ISSN: 2393-8528

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Journal Index In ICI World of Journals – ICV 2016 – 69.57

Volume 4 Issue 6; November-December 2017; Page No. 41-45

Efficiency Enhancement of Cloud Security using Certificate Authority

[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

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. It is being forecasted that more and more users will rent computing as a service, moving the processing power and storage to centralized infrastructures rather than located in client hardware. This is already enabling start-ups and other companies to start web services without having to invest upfront in dedicated infrastructure. However, a major barrier for cloud adoption is real and perceived lack of security. Digital certificates are an essential part of the foundation that enables secure digital communications, providing secure access to data, applications and cloud infrastructures. Digital certificates are an established, standards-based method to enhance trust over vulnerable networks. They are the digital equivalent of a driver's license or any other form of identity issued by a trusted third party in the physical world. In this paper we have discussed the cloud security by certificate authority technique.

1. Introduction

Cloud computing is rapidly emerging as a new paradigm for delivering computing as a utility. It allows leasing of IT capabilities whether they are infrastructure, platform, or software applications as services on subscription oriented services in a pay-as-you-go model. —Cloud computing is the next natural step in the evolution of on-demand information technology services and products. To a large extent, cloud computing will be based on virtualized resources. Cloud Computing is here to stay, as it is proposed to transform the way IT is deployed and managed, promising reduced implementation, maintenance costs and complexity, while accelerating innovation, providing faster time to market, and providing the ability to scale high-performance applications and infrastructures on demand. Even though cloud offers a multitude of benefits to individuals and organizations, cloud is under high risk of attack.

For more than a decade, commercial Certificate Authorities (CAs) have acted as trusted third parties, protecting the exchange of private information over the public Internet. But in recent months, there has been a cloud of controversy hanging over the head of commercial certificate authorities. A string of highly publicized CA security breaches of 2011 sparked a debate as to whether SSL certificate technology and the entire CA industry that distributes it are fundamentally broken. Fortunately, the answer is categorically and unequivocally "no." Digital certificates and PKI still provides excellent protection against evolving cyber security threats. With the right tools and processes, CAs are fully capable of providing the greatest assurance possible that their certificates – and the websites that use the certificates – are genuine and safe for online business.

2. Certificate Authority

The certificate authority, or certification authority, is the public key infrastructure (PKI) entity that digitally signs certificates and certificate revocation lists (CRLs). The CA generates some certificate information but is primarily responsible for collecting information from authorized sources and entering that information into a certificate before signing.

The CA digitally signs and issues a subscriber's certificate when authorized by the appropriate trusted person or process, called a registration authority (RA). The RA ensures that only valid and appropriate information is included in the certificate and maintains evidence that due diligence was exercised in confirming the

*Corresponding author: Pawan Kumar Mishra

information to the required assurance level of the PKI.

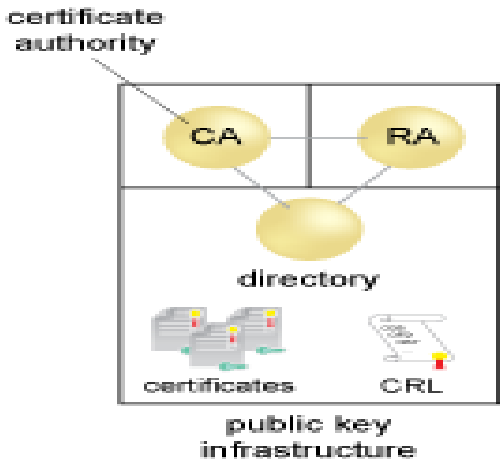

Fig. 1: An Example of a Certificate Authority as part of a Public Key Infrastructure (PKI).

Figure 1 shows a certificate authority issuing certificates and CRLs as part of a PKI. The PKI must be operated in accordance with a certificate policy and certificate practice statement (CPS) that establishes the security assurance level of the issued certificates. Periodic audits are performed to confirm that the PKI is being operated in accordance with their CPS.

