International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 3, May-June-2018, ISSN (Online): 2395-566X

Security Analysis and Implementation of Private Cloud Infrastructure using Cloud Stack

Jitendra singh
Shobhit university modipuram
Meerut, India
jitummmec@yahoo.com

***Abstract*- In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Big companies like Amazon, Google, Microsoft etc., expand their market by adopting Cloud Computing systems which enhance their services provided to a large number of users. However, security and privacy issues present a strong barrier for users to adapt into the Cloud. This research investigates the security features and issues of implementation of cloud platforms using Cloud Stack. The goal was to identify security weakness in terms of Authentication and Identity Management (IAM), and Data Management. Base on the findings, specific recommendations on security standards and management models have been proffered in order to address these problems. These Recommendations if implemented, will lead to trust in cloud computing systems, which in turn would encourage more companies to adopt cloud computing, as a means of providing better IT services.**

***Keyword*- Cloud Computing, Security & Cloud Stack**

I. INTRODUCTION

The term Cloud computing refers to the delivery of computing as a service rather than a product. i.e. providing resources, software, and information to computers and other devices as service over a network (typically the Internet) as shown in figure 1 below. Cloud computing provides services without requiring users to know the location and details of its operation [1]. Furthermore, it is a design concept which tries to separate the application from the operating system on which the hardware runs.

Due to its high scalable nature, it can provide infinite computing resources on demand, which remove lots of burden on cloud service providers when it comes to hardware provisioning. Since an up-front commitment can be eliminated, smaller cloud providers are able to provide services to companies and can also increase their hardware resources only when there is high demand.

During usage of cloud services, users are charged based on short-term basis. For instance a user can be charged for storage service on a daily base. Because of the scalability of Cloud in providing services, users can benefit from different services (e.g. Data as a Service (DaaS), Software as a Service (SaaS) or Platform as a Service (PaaS). Therefore, one can say that Cloud Computing has evolved at an incredible pace.

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the Information Technology (IT) industry. Big companies like Amazon, Google, Windows Azure, Open Stack, Cloud Stack has expanded their market by adopting Cloud Computing which has enabled them to provide for large number of users.

However, security and privacy issues present a strong barrier for users to adapt to this new form of IT. According to an International Data Cooperation (IDC) survey in August 2008, security was regarded as the top challenge in cloud computing [3]. Security is one of the top concerns, says users of cloud computing who fear that their business information and critical IT resources in the Cloud are vulnerable to attacks.

Furthermore, cloud computing became a hot topic at the RSA security conference in San Francisco in April 2009, where Cisco CEO Chambers said that Cloud computing was inevitable, but that it would shake up the way that networks are secured[4].

Most cloud security problems arise because of lack of control, lack of trust mechanisms, multi tenancy etc. These problems exist mainly in third party management models and also self-managed cloud platforms. Security is very difficult to implement in cloud computing because of the different forms of attacks in both the application side and in the hardware components. In fact, some attacks with catastrophic effects only need one security flaw.

When it comes to privacy, its concept varies widely among countries, cultures, and jurisdictions. Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data. But

in the end the general idea about privacy lies in how organizations account for user's data, as well as the transparency to an organization's practice around personal information.In this research, an investigation has been made on the security features of cloud platforms using Cloud Stack as a case study.

The goal of this thesis was to identify security weakness related to Authentication and Identity Management (IAM), and Data Management. Base on the findings, different recommendations have been provided on how to address these problems. These Recommendations if implemented, will lead to trust in cloud computing systems which in turn would encourage companies to adopt cloud computing

II.CLOUD INFRASTRUCTURE OVERVIEW

Resources within the cloud are managed as follows:

- **Regions:** A collection of one or more geographically proximate zones managed by one or more management servers.
- **Zones:** Typically, a zone is equivalent to a single data enter. A zone consists of one or more pods and secondary storage.
- **Pods:** A pod is usually a rack, or row of racks that includes a layer-2 switch and one or more clusters.
- Clusters: A cluster consists of one or more homogenous hosts and primary storage.
- **Host:** A single compute node within a cluster; often a hypervisor.
- **Primary Storage:** A storage resource typically provided to a single cluster for the actual running of instance disk images. (Zone-wide primary storage is an option, though not typically used.)
- **Secondary Storage:** A zone-wide resource which stores disk templates, ISO images, and snapshots.

