A Review on Security Issues in Cloud Computing

R. Yogamangalam and V.S. Shankar Sriram
School of Computing, SASTRA University, Tamil Nadu, India

Corresponding Author: R. Yogamangalam, School of Computing, SASTRA University, Tamil Nadu, India

ABSTRACT

Security is protecting the resource against the threats. It is also provided by identifying the assets and maintaining the properties of the assets. The cloud is a virtualization of resources that maintains and manages itself. Security in Cloud is a different scenario. This review paper deals with various security issues in the Cloud computing.

Key words: Cloud computing, service level agreement, quality of service, SaaS, IaaS, PaaS, SECaaS, DACI

INTRODUCTION

Cloud computing is becoming one of the most important word in the industry. The term cloud computing is not a new thing and has been developed from the combination of grid computing, utility computing, distributed computing, Virtualization and Clustering. The cloud is a virtualization of resources that maintains and manages itself. Cloud computing eradicates the need for any organization to manage its resources. Cloud computing provides self-service capability to its application user. It provides a layer of abstraction between the application, operating system and hardware. This technology becomes a fertile ground for huge investment. Even though the benefits of this method is clear, security is not up to the mark. If there is no security, there is no reliability in the data that are used by various Cloud users is the need to develop proper security for the further implementation in the cloud.

CATEGORIES OF SERVICES

Cloud computing can be viewed as software as service (SaaS) or infrastructure as service (IaaS) or platform as service (PaaS). Cloud computing access resources and services from a pool of dynamic resource. The cloud computing model consists of cloud providers and cloud users. These users sent request to the cloud and the providers in turn process the request with high performance and provides the Quality of Service (QoS).

The cloud user are able to access their data from anywhere at any time. Providers also provide online services to the cloud users. Cloud computing provides deflexibility in functionality and better scalability. As the application is running over distributed environment which are owned by external organization, application security risk and privacy form an important challenge that needs to be addressed. The security issues are divided into two categories: issues faced by the cloud providers and the issues faced by the cloud users. Cloud providers provide security to the user data through the mechanism Service Level Agreement (SLA). Security will be based on data sets, cloud infrastructure, data storage and based on the services provided by the cloud providers. Security features of data like privacy, authentication, application venerability, data integrity, access control,
Fig. 1: Cloud services

Fig. 2: Categories of services

Confidentiality plays a vital role in communication. Security issues also lie in service models at delivery as SaaS, PaaS, IaaS. These services are shown in Fig. 1 and described in the Fig. 2.

Security issues lie on different phases such as User’s authentication, open source provision, virtual infrastructure, SLA, data storage, resource request. There are various security breaches in services (Subashini and Kavitha, 2011). There are various security issues related to the service delivery models (Sharma et al., 2011).

USER’S AUTHENTICATION

Accessing and sharing of resource locally among various users should maintain authentication to protect the resource from intruders. The user-centric identity management in which the user’s are allowed to choose the identity information to authenticate. So that the valid users are allowed
to access the online resources available in the cloud. The proposed protocol was OpenID. Whenever the user wants to enjoy the services that are provided by the provider, he must be authenticated by the security provider. The authentication is based on the identity information (Recordon and Reed, 2006). Public cryptography was proposed along with federal identity management to strengthen the cloud computing security. In that user should be authenticated to access the resources provided by the cloud by using a single sign-in to a particular cloud provider and can access their accounts from various cloud providers without any authentication to each. This simplifies the user's process of authentication (Yan et al., 2009). Some methods to identify the information leakage in the cloud. Information leakage is due to the unauthorized user. Due to the information leakage, the security of the cloud can't be maintained. It can be identified by placing malicious virtual machines in the co-located manner to capture the processing information by the third party (Ristenpart et al., 2009). Security to the user data and as well to the application via User centric architecture. The architecture provides security in different levels such as SAAS, platform as a service (PAAS), Infrastructure as a service (IAAS). Security As a Service (SECAaaS) is a user centric architecture and a type of SAAS. SECAaaS gives cloud users more control over their security. The solutions for authentication and data integrity by Trusted Cloud Computing Platform (TCCP). It provides IaaS by allocating a separate environment for the execution of guest virtual machines (Santos et al., 2009).

**SLA:** A methodology to evaluate the security through SLA’s for the web services (Casola et al., 2006). The capability maturity model for the Cloud providers to protect the data and the programs of the users in the cloud from intruders. The cloud providers should satisfy the user's security through the SLA (Creese et al., 2009). The architectures for multilevel SLA management regarding the resource allocation and to avoid the issues. The services are of different levels and each has its own issues. All the security issues should be solved using SLA (Comuzzi et al., 2009). The important role of SLA between the cloud service provider and cloud user in terms of security (Kandukuri et al., 2009). A method to avoid SLA violations. The security issues may also occur due to the resource allocation among various users. To avoid that Cloud Management allocate resources based on the SLA's. Then measurements and monitoring are done to detect the violations of SLA, when more number of resources are to be allocated to the users. Author proposed a method to solve the problem of resource allocation to the user in turn which avoids SLA violation (Brandic et al., 2010). The security services provided by the providers to the users based on the SLA’s. They also mentioned about the types of clouds that can be accessed by the various users and their related security measures by the cloud providers (Ramgovind et al., 2010). A method based on SLA. When the user wants to access resources from hybrid cloud, there will be security issues. The method paved the way to utilize SLA to allocate resources and it provides trust to the user about the provider. A domain specific language for SLA’s to allocate the resource according to the requirements of the Cloud User (Bernsmed et al., 2011). An enhanced resource management by isolating attributes in SLA’s to prevent side-channel attack. They provide solutions for the attacks (Raj et al., 2009).

