ISSN:0975-9646

Network Security through SSL in Cloud Computing Environment

Pankaj Patidar[1] Arpit Bhardwaj[2]
[1]Department of Computer Science Engineering, TIT, Bhopal
[2]Department of Computer Science Engineering, SDITS, Khandwa

***ABSTRACT*-Cloud Computing is a style of computing in which business provides application data and any type of IT resource as a services to client. To gain access to services of cloud computing you only need Internet access. Cloud computing is clearly one of today's most enticing technology areas due to its cost-efficiency and flexibility. But with this facilities it is not gaining as much popularity as it have to be, most of the organization are not want to deploy cloud environment. Security is one of the major issues which reduces the growth of cloud computing. In this paper we describe how the organization can deploy this computing environment without being worried about security issues.**

***KEYWORDS*-SaaS, PaaS, IaaS, Multi-tenant, Security, SSL.**

1. INTRODUCTION

Cloud Computing is a style of computing in which business processes, application, data and any type of IT resource can be provided as a service to the user. It is a construct that allows you to access applications that actually resides at a location other than your computer or other internet connected device. Cloud computing get its name as a metaphor for the internet. Typically, the internet is represented in network diagram as a cloud. (A metaphor is an imaginative way of describing something by referring to something else which is the same in a particular way. Cloud computing has become a significant technology trend, and many experts expect that cloud computing will reshape information technology (IT) processes and the IT marketplace. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

1.1 Services:

Services in cloud computing is the concept of being able to use reusable and fine grained component across a vendor's network. This is widely known as "as a service". Offering with as services as a suffix include traits like following:

1. Low barriers to entry, making them available to small businesses.
2. Large scalability.
3. Multi-tenancy, which allow resources to be shared by many users.
4. Device independence, which allows user to access the systems on different hardware.

Services of cloud computing is divided in following three categories:

1. Software as a Service.(SaaS)
2. Platform as a Service.(PaaS)
3. Infrastructure as a Service.(IaaS)

Software as a Service

Software as a Service (SaaS) is a model in which an application is hosted as a service to customers who access it via Internet. When the software is hosted off-site, the customer doesn't have to maintain it. On the other hand, it is out of customer's hands when the hosting service decides to change it. The idea is to use the software out of the box as is and do not need to make a lot of changes or require integration to other system. Cost can be an important factor in this computing environment for accessing any software, rather than pay for it once and be done with it , the more you use it ,the more you will have to pay ("pay-for-use").

SaaS provides network based access to commercially available software. Since the software is managed at a central location, customers can access their application wherever they have web access.

Platform as a Service

Platform as a Service (PaaS) is another application delivery model that provides all the resources required to build application and services completely from the Internet, without having to download or install software. PaaS services include application design, development, testing, deployment and hosting. Other services include team collaboration, web service integration, security, scalability, storage, state management and versioning. PaaS generally offered some support to help.

Infrastructure as a Service:

Infrastructure as a service is the next form of services available in cloud computing. Where SaaS, PaaS are providing applications to customers, IaaS doesn't. It simply offers the hardware so that your organization can put whatever they want onto it. Rather than purchase server s, software, racks, and having to pay for the datacenter space for them, the service provider rents those resources.

2. CHARACTERISTICS OF CLOUD COMPUTING

Following are the five essential characteristics of cloud computing:

2.1 On demand self services:

Computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com.

Broad network access:
Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.

Resource pooling:
The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services.

Rapid elasticity:
Cloud services can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service:
Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

2.2 Deployment Model:
Deployment of cloud computing can depend on the requirement and identifies as following four types which is also shown in figure.

Public cloud:
Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned to the general public on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who bills on a fine-grained utility computing basis.

Private cloud:
Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from lower up-front capital costs and less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

Community cloud:
Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the benefits of cloud computing are realized.

Hybrid cloud:
Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. It can also be defined as a multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.

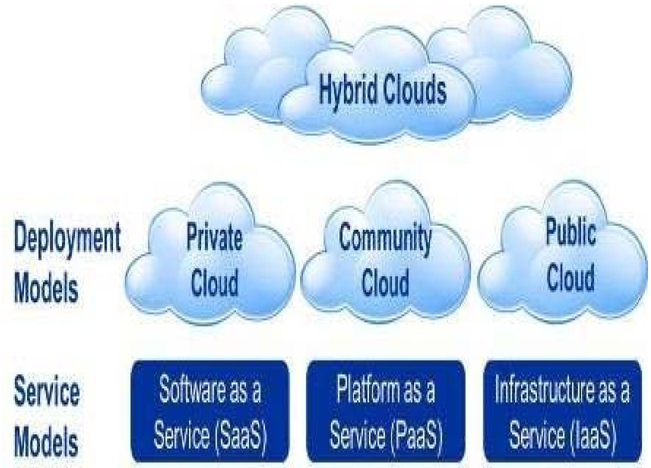
Hybrid Clouds
Deployment Models
Private Cloud
Community Cloud
Public Cloud
Service Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)

Figure 1.Service and Deployment Models of Cloud

3.CLOUD SECURITY ISSUES

In the cloud computing the client stores its data to the location about which he does not know anything, and therefore some sort of security mechanism is needed to ensure the client for not being worried about its data. A recent survey by Cloud Security Alliance (CSA) & IEEE indicates that many organization are wont to implement cloud computing but they need the security solution.
Security in the cloud computing environment can be identifies as following:

1. Security in SaaS.
2. Security in PaaS.
3. Security in HaaS.

In this paper we are representing network security; therefore we are going to have brief look on security in SaaS. Although SaaS offer great advantages to the clients but there are some security issues are related to it.
In SaaS, the client has to depend on the provider for proper security measures. The Cloud Service Provider (CSP) has to ensure the client about security. The following key security issues should be considered as integral part of SaaS implementation.

