Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 115 – 121

Procedia Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Survey on the Key Management for securing the Cloud

Pradeep K V[a], V.Vijayakumar[b]*

[a]Research Scholar, VIT University, Vandalur – Kelambakkam Road, Chennai – 600048, India,
[b]Professor, VIT University,Vandalur – Kelambakkam Road, Chennai – 600048, India

Abstract

Importance of cloud is due to its unlimited supply of services such as server, storage of data and what not anything as a service (Xaas) is possible. As long as users enjoy its advantages need to take care of the security issues raises due to its infrastructure which is distributive and as function of the armed service to the consumer provider extend their hands to secure the data .This paper mainly concentrating in how many ways provider will offer security and how the mechanism works and which is most suitable for each and every type of service and cost involved for the security provision.

Keywords: Cloud Security; Cloud Services; Key Management.

1. Introduction

Cloud computing has become an impotent business model where computational resources are rented to customer by provider. Virtualization technology is key for cloud computing. The services provided by the service provider can be categorized into three types which are infrastructure as a service (Iaas) , software as a service(Saas), platform as a service(Paas). In general cloud technology is described in three types such as public cloud where services are

* Corresponding author. Tel.: +91-9445825675.
*E-mail address:*pradeep.kv@vit.ac.in

doi:10.1016/j.procs.2015.04.072

provided to anyone. Private cloud where services are provided to particular private organization which owns the privilege of cloud services and the remaining is community cloud where different organizations share the resources between the min orders to solve their common issues. In cloud technology there is a need of strong security model because the applications and data of different tenants will use same resources which can be vulnerable to security attacks. Vulnerability in operating system or application can be exploited by attacker to generate attacks which may target physical infrastructure or virtual machines of other users. The important aspect in achieving security is using cryptographic techniques.in general keys are used in encryption and decryption processes. In general these keys are of two types**:**

1) Secret key: This is a key which is broadly used for

- With the help of the Cryptographic algorithms it is possible to execute the encryption and decryption and
- To furnish data wholeness with the help of message authentication codes.

It exhibits the symmetric behaviour because the same key is used for execution of encryption and decryption or for the integrity verification.

2) Public/Private Key Pair: A distich of numerically linked keys used for certification, digital signature or key administration in asymmetric cryptography. By looking at the name we can predict that the generator of the key who is owner of it contains the private key for security purposes, the private key is used by the owner of the key pair, is kept secret, and should be protected at all times, and the other key is for the multicasting to the group which is public use to accomplish or reverse

There are additional keys like public and private authentication key pair: this key pair is used to authenticate.
Public and private signature key pair: To establish a trusted key between two parties it needs this key pair where public key is used to verify the private key pair which is used by a single party. Example for this type of key is S/MIME messages. Coming to particular cases a pair is necessary for both the verification and signature functions. which will valid up to 3 years in use

Public and private establishment pair: Mainly for the inserting a key between the two parties and it is often encouraged not to use the same key insertion and attestation, but there are some devices such as webservers use the same key for two purposes and it is traditionally main part in the networking platform and key pair is valid up to 3 years.

Symmetric encryption and decryption key: Nature of the key must be symmetric for both encryption and decryption of either data or messages and these keys have short life if data is transmitting particularly for each message and each session

Symmetric message authentication code key: This key will ensure the integrity of the data to do so it requires three proficiencies:

- Necessary to use the encryption algorithm which is symmetric and MAC mode of operation for example CMAC using AES
- Algorithm to be symmetric and an attested encryption mode (GCM or CCM using AES)
- Need to use Hash Function (HMAC)

Symmetric wrapping key: A symmetric wrapping key is utilized to convert a proportional key or a topsy-turvy private key. In addition it is also known as Key Encrypting Key.