**VIRTUAL INFRASTRUCTURE**

The virtualized Infrastructure of the cloud should be secure against the vulnerabilities. Hackers attack the infrastructure by introducing malicious code to achieve Denial of Service (DOS). So, the virtualized environment has been protected by cloud providers using Infrastructure as a Service
(IAAS) (Carpenter et al., 2007). An overall view about the security issues in cloud computing, Open Identity Management authentication for the cloud user makes integration difficult. They also observed that the issues related to virtualization are not specific to the cloud but issues due to the open source affects the cloud security (Sengupta et al., 2011). The various security services on the infrastructure that all are on demand for the cloud users. They proposed the dynamically provisioned access control infrastructure (DACI) architecture and also provide the context for security mechanism (Demchenko et al., 2011). The security problems in virtual networks are analyzed based on Xen platform (Wu et al., 2010). The solution for managing the distributed Virtual machines by introducing Xen Virtual Machine Monitor (VMM) for security purposes (Murray and Milos, 2008). Virtual machines are also used to maintain the integrity of the cloud (Li et al., 2012). A solution Private Virtual Infrastructure (PVI) which provides security to the client against the risks (Krautheim, 2009). The security risks in IaaS and provided some solutions as encryption and access control to verify the user’s accessing the resources or the data across multiple clouds and too from different environment (Vaquero et al., 2011). Virtualization provides security by providing the integrity for quest virtual machines and the cloud components (Lombardi and Di Pietro, 2011). Virtualization for hardware can be done with the help of hypervisors which provide security (Perez et al., 2008).

DATA STORAGE
The Cloud management moves the data and application software to the datacenters since it is a distributed storage. The data storage security is important to provide QoS. A method based on homomorphic token with a distributed verification of coded data. So, that security of the data is maintained during the access (Wang et al., 2009a, b; Hendricks et al., 2007). Some techniques to secure data that are used for the computation (Jensen et al., 2009a). The solutions for controlling the data in the cloud using computational encryption techniques (Chow et al., 2009). A security solution for processing the huge amount of data in the cloud (Khalid and Mujtaba, 2009). Some security techniques for managing the stored data. While processing the data across the various clouds there are some security lacks which can be overcome by the above suggested technique (Zhou et al., 2010). For providing the data security in the cloud a prometheus design tool provides the consistency. There are five types of agents to provide the service to the users. These agents work independently but communicate among themselves to fulfill the requirements of the users (Talib et al., 2011, 2012).

OPEN SOURCE PROVISION
Most of the security risks are due to the usage of open source provisioning tools, application servers, databases and scripting languages in the cloud computing. There may be the possibility of security risks like SQL injection, cross site scripting, database row-level security and Web 2.0 specific security. Due to this open source “there is a possibility of metadata spoofing attack, in which an adversary can overwrite WSDL metadata and the compromised client can generate un-warranted actions” (Jensen et al., 2009b). Some methods for the user to select the platform where to deploy the applications of the cloud for the security purposes (Petcu et al., 2011).

RESOURCE REQUEST
The Security-oriented modeling languages for requesting the resource (Murray and Milos, 2008) Security assists with SOAP messages. The request by the User to cloud is by means of HTTP. They also defined about the XML security standards like XML signature and XML Encryption and the way that they are applied to the SOAP messages to retain the security (Jensen et al., 2009b).
SOLUTIONS

Various risks that are due to sharing of resources among the various users. The risks may be attacks and they provided solutions as cloud providers should do network based co-residence checks to handle the attackers (Ristenpart et al., 2009). The solutions "namely partition-looked cache (PLe cache) and random permutation cache (RPcache), to defeat cache-based side channel attacks" (Kong et al., 2008). The self manageable cloud services to overcome the failures and if any environmental changes that affects the Cloud (Brandic, 2009). Whenever, client request for data to process the information from the cloud providers, information is provided and there will be exchange of information among the clouds too. So, there is a situation for privacy disclosure problem to arise. So, the privacy preserving technologies that can be implemented in cloud services (Sharma et al., 2011). The Advanced Cloud Protection System (ACPS) to guarantee security to the resources in the virtualization. ACPS can monitor the integrity of guest and infrastructure components to provide the security (Sengupta et al., 2011). Some line of defense against the threats. The defenses may be Firewall, intrusion detection and prevention (Skene et al., 2010). The security of cloud can also be provided by securing the basic operating systems and the virtual machines that are used for cloud computing (Santos et al., 2009). The solutions regarding the security of the cloud by introducing a trusted third party who will provide all the security regarding integrity, confidentiality and communication (Zissis and Lekkas, 2012). Virtualization is the best thing that would provide users to invest less on hardware and multiple machines can be executed in a single with high degree of security (Jyoti et al., 2011).

CONCLUSION

This contribution provided an insight of various security issues on the Cloud like User’s authentication, open source provision, virtual infrastructure, SLA, data storage.

REFERENCES