3. Cloud Service Models

Cloud can be thought of as a boundary from where a consumer's management and responsibilities ends and the activities of cloud service provider starts. With the development of Cloud Computing, different vendors offer clouds that have different services correlated with them. The collection of services offered by Cloud service providers is universally known as service model. There are basically three service types:

a) Infrastructure-as-a-Service

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. Using this service model, Clients are responsible for the management of the data, applications, operating systems, interactions with the system and runtime whereas the service provider have the responsibility of virtualization, networking, servers and storage. Some examples of IaaS service providers are as follows:

- Amazon Elastic Compute Cloud (EC2)
- Eucalyptus
- GoGrid
- RackSpace Cloud

b) Platform-as-a-Service

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. The client manages the data and application that it is deploying whereas the service provider manages everything else like the operating systems and the cloud infrastructure. Following are some examples of PaaS service providers:

- Force.com
- Google AppEngine
- Windows Azure Platform
- Flexiscale

c) Software-as-a-Service

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). It is a cloud service where customers are able to access software applications over the Internet. The customer has the responsibility of entering and managing its data whereas the vendor manages everything else down to infrastructure. Examples of SaaS cloud service providers can include:

- Google Apps
- Salesforce.com
- Microsoft office 365
- Apprenda

4. Cloud Security

Cloud Security refers to a broad set of policies, technologies and controls deployed to protect data, applications and the associated infrastructure of Cloud Computing i.e. Cloud Security focuses on security issues from Cloud Computing system, such as privacy protection, data encryption and resources availability under security threat. Undoubtedly, keeping your data and running your applications on someone else's hard disk using someone else's infrastructure appears daunting to many. Security may, in fact, be the single most important area of Cloud

Computing that you need to plan for. Some common security concerns around Cloud Computing can be divided in four different categories [20]:

(i) Cloud infrastructure, platform and hosted code: This comprises concerns related to possible virtualization, storage and networking vulnerabilities.

(ii) Data: This category comprises the concerns around data integrity, data lock in, data provenance, and data confidentiality and user privacy specific concerns.

(iii) Access: This comprises the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication, and user identity management.

(iv) Compliance: Because of its size and disruptive influence, the cloud is attracting attention from regulatory agencies, especially around security audit, data location; operation trace-ability and compliance concerns.

Security issues in cloud have played a major role in slowing down its acceptance. In two surveys carried out by International data Corporation (IDC) in 2008 and 2009 respectively, security came top on the list

5. Network Simulator

Network simulator ns2 is an event-driven network simulator used for networking research. It is a widely used tool for simulating internetwork topologies to test and evaluate various networking protocols. There is a substantial support and flexibility in ns2 to simulate various traffic generation patterns, routing and multicast protocols. In order to study different networking issues like protocol interaction, congestion control, effect of network dynamics, scalability etc. it is necessary to simulate various scenarios that include different topology sizes, density distribution, traffic generation, membership distribution, real-time variance of membership, network dynamics etc. The ns2 scenario generator can be used to create different random scenarios for simulation. In ns2, characteristics of physical media of communication like delay, bandwidth, error rate, antennas and wireless physical interface parameters etc. can be defined. This helps in making the simulation studies as close to realistic scenarios as possible. NS2 provides the flexibility to add and experiment new protocols or ideas. Recently, much support has been added for simulating wireless networks and interconnecting wired and wireless networks. Trace support in ns2 may be used to trace packets for wireless and wired scenarios. NS2 currently supports two mobile networking models. The basic wireless model was ported from CMU/Monarch group. It essentially consists of mobile nodes, which are movable and are able to transmit and receive on channels, with additional supporting features that allow simulations of multi-hop Ad-Hoc networks and wireless LANs. Four Ad-Hoc routing protocols that are currently supported as Destination Sequence Distance Vector (DSDV), ad-hoc On-Demand distance vector (AODV), Optimize link state routing (OLSR).

