International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue (6) NCRTCST-2013, ISSN 2249–071X

National Conference on Recent Trends in Computer Science and Technology (NCRTCST)-2013

Prior Authentication Approach to Enhance Security in CloudComputing

P. M. Jyosthna
Assistant Professor, CSE Department,
B.V.R.I.T Narsapur, Hyderabad, AP, India
Email: jyosthna.p@bvrit.ac.in, Phone: +91 9866875673

J. Suman
Assistant Professor, CSE Department,
B.V.R.I.T Narsapur, Hyderabad, AP, India
Email: suman.j@bvrit.ac.in, Phone: +91 9966667244

***Abstract* – Now a days Cloud computing is an upcoming Technology. Cloud allows users to access and share resources such as software, platform and infrastructure by means of virtualization. Even though it offers many advantages, several large organizations like banks, financial organizations and few government agencies are still considering it to be unsafe place. This is because; security and privacy issues are strong obstacles for users to adapt into Cloud environment.**

To gain total acceptance from all potential users, cloud computing require some standardization in the security environment and third-party certification to ensure that these standards are met. In this paper we propose a secure two way authentication procedure for clients and service providers using TCA (Trusted Certification Authority). This can be done before service level agreement (SLA). Our theoretical analysis gives low burden on service providers and requires a reasonably low verification effort at the client side, and protect from repudiation attack.

***Keywords* – Cloud Computing, Security, Service Level, Agreement.**

I. Introduction

Cloud Computing has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, cost effective, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1].

There are different kinds of cloud deployment models available. They are Private cloud, Public Cloud and Hybrid Cloud.

Private Cloud:

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization’s internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloudvendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.[2]

Public Cloud:

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.[3]

Hybrid Cloud:

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, Provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows s interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.[4]

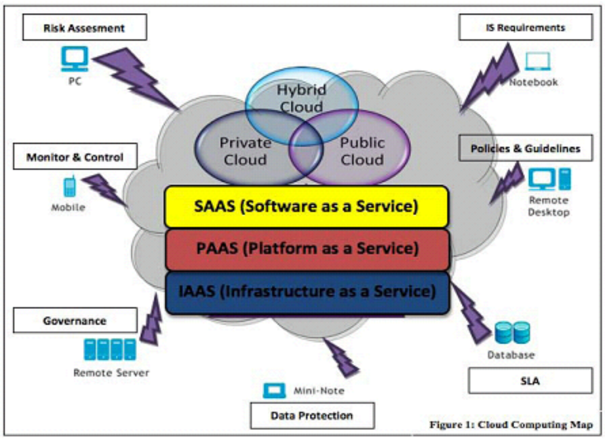

Fig.1. Cloud deployment model [3]

Cloud Computing provides majorly the following services like SAAS, PAAS and IAAS.

Software-as-a-Service

Software-as-a-Service (SaaS) is a model of service delivery whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud consumer does not Manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

Platform-as-a-Service

Platform-as-a-Service (PaaS) is a model of service delivery whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud consumer has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud consumer.

Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) is a model of service delivery whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud consumer generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud consumer.

Though they are many advantages in Cloud Computing, it also brings new and challenging security threats towards user's outsourced data. In cloud computing, clients do not know where the data is actually stored. The data as well as processing is somewhere on servers. So, service providers should give assurance to clients about data availability and data Integrity. In cloud computing SLA is the only legal agreement between the service provider and client to trust each other.

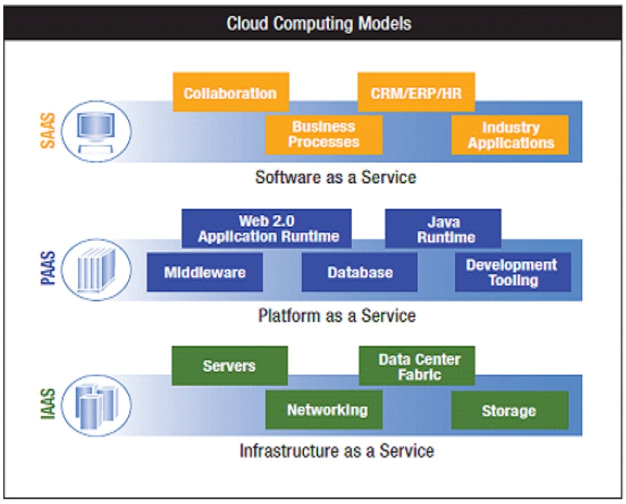

Fig.2. Cloud computing service delivery models [5]

II. The Service Level Agreement

A document which defines the relationship between service provider and client is called a service level agreement. Obviously SLA is very important document for both the parties. Generally SLA document covers the following points [6].

1. Privileged user access.

Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information about the people who manage our data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

2. Regulatory compliance.

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are signaling that customers can only use them for the most trivial functions.

3. Data location

When we use the cloud, we probably won't know exactly where our data is hosted. In fact, we might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4. Data segregation

Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.

5. Recovery

Even if we don't know where your data is, a cloud provider should tell us what will happen to our data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure.

6. Investigative support

Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If we cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then our safe assumption is that investigation and discovery requests will be impossible.

7. Long-term viability

Ideally, cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But must be sure about the data will remain available even after such an event.

