PRIVACY AND SECURITY CONCERNS IN CLOUD COMPUTING

P.SRAVANI REDDY1 UMA MAHESHWARI2
1,2Department Of Computer Science And Engineering
1,2Saveetha School Of Engineering, Chennai, India.

Abstract— In Cloud Computing environment, when clients or providers want to authenticate themselves to the cloud, they face some problems like the security level of their credential information to be stolen or by illegal using of their decrypted messages by attackers during the communication process. The service providers and clients delegate a third party to monitor and enforce the data center in the infrastructure level of cloud. However, the third party might not be a trusted enough for one of them or for both, so they need to manage their data by them selves. In this paper, I will go over one technique for each issue to solve the privacy problem. Web Service Security model for encrypted and decrypted messages, and Private Virtual Infrastructure model for monitoring the data over cloud.

Key words: Cloud Computing, Cloud Security, Locator Bot, Virtual Private Infrastructure, Web Service Security

I. INTRODUCTION

In Cloud Computing environment, there are different issues that users should consider when they get the benefits of the Cloud services. Most considered issues are related to the boundaries of the organization, which direct us in deep to the issue of loosing the control of the organization resources within the cloud environment [1]. That happens when the resources are moved to the cloud environment then the owner of these resources losses the monitoring and controlling on their functionality One of the most important issues is the inside and outside security threat. The outside threats are similar to the tradition large datacenters [2]. Cloud Computing is not a new concept that we use to provide the information via networks. Since that, the same traditional networks security issues cloud computing has been faced, and we need to figure out these problems. Cloud computing is faced by different challenges to be applied with a high level of security [3]. The responsibility of facing the security issues in the cloud is divided between different parties like the user, service vendor and a third party who located in between of the user and the provider to provide some security services like Service Level Agreement [2].

There are two different security models that support two different levels of services in cloud computing to secure the first model is web-service security(WS-security) that supports working in message level ,this model provides encryption integrity, and confidentiality. The second model is Private Virtual Infrastructure (PVI) that discuss the safety of Data centers in the cloud by distribute the duties between the service provider and the client[4].

II. WEB SERVICE SECURITY MODEL

This part is one of the most significant solutions for the security issue in Web Services, which provides some security services to the cloud like integrity, confidentiality and authentication [5]. This solution explains how to apply the security XML standards, which are XML signature and XML encryption to the SOAP messages.

A. MXL Security Standards

The first standard is the XML Signature, which allows the process of digitally signing the XML fragments to proof authenticity or to ensure the integrity. A simple structure of the XML Signature element is as follows [5]:

```xml
<Signature>
  <SignedInfo>
    <Signature>
      <SignatureMethod Algorithm="..."/>
    </Signature>
  </SignedInfo>
  <Reference URI=""/>
  <DigestMethodAlgorithm="...">
    <DigestValue>...<DigestValue>
  </DigestMethodAlgorithm>
  <SignatureValue>...<SignatureValue>
</Signature>
```

The second one is the XML Encryption, which provide the encryption service to the XML fragment to be encrypted to ensure data confidentiality. The process is as follows an encrypted Data element takes a place of the encrypted fragment containing the cipher text as a content of the encrypted fragment.

B. Transport Layer Security (TLS)

It has been introduced under its common name “Secure Sockets Layer (SSL)”. This layer consists of two main parts [5]:

1) Record Layer

which encrypts/decrypts TCP data streams using the algorithms and keys negotiated in the TLS Handshake

2) TLS Handshake:

which is used to authenticate the server and the client. Today, it is considered as the most important cryptographic protocol worldwide, since it is implemented in every web browser.

3) Web Service Security Issues

I will illustrate two main issues that WS-Security model is faced, which are XML Signature element wrapping and web browser security.
Web Service Level Agreement (WSLA) framework is developed for SLA monitoring and enforcement in SOA [8, 9]. In cloud computing environment, the monitoring and enforcement tasks are delegated to a third party to solve the trusted problem [2].

In order to verify the security within the cloud, each service in the cloud needs to be able to report security properties present and the report must be verifiable. This ability means that clients need visibility into the security settings and configuration of the fabric. Trusted Computing Techniques have been chosen to verify these settings and report the configuration of the fabric in PVI. Additional requirements for PVI are that communications to and within PVI should be done through virtual private networking and all links should be encrypted with IPSec or SSL tunnels. This step provides confidentiality on the network and prevents other users within the cloud from eavesdropping and modifying communications of PVI [9]. One of the components of the PVI is the PVI Factory; which represents where all the components are replaced on. The PVI Factory should be fully controlled by the owner of the information either being standalone unit or in the site of the owner [4].

### A. Trusted Computing

Trusted Computing provides users to verify their security postures in the cloud and control their information, allowing them to achieve the economies of scale, availability, and agility that the cloud promises.

### B. Trusted Platform Model (TPM)

It is a cryptographic component that provides a root of trust for building a trusted computing base. The TPM stores cryptographic keys that can be used to attest the operating state of the platform. The keys are used to measure the platform, which are then stored in the TPM’s Platform Configuration Registers (PCRs) [9]. When clients want to attest a platform, clients can request the PCRs and verify that the platform meets its requirements and policy.

What is the problem?

Trusted Platform Model is only works for non-virtualized environments.

To solve of the problem

TPM needs to be virtualized. So, Virtual TPM has been developed and implemented for each virtual machine (VM) on a trusted platform. Individual computing platforms within the cloud each have a TPM owned by the service provider. VTPMs are linked to the physical TPM and used to secure each VM in the cloud [6].

Locator Bot (LoBot) is an architecture that cryptographically secures each VM by tightly coupling a VTPM in its own stub domain. LoBot allows each VM to be verifiable by its owner and provides secure provisioning and migration of the VM within the cloud as well [9]. The LoBot application at the target environment, this probe application, receives and unseals the resource environment. So, if the source environment got changed and unknown tampering within exist transfer, the decryption phase will detect this changes. The probe measures do the measuring of the source environment one more time to make sure that everything is safe and to validate the integrity and to ensure the successfully of lunching process in the target environment.

### III. PRIVATE VIRTUAL INFRASTRUCTURE (PVI) MODEL

Usually, there is a third party that works with service provider and client to control and save datacenter. In cloud computing, PVI model has been suggested to distribute the responsibility of control and save datacenter between providers and clients. In this model, users would have security over their information in cloud and providers would have security over the fabric of the server [5].

The service level agreement (SLA) between the client and provider is critical to defining the roles and responsibilities of all parties involved in using and providing cloud services. The service level agreement should explicitly call out what security services the provider guarantees and what the client is responsible for providing.
IV. CONCLUSION

In this paper I represent two solutions for two problems in Cloud Computing. The first model is Web Service Security (XML Signature and XML Encryption) that solves the unauthorized using of decrypted messages. Although, the idea of this model can solve this problem, the web browsers are not able to apply this model. So, we need to develop a web browser that supports the idea of this model. In the other hand, a third party monitors the datacenters in cloud, so PVI model can determine the responsibilities for client and provider. The problem that I believe is when client wants to know which platform meet his requirements because it will still problem for the client to determine his requirements and control the security side in the infrastructure. The client will cause a number of problems in the data center and in the cloud computing system.

REFERENCES