Security in Inter-Cloud Communication

Sudhir Dhage and Akassh A Mishra
Dept of Computer Engineering
Sardar Patel Institute of Technology, Andheri
Mumbai, India
e-mail: sudhirdhage@gmail.com, akassh.mishra@gmail.com

***Abstract*—Cloud Computing is an upcoming technology which has various advantages over the current existing system. Since, it's a new technology there are various areas which needs to be improved such as security issues, virtualization, Intrusion detection, etc... The Present paper proposes an Application which makes a difficult task of Inter Cloud Communication secure and automated. The cloud which is implemented by various companies has different architecture and they contain tremendous amount of data. If two companies which have different cloud architecture want to share resources and data the application which the present paper proposes will help those companies to share their data as well as their resources keeping in Mind the security issues for data and resources. The Main idea for this implementation will be based on XML which can help in exchanging the data between the clouds and for handling the security issues the protocol SSL will be used. The future scope of this technology is tremendous, since one cloud can use the resources of other cloud and this could help some weak cloud architectures to process a very strong request in terms of resources by taking resources for some other external clouds.**

***Index Terms*—PubSub Hubbub protocol; Diffie-Hellman; public cloud; private cloud; infrastructure; SSL.**

I. INTRODUCTION

The Inter cloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based. Inter cloud will have the dimensions of one machine comprising all servers and attendant cloud books on the planet.

The Inter cloud scenario is based on the key concept that each single cloud does not have infinite physical resources. If a cloud saturates the computational and storage resources of its virtualization infrastructure, it could not be able to satisfy further requests for service allocations sent from its clients. The Inter cloud scenario aims to address such situation, and in theory, each cloud can use the computational and storage resources of the virtualization infrastructures of other clouds. Such form of pay-for-use may introduce new business opportunities among cloud providers if they manage to go beyond theoretical framework. Nevertheless, the Inter cloud raises many more challenges than solutions concerning cloud federation, security, interoperability, Quality of Service, vendor's lock-ins, trust, legal issues, monitoring and billing.

II. RELATED WORK

Cloud Security Alliance is playing a role is securing the cloud. Security, which is one of the major concerns about cloud computing that, is delaying its adoption. One of the biggest security concerns about cloud computing is that when you move your information into the cloud, you lose control of it. The cloud gives you access to the data, but you have no way of ensuring no one else has access to the data. Therefore, Cloud Security Alliance provides "Guidance for Identity & Access Management".

III. PROBLEMS IN INTER-CLOUD COMMUNICATION

A. Security

The relative security of cloud computing services is a contentious issue which may be delaying its adoption. Issues barring the adoption of cloud computing is due in large part to the private and public sectors unease surrounding the external management of security based services. It is the very nature of cloud computing based services, private or public, that promote external management of provided services. This delivers great incentive amongst cloud computing service providers in producing a priority in building and maintaining strong management of secure services. Organizations have been formed in order to provide standards for a better future in cloud computing services. One organization in particular, the Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing.

B. Open standards

Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium is working to develop consensus on early cloud computing standards and practices.

IV. Solution to Problems in Inter-Cloud Communication

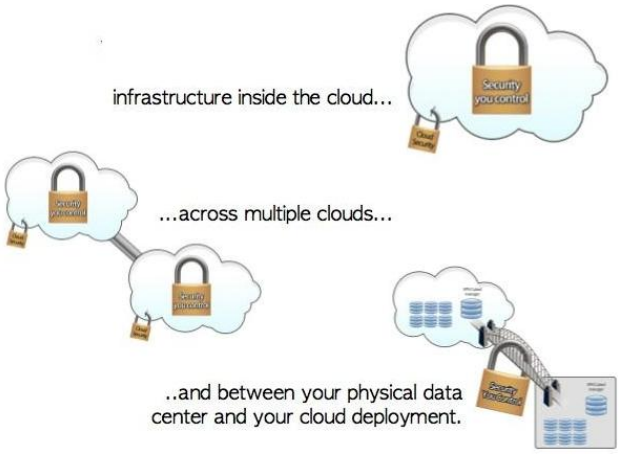

Fig. 1. Security Perimeter for Cloud Computing

As shown in figure 1 we can see the various security perimeters which describe where the security needs to be implemented.