III.CLOUDSTACK TERMINOLOGY

1. about Regions

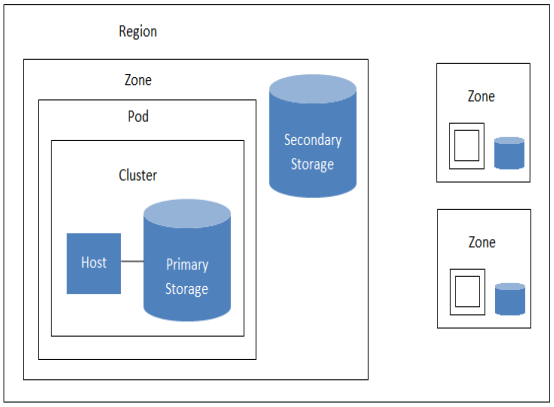
To increase reliability of the cloud, you can optionally group resources into multiple geographic regions. A region is the largest available organizational unit within a Cloud Stack deployment. A region is made up of several availability zones, where each zone is roughly equivalent to a datacenter.

Each region is controlled by its own cluster of Management Servers, running in one of the zones. The zones in a region are typically located in close geographical proximity. Regions are a useful technique for providing fault tolerance and disaster recovery. [71][72]

By grouping zones into regions, the cloud can achieve higher availability and scalability. User accounts can span regions, so that users can deploy VMs in multiple, widely-dispersed regions. Even if one of the regions becomes unavailable, the services are still available to the end-user through VMs deployed in another region. And by grouping communities of zones under their own nearby Management Servers, the latency of communications within the cloud is reduced compared to managing widely-dispersed zones from a single central Management Server.

Usage records can also be consolidated and tracked at the region level, creating reports or invoices for each geographic region. [72]

Fig. 1 A region with multiple zones



Regions are visible to the end user. When a user starts a guest VM on a particular Cloud Stack Management Server, the user is implicitly selecting that region their guest. Users might also be required to copy their private templates to additional regions to enable creation of guest VMs using their templates in those regions.[72]

IV.CONCLUSION

Both the theoretical and practical findings have clearly shown that there is great need to improve the security and privacy situation in cloud computing . Since cloud computing is relatively new, it is necessary to undertake more studies of security issues in cloud computing. This will improve the current security status of the cloud and as a result more people will find it necessary to adopt and become users of cloud services,thereby creating a steady economic growth for both the service providers and users.

REFERENCES

[1]. J. Mulerikkal, P. Strazdins, B. Thekkanath, "High Performance Cloud Computing Using an Efficient Data Service", proceedings of IEEE Asia Pacific Cloud Computing Congress, November 2012.
[2]. "State of the Cloud Report", RightScale Ltd Whitepaper, 2014.
[3]. A. Paradowski, L Liu, B. Yuan, "Benchmarking the Performance of OpenStack and

CloudStack", Proceedings of IEEE 17th International Symposium on Object/Component-Oriented Real-Time Distributed Computing, 2014.

[4]. OpenStack Documentation, [online] Available: http://docs.openstack.org/juno/install-guide/install/apt/content/ch_overview.html.

[5]. J. P. Martin, C. Krishna, M. J. Hareesh, S. Anish Babu, S. Cherian, Y. Sastri, "Learning Environment as a Service (LEaaS): Cloud", IEEE Fourth International Conference on Advances in Computing and Communications Kochi, 2014.

[6]. S. Anish Babu, M. J. Hareesh, J. P. Martin, S. Cherian, Y Sastri, "System Performance evaluation of Para virtualization Container virtualization and Full virtualization using Xen Open VZ and XenServer", IEEE Fourth International Conference on Advances in Computing and Communications Kochi, 2014.

[7]. Virtual Machine Disappearing Cloudstack-users Mailing List Archives (Webpage), [online] Available: http://goo.gl/oBtzdf.

[8]. Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions Point of View White Paper for U.S. Public Sector

[9]. Vijay Sarathy, Purnendu Narayan and Rao Mikkilineni "Next generation Cloud Computing Architecture Enabling real-time dynamism for shared distributed physical infrastructure "

[10]. N. Prasad, D.Chaitanya Kumar, A .Srinivas Rao "Architecture of Cloud Computing"