ISSN: 2393-8528

IJICSE Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 5; September-October-2017; Page No. 10-12

CERTIFICATE AUTHORITY ENHANCED CLOUD SECURITY

[1]Pawan Kumar Mishra, [2]Manoj Kumar

[1]Research scholar, Shri Venkateshwara University, Gajraula, Amaroha, UP

[2]Associate Professor, Dept. of CS, Shri Venkateshwara University, Gajraula, Amaroha, UP

ABSTRACT

In this era of information sharing "cloud computing" plays a vital role for storing and accessing data over internet via secured as well as unsecured computer network. Due to ease of access of clouds, information security is becoming an issue for those who are transmitting and receiving sensitive information through cloud. Here we are trying to solve this problem using some cryptographic mechanism. In this paper we will use the concept of registration authority and certificate authority to identify that the communicating entity is supposed to do so or not. Certificate authority is a trusted third party who is responsible to provide certificate and access level for nodes which are trying to communicate with cloud. First of all, an incoming node must have to communicate with certificate authority with their credentials for acquiring certificate for communicating with cloud. Those credentials are checked and verified by certificate authority and then a certificate is granted to that node. Once certificate is granted, that certificate is shared to cloud server also for matching purpose, when the corresponding will communicate with cloud server. If everything will happen in right manner then that node can access cloud data according to their access level.

Keywords: Cloud Computing, Certificates, Certificate Authority (CA), Registration Authority (RA)

INTRODUCTION

Cloud computing, basically, is an Internet based delivery model of services categorized as Infrastructure-as-a-Services (IaaS), Platform-as-a-Service (PaaS) as well as Software-as-a-Service (SaaS). It is becoming a trendy option for renting virtual storage and virtual machines as infrastructure services; for developing and deploying the applications on the cloud infrastructure; and for renting a complete operating environment. It provides an easy access to the multiple end users i.e. users can access the services from wherever they want to without concerning about the storage, management, and cost and so on. IaaS is a way of delivering virtual machines, virtual infrastructure, virtual storage and other hardware assets as resources as an on-demand service that clients can provision. PaaS is a way of delivering virtual machines, operating systems, services, applications, control structures and development frameworks. The client is allowed to deploy its applications on the infrastructure of the cloud or use applications that were programmed using PaaS service provider's compatible languages and tools. SaaS is a cloud service with complete operating environment including the cloud management as well as the user interface. By the use of a thin client interface, the application is made available to the client (usually though the browser).

Following are the essential characteristics of Cloud Computing:

(i) On-demand self-service: any user may facilitate computer resources without the permission of service provider authority of cloud.

(ii) Broad network access: Access to resources in the cloud is available over the network using standard methods in a manner that provides platform independent access to clients of all types. This includes a mixture of heterogeneous operating systems, and thick and thin platforms

Corresponding author: Pawan Kumar Mishra

such as laptops, mobile phones, and Personal Digital Assistant (PDA).

(iii) Resource pooling: A cloud service provider creates resources that are pooled together in a system that supports multi-tenant usage.

(iv) Rapid elasticity: Resources can be rapidly and elastically provisioned. The system can add resources by either scaling n systems (more powerful computers) or scaling out systems (more computers of the same king), and scaling can be automatic or manual.

(v) Measured service: The use of cloud system resources is measured, audited, and reported to the customer based on a metered system. A client can be charged based on a known metric such as amount of storage used, number of transactions, network I/O or bandwidth, amount of processing power used, and so forth.

Cloud security with CA:

Cloud security is a term used to represent a broad set of policies, controls and technologies used to protect data, applications, and the associated infrastructure of cloud computing. The concept of certificate authority will be more suitable to provide access of cloud only for those which are non fictitious and supposed to access the cloud resources. Following are the algorithms involved with certificate authority:

1. Issuance of certificate:

When a new node N wants a certificate to access cloud server, it should take the following steps:

(i) N communicates with RA. RA verifies credential of N and contacts CA.

(ii) Registration authority issues CN (Certificate of N) for N and sent it to CA and N.

(iii) N sends CN to R_{CA}(repository in CA, where CA, is the Certificate Authority), and requests Ci (set of certificates) from R_{CA}.

(iv) R_w issues Ci, and sent it to N and Cj is sent toR_{CS}(Repository of Cloud Server).

2. Communication with cloud server:

When a new node N wants to communicate with cloud server after certificate issuance, it will take the following steps:

(i) N transmits Ci to R_{CS}(Repository of Cloud Server).

(ii) R_{CS}verifies Ci as:

IF Ci = Cj

THEN

N is authorized node.

Now N is allowed to access cloud resources.

ELSE

N is an unauthorized node.