1. Data Security.
2. Network Security.
3. Data locality.
4. Authentication and Authorization.

3.1 Data Security:
Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data. In a traditional application deployment model, the important data of each organization continues to reside within the organization boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the organization data is stored outside the organization boundary, at the SaaS service provider end. Therefore the service provider has to use techniques such as encryption, strong user authentication and back up for providing data security.

3.2 Network Security:
In the cloud computing environment all the data flows through the internet that is subjected to influence by

various type of attacks. Therefore the service provider has to use some network security mechanism. In the next section of the paper we will have detail look on network security.

3.3 Data locality:

In a cloud environment, the consumers use the applications provided by the SaaS and process their business data. But the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of importance in many organizations architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the data of the consumer.

3.4 Authentication and Authorization:

Because in the application and data is hosted outside of the organization in the cloud computing environment, the cloud service provider has to use Authentication and Authorization mechanism.

Authentication is the mechanism whereby systems may securely identify their users. Authentication systems provide answers to the questions:

- Who is the user?
- Is the user really who he/she represents himself to be?

Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system. Authorization systems provide answers to the questions:

- Is user X authorized to access resource R?
- Is user X authorized to perform operation P?
- Is user X authorized to perform operation P on resource R?

4. NETWORK SECURITY

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. In cloud computing all data flow over the internet need to be secure in order to prevent in order to prevent leakage of sensitive information.This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security.

SSL (Secure Socket Layer) is a protocol developed by Netscape that enables a web browser and a web server to communicate securely; it allows the web browser to authenticate the web server.

SSL stands for Secure Sockets Layer protocol developed by Netscape and is the standard Internet protocol for secure communications. The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is httpusing a Secure Socket Layer (SSL). A secure socket layer is an encryption protocol invoked on a Web server that uses HTTPS. SSL is a type of sockets communication and resides between TCP/IP and upper layer applications, requiring no changes to the application layer. The position of SSL protocol is shown in figure:-

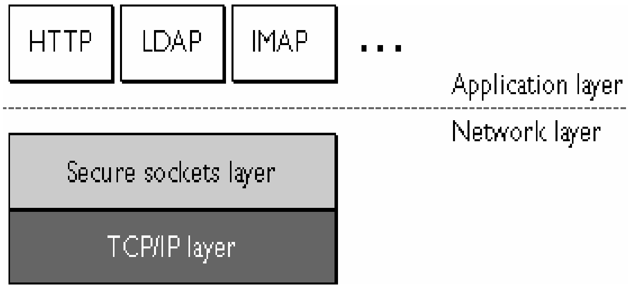

Figure2. Network Security of Cloud

The SSL protocol includes two sub-protocols: the SSL record protocol and the SSL handshake protocol.

The SSL record protocol defines the format used to transmit data.SSL handshake protocol involves using the SSL record protocol to exchange a series of messages between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection. This exchange of messages is designed to facilitate the following actions:

- Authenticate the server to the client.
- Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
- Optionally authenticate the client to the server.
- Use public-key encryption techniques to generate shared secrets.
- Establish an encrypted SSL connection.

SSL technology is used to establish a secure and encrypted communication channel between two Internet connected devices. The SSL protocol uses RSA algorithm which is a public key algorithm for encryption and decryption developed by Rivest, Shamir, and Adleman.

SSL protocol also uses concept of Certificates. Certificates are digital documents attesting to the binding of a public key to an individual or other entity. An SSL certificate contains the following information:

1. The domain for which the certificate was issued.
2. The owner of the certificate (who is the also the person/entity who has the right to use the domain).
3. The physical location of the owner.
4. The validity dates of the certificate.

SSL provides confidence in the integrity and security in network infrastructure. Clients are becoming increasingly aware of the advantages of SSL security.

CONCLUSION

In this paper we describes the security issues related to the cloud computing. We show how the organization can ensure data protection and deploy this environment. We also show the importance of encryption. For providing solution to this security issues we rely on Secure Socket Layer Protocol which is based on RSA algorithm for encryption and decryption of data which flow through internet.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone.

REFERENCES

[1] Subedari Mithila, P. Pradeep Kumar (2011) “Data Security through Confidentiality in Cloud Computing Environment” International Journal of Computer Science and Information Technologies, Vol. 2 (5), 1836-1840.

[2] M S.Bhiogade (2002) “Secure Socket Layer” Informing Science InSITE - “Where Parallels Intersect”.

[3] Amit Batra, Rajender Kumar, Arvind Kumar (2011) “A Review of Storage and Fault ToleranceApproaches Used in Cloud Computing” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011, 1971-1978.

[4] Deep Vardhan Bhatt, Stefan Schulze, Gerhard P. Hancke(2006) “Secure Internet Access to Gateway Using Secure Socket Layer” ieee transactions on instrumentation and measurement, vol. 55, no. 3.

[5] Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono (2009) “On Technical Security Issues in Cloud Computing” IEEE International Conference on Cloud Computing.

[6] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou (2009) “Ensuring Data Storage Security in Cloud Computing”.

Pankaj Patidar -Pursuing M.E. from Department of Computer Science Engineering,T.I.T, Bhopal

Arpit Bhardwaj -Working as a Senior Lecturer S.D.I.T.S Khandwa