place between the two different clouds without affecting each other. These clouds would typically be generated by the enterprise and responsibilities for management would be split amongst the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services [7]. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major flaw in the hybrid cloud is the difficulty in creating and governing such a solution effectively. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be any type of a cloud combination i.e. private, community or public clouds which may be linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by a third party service provider or them and rarely offered cloud model. These clouds are based normally on an agreement between business organizations which are related such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook .

V. Issues in cloud with security

Cloud computing has number of possibilities and challenges come across. Security of Cloud is considered to be the most critical point to be considered. The approach to Cloud computing security is very vast and dynamic. The location of the data is a major issue in the security of Cloud computing. One of the important flexibilities for cloud computing is Location transparency, which is security threat at the same time. Cloud users personal data security is thus a concern in a cloud computing environment [10, 11]. The strategic policies of the cloud service provider are of highest significance [12] as the technical security solely is not adequate to address the problem. Trust is another issue which is raised for the security concerns to use cloud service [13] for the reason that it is directly related to the authenticity and credibility of cloud computing environment. Trust in cloud might be dependent on a numerous number of different factors among which some are automation management, human factors, processes and policies [13]. It is most influential soft factor that is driven by security issues inherent in cloud computing to a great extend. The attacks that are applicable to the computer networks and the data in transit equally applies to cloud based services – few of them in this category are the man- in –the middle attack, phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service)attack is one common yet major attack for cloud computing infrastructure [14]. The security of the virtual machine will define the integrity and level of security of a cloud environment to greater extent [15].

Thus, in cloud computing context, a security concern is always some type of risk but any risk cannot be judged blindly to be a concern of security. Allocation of responsibilities among the parties involved in the cloud computing infrastructure might result inconsistency experience which might lead to a security vulnerabilities situation eventually. Any security tools or any other kind of software that are used in a cloud environment might have loopholes in security which would pose in turn as security risks in the infrastructure of cloud itself. The cloud existing as a contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible loopholes in security that could be exploited by an attacker. The approach by which the cloud computing is done has made it prone to both network security issues and information security [15].

VI. Conclusions

Cloud computing as of now we know that it refers to the sustained storage and the advanced sharing of data over the internet. But, the threats from the security is embedded in cloud computing approach is proportional to the offered advantages directly. Also, it allows the users to store the data privately as per the requirement. Various methods for computation and strategies in cloud computing for different functioning are elaborated. Every person who accesses the internet does not use the applications of cloud properly so that the use of cloud can be efficient. This is because of the threats to the entire concept of Cloud computing and its security which creates the doubt in user's mind to use and rely upon the services being provided. Security issues may be of any kind. There are new security techniques being added to the list of different techniques already being used to reduce the risks in cloud. But still there are many more hindrances and computational problems that are and might occur today or in the coming future. The work has to be done in order to support cloud computing and understanding the challenges regarding security issues in cloud.

REFERENCES

[1] Mehul Nanda, "Hindrances in the security of Cloud Computing", IEEE- Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference, July 2016.

[2] R. Yamini, *"Power Management In Cloud Computing Using Green Algorithm*", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM-2012), March 30, 31, 2012.pp-128-133.

[3] Ashima Narang "Various *Load balancing techniques in Cloud Computing",* International journal of Computer Science and Mobile Computing , December 2014, pg 502-509

[4] .Fei Hu, Meikang Qiu, Jiayin li, Travis Grant, Draw Tylor, Seth McCaleb, Lee Butler and Richard Hamner, *"A Review on Cloud Computing:Design Challenges in Architecture and security"*journal of Computing and Information Technology-CIR 19,2011.

[5] LizheWang,Jie Tao, Marcel Kunze*"Scientific Cloud Computing:Early Definition and Experience*"The 10thIEEE International Confrrence Computing and Communications 2008.

[6] Rabi Prasad Padhy, "*Cloud Computing:Security Issues and research challenges", IJCSITS, December 2011.*

[7] B. R. Kandukuri, R. Paturi V, A. Rakshit, "*Cloud Security Issues*", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[8] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "*On technical Security Issues in Cloud Computing,*" Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[9] Monjur Ahmed " *Cloud computing and security issues in the cloud*", International journal of Network Security and its Applications, Vol 6, No 1, 2014

[10] Joint, A baker, E, and Eccles, E. "*Hey, you, get off of that cloud?* "Computer law and security Review, 25, 270-274, 2009.03.001

[11] King, H J and Raja " *protecting the privacy and security of sensitive customer data in the cloud*.", 308-319, Computer Law and security reviews 28, 2012.

[12] Ryan, P., Falvey, S. "*Trust in the clouds*", Computer Law and Security Reviews, 28, 513-521, 2012.

[13] Abbadi, I.M. and Martin, A., " *Trust in the Cloud*", Information security technical report, 16, 108-114, 2011.

[14] Dou, W, Chen, Q. and Chen J., " *A confidence-based filtering methods for DDoS attack defense in Cloud environment*" Future Generation Computer System, 29, 1838-1850, 2013.

[15] Rashmi, sahoo, G. and Mehfuz, S. *" Security software as a service model on Cloud Computing: issues and Solutions.* ", International Journal on Cloud Computing: Services and Architecture, 2013.