Performance analysis of Certificate Authority using NS2:

We try to show the Certificate Authority performance with the help of Network Simulator NS2. In a graph two coordinate x and y Certificate Authority performance graph to show with 100 nodes. In performance graph on x coordinate show the number of nodes which is used and on y coordinate show the Certificate Authority performance with node. In this graph, Certificate Authority performance is very high with starting number of nodes, after increasing the number of nodes the performance is slowly decrease and after last graph find a straight line means performance of Certificate Authority is going to compromised because Certificate Authority has store the entity of all nodes. An entity has maximum identity information, Photo ID, and other information are in certificate then if this types of information has keep to all nodes in Certificate Authority, after the computation and key management become complex Certificate Authority. If the number of node are more at Certificate Authority, this will be the main reason of poor performance and compromised security of Certificate Authority.

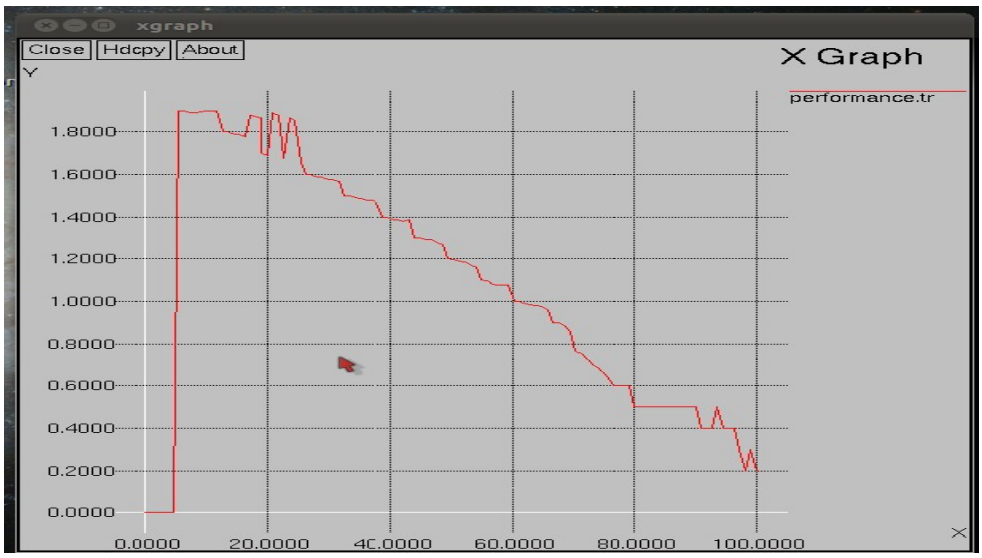

Figure 1: Performance graph of Certificate Authority in NS2

Conclusion:

In Cloud computing, due to unreliable wireless media host mobility and different infrastructure, providing secure communication is a challenge. To use the concept of registration authority and Certificate Authority, we will get high security. Certificate Authority are not work well, because in mobile Ad-hoc network the computation load and complexity for key management is strongly subject to restriction of the node's available resources and the dynamic nature of network topology and Ad-hoc network have a big infrastructure. So on Certificate Authority can create a problem of computation, load and complexity due to big dynamic infrastructure for seeing this reason we uses distributed Certificate Authority concept in Cloud Network.

Distributed Certificate Authority work properly small and simple Cloud Network infrastructure, we get high performance in comparison to ad-hoc network. In this we define three architectures model of Cloud. Every model has different characteristics with increasing number of nodes and clusters. Using of clustering it reduces the storage requirements, communication overhead, for this increases the efficiency of certificate management, and if any cluster or Certificate authority fail then the load of fail certificates is handover to other nearest Certificate Authority.

References:

1. Y.Dong, Victor O.K. Li ,Lucas C.K. Hui,S.M.Yiu "Dynamic Distributed Certificate Authority Services for Mobile Ad Hoc Networks" of IEEE Communication society in the WCNC 2007 proceedings
2. Wenbi Rao,Shouwn Xie" Merging Clustering Scheme in Distributed Certificate Authority for Ad Hoc Network" ICWMMN 2006 pcoceeding.
3. Bing Wu, Jie Wu, Eduardo B. Fernandez, Spyros Magliveras " Secure & Efficient Key Management in MANET" on international conference of IEEE in 2005.
4. Shuxin Liu, Jianhua Peng,Caixia Lua "Analysis of Cloud Network Security Based On Node Function" on Seventh International Conference on Computational Intelligence and Security 2011.
5. Amir Esmailpour and Nidal Nasser, "Topological-Based Architecture for Cloud Networks" on IEEE Wireless Communications February 2011.
6. Rafael De Tommaso do Valle, Dedora Christina Muchaluat-Saade "Mesh Admin: an Integrated Platform For Cloud Network Management" on Network Operations and Management Symposium of IEEE 2012.