A. Security in Infra structure inside the cloud

The Main issue with cloud computing is that when we move our information into the cloud, we lose control over it. The cloud gives us access to the data, but we have no way of ensuring no one else has access to the data. How can we protect ourselves from a security breach somewhere else in the cloud, Is the main question that needs to be tackled?

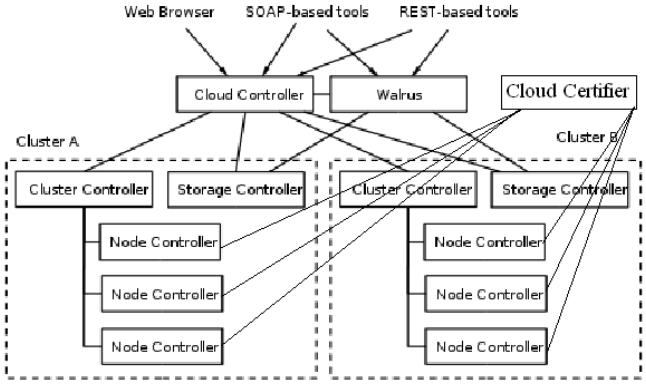

Figure 2 Secure Cloud Architecture

SSL protocol is the basis of all that protocol that implements security. For handling security Cloud will contain one more component known as "Cloud Certifier" is installed. Cloud Certifiers assigns and contains all the public key of node controller. Whenever a request is allocated to a particular node corresponding public key is sent to user as an http response or can also be sent using pub sub hub bub protocol which can make this process instantaneous. Cloud Certifier is responsible for assigning maintaining reviewing node controller key within the cloud infrastructure so that there is no external intrusion that takes place in cloud.

B. Security across multiple clouds

In this Security aspect also cloud certifier plays an important role. Cloud Certifier not only manages node controllers but also maintains a unique key for the whole cloud architecture which helps in inter-cloud communication. Unique key will only come in picture when a Particular cloud approaches another cloud for resources or data sharing. This unique key will be exchanges between the clouds using "*Diffie-Hellman Algorithm*". After that what ever request and response any cloud wants to send to other cloud is secure.

C. Security in Data centers and clouds deployment

This security aspect is the makes use of above two algorithms for data interaction. When the data is sent from data centers to cloud it is encrypted with cloud's unique key. No role is played by public and private key of Node controller in this aspect of security.

1) *Open Standards:* Open standard issues can also be solved to some extend by use of XML as the backbone of request response. A request about the resource can be standardized in a particular format which could help in communication irrespective of different standard and architecture and correspondingly a particular response will be generated which will also be in XML format. Open Standards issue can be handled by standardizing request response process.

V. CONCLUSION

The present paper proposes a solution to overcome the problem of security in inter-cloud communication by use of basic security protocol SSL and pubsubhubbub protocol for instantaneous sending of request. It also proposes to uses Diffie-Hellman Key exchange algorithm which helps in transferring symmetric key across the cloud. The present paper also introduces a change in architecture of cloud but introducing a new component called "*Cloud Certifier*", which will maintain the private and public keys for all the node controllers and also contains a Unique Cloud key which is used in Diffie-Hellman algorithm.

The problem of Open Standards is solved to some extend by using a universal structured data formatter, XML which can be used for sending request and response across the different standards and architecture. In short standardizing a request and response process leads to solution of open standards issue.

References

[1]. "Eucalyptus Completes Amazon Web Services Specs with Latest Release". Ostatic.com.

[2]. "Security of virtualization, cloud computing divides IT and security pros". Networkworld.com.

[3]. "Are security issues delaying adoption of cloud computing?" Networkworld.com.

[4]. "Cloud Security Alliance Official web page". Cloudsecurityalliance.org

[5]. "Intercloud is a global cloud of clouds". Samj.net. 2009

[6]. Scheier, Robert L.,"What to do if your cloud provider disappears | Cloud Computing". InfoWorld.

[7]. http://www.infoq.com/resource/news/2008/10/cloud-vpn

[8]. http://code.google.com/p/pubsubhubbub/

[9]. Diffie–Hellman Key Exchange – A Non-Mathematician's Explanation by Keith Palmgren