6. Performance graph of Certificate Authority in NS2

We are trying 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 node; after increasing the number of nodes the performance is slowly decrease. At the end of graph, it becomes a straight line i.e. the performance and security of CA is going to be compromised, because CA has the attribute of all node such as identity information. If all these information for maximum node are kept together at CA then the computation of key management will become more complex for certificate authority. If the number of node more in Certificate Authority, this is the main reason of poor performance and compromised security of Certificate Authority.

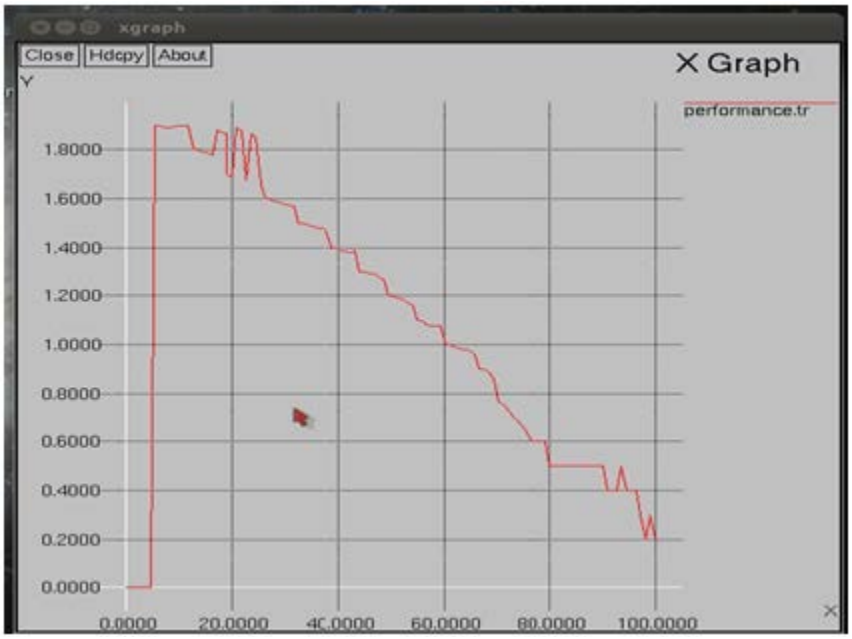

Fig. 2: Performance Graph of Certificate Authority in NS2

7. Conclusion

In Ad-hoc network due to unreliable wireless media host mobility and different infrastructure, providing secure communication is a challenge in Cloud Network, the concept of Certificate Authority, using these idea 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. Hence, Certificate Authority can create a problem of computation, load and complexity due to big dynamic infrastructure. On seeing this reason, we will use distributed Certificate Authority concept in Cloud Network.

Distributed Certificate Authority work properly for small and simple Cloud Network infrastructure, we get high performance in comparison to ad-hoc network. In this we define three architectural model of Cloud. Every model has different characteristics with increasing number of nodes and clusters. Use of clustering reduces the storage requirements, communication overhead, for this increases the efficiency of certificate management, and if any cluster or Certificate authority fails, then the load of failed certificates will be handed over 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. Indre Egners,Ulrike Meyer "Cloud Network Security: State of Affairs"on
5. Shuxin Liu, Jianhua Peng,Caixia Lua"Analysis of Cloud Network Securty Based On Node Function "on Seventh International Conference on Computational Intelligence and Security 2011.
6. Amir Esmailpour and Nidal Nasser, "Topological-Based Architecture for Cloud Networks" on IEEE Wireless Communications February 2011. [7] 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.

7. Md. Forhad Rabbi, Md.Taufiqur Rahman, Md.Afser Uddin, G.m. Abdullah Salehin" An Efficient Cloud Network: A New Architecture".

8. Sok-Hyong Kim and Young-joo Suh" Local Channel Information Assisted Channel Assignment for Multi-Channel Cloud Networks" on international conference of IEEE 2008.

9. N.Ben salem,J.-p.Hubaux,"Securing Cloud Networks,"wireless communication IEEE 2006