III. PROBLEM DEFINITION

The above said points cover about confidentiality and availability but there is no much importance for authentication. Here in this paper we are proposing an authentication approach before going to Service level agreement. The idea here is if we take care about security issues at lower level it will not lead to more vulnerability at higher level. If service providers and clients are both authenticated then they can securely go for the next process. We are proposing an authentication with the help of the certificates that are generated by Trusted Certification authority (TCA).

Trusted Certification Authority:

If any user wishes to gain access to cloud services, then they have to get registered with standard certificate issued by the Trusted Certification Authority (TCA).Cloud Service Providers also take their own certificate from TCA. These certificates are created and maintained by some Trusted Certification authority (TCA). To secure these certificates they use strong public-key cryptography and digital signature. TCA can use any standard authentication service formats like X.509.

Any certificate should include the following elements

Serial number (SN): It is a unique integer value

Signature Algorithm Identifier (SI): The algorithms used by the TCA to sign the certificate

Issuer Name (CA): Name of the TCA that created and signed this certificate

Period of validity (TA): validity time period of certificate.

Use/provider name (A): the name of the user/provider to which this certificate refers.

User's/provider's public key Information (AP): The public key of the user/provider plus an identifier of the algorithm for which this key is to be used

Issuer unique identifier (CD): a unique identifier to identify Issuer uniquely

User/provider unique identifier (AI): the user/provider uniquely identify using this identifier

Signature: It contains hash code of the above fields and encrypted with TCA's private key. This field includes the signature algorithm identifier.

CA<< A>> = CA {SN, SI, CA, TA, A, AP, CD}

Where

CA << A >> = the certificate of user A certified by Certificate Authority (CA).

CA {I} = the signing of I by CA.

This certificate gives low burden on service providers and requires a reasonably low verification effort at the client side, and protect from repudiation attack.

Authentication Procedure:

Now the authentication procedure is done between client and service provider as follows.

1. Client sends a request message to the provider as "Client – Hello".
2. Provider request for the Client certificate as "Server – Hello".
3. Client sendshis certificate to the provider and request for the provider's certificate.
4. Provider's sends his certificate and Authenticated message to Client.
5. Now client send Authenticated message to provider.
6. To validate the reply Client sends signed copy of nonce.

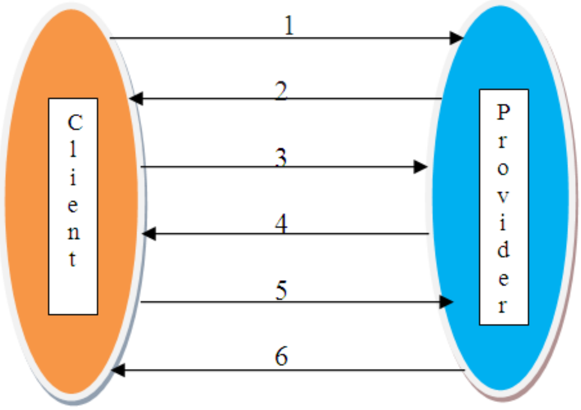

Fig.3. Authentication Procedure between client and service provider.

1: Client – Hello
2: Server – Hello
3: CA << A>>
4: CA<<P>>,
P{t_P, r_P, A, sgndata, E_{KUa} [Kpa] }
5: A {t_A, r_A, P, r_P, sgndata, E_{KUp} [Kap] }
6: P {r_A}

Where

t_A– is a timestamp which consists of an optional generation time and an expiration time. It prevents delayed delivery of messages.

r_A - The nonce can be used to detect replay attack. The nonce value must be unique within the expiration time of the message.

P/A can store the nonce until it expires and rejects any new message with the same nonce.

Sgndata - Message to be conveyed to B.

E_{KUp} [Kap] – A session key to P is encrypted with P's public key.

After completion of authentication procedure Cloud service provider will sends SLA document and they can continue their communication securely. Now the communication gives assurance about security for both the parties.

IV. Conclusion

Cloud computing offers many services dynamically over the internet. It works based on the concept of pay-per-use. Any client-server application communication starts with authentication procedure. In cloud computing, communication between client and provider starts with SLA document which is a legal agreement between them. Here in this paper we are proposing an authentication process before going to service level agreement with the help of certificates generated by TCA.

References

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd,2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

[2] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[3] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.

[4] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[5] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009.

[6] " Cloud Security Issues", 2009 IEEE International Conference on Services Computing.

Author's Profile

P. M. Jyosthna
received B.Tech. and M.Tech. Degree from JNTU Hyderabad. At present she is working as an Assistant Professor in the Department of Computer Science and Engineering at Padmasri Dr. B. V. Raju Institute of Technology, Narsapur, Medak Dt, Hyderabad. Her Research interests are in the areas of Cloud Computing and Network Security.

J. Suman
received B.Tech. Degree in Computer Science Engineering from JNTU, Hyderabad and M.Tech Degree in Computer Science Engineering from ANU Guntur. At present he is working as an Assistant Professor in the Department of Computer Science and Engineering at Padmasri Dr. B. V. Raju Institute of Technology, Narsapur, Medak Dt, Hyderabad. His Research interests are in the areas of Cloud Computing and Network Security