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.

***States of the Key***:

There are different states for the key from generating the key to the destruction.

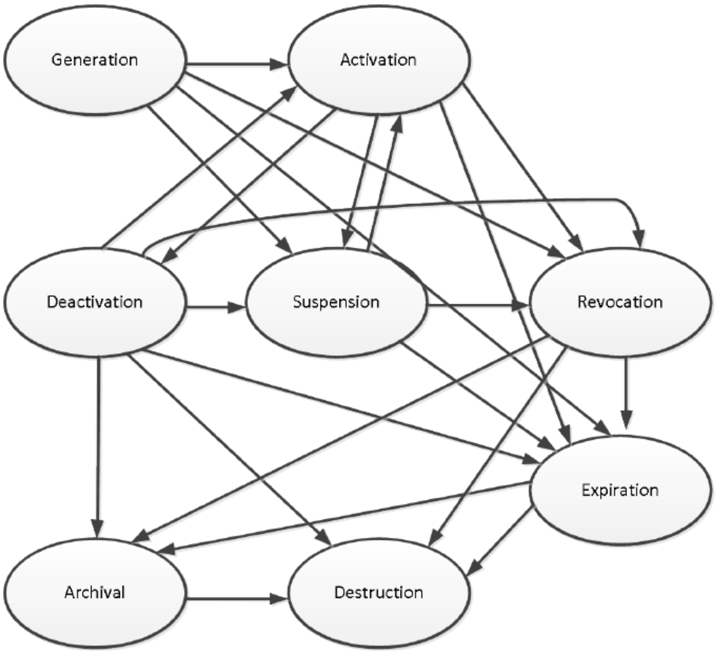

***Fig 1: States of the key***

There are different states for keys which are
1) Generation: At this state public or private key pair is rendered.
2) Activation: Key can be activated when it is available or the date that is mentioned along with metadata.
3) Suspension: Key can be suspended when status of the key is unknown or the owner of the key is not acknowledged. In the case of public key when a private key is suspended it is acknowledged to other parties.
4) Expiration: Key may be expired when a crypto period is ended.
5) Destruction: Key is demolished when there is no use.
6) Archival: Key is needed after crypto period then it is archived.

## *Related work:*

In this section various cryptographic techniques are used in common is discussed.in general when cryptography is considered there are two types of cryptography algorithms which are depend on the symmetric or asymmetric nature. Asymmetric is also known as public key algorithms.
Examples of asymmetric algorithms are:

1)RSA: Which is a public key algorithm commonly used encoding algorithm RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman who has proposed this algorithm.in this RSA algorithm two key public and private key which are different. Public key is used for encrypting the message and it is known for any one.private key is used for decrypting message.it is kept secret.

2) Diffie Hallman: this is a key exchange algorithm that is commonly used. Accords both the users to substitute a secret key over an Arcanum channel without any prior secrets. Symmetric algorithms are more where only a key is used for both encoding and decoding. Thus in symmetric algorithms key exchange is prior to the message transmission. Both sender and receiver must authenticate the key for message transmission.

Symmetric algorithms are classified in to two types block and stream algorithms. Following are some of the most commonly used symmetric algorithms:

1) DES: Data Encryption Standard is woks on the Feistel block cipher. Developed by the IBM cryptography researcher which is in the form of block.

2)AES: Advanced Encryption Algorithm it is invented to overcome the failure of DES like delay in implementing on board so it concludes that it is only for the hardware so AES which is for software comparatively AES runs faster and hence runs relatively slowly. AES can use a 128, 192, or 256 bit encryption key but DES uses 56 bit key

3) Blowfish: It is the encryption algorithm introduced in 1993.it uses 38 to 448 bit key length. It is 16round Feistel cipher and uses large key-dependent S-boxes. In the performance evaluating of different algorithms on power consumptions done by S. Abdul. Elminaam et.al.in 2009, blowfish has shown better performance than other.

4) RC2: RC2 is mainly for the data security which is invented by the Ron Rivest which is a cipher of varying length

5) RC4: It is accepts the arbitrary length stream cipher which is also developed by Ron Rivest in 1987 which is 256 bytes and provides the speed processing and it has alien security and it is fiddling to break.

6) RC6: Derived form of RC5 is designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to cope up with the anticipations of the AES contention. The encoding and decoding of the same key happens in the symmetric algorithm rule where as in asymmetric algorithm rule different keys are used for the encoding and decoding requires 3000 bit key to accomplish the same grade and these are much faster in terms of operating

## *Proposed Work:*

Managing the keys is a most important thing in the cloud environment in order to provide synchronisation for data flow in the networks. Encryption is the main thing to assure the security but with lot of computational power and the keys generated by encryption will be a problem in terms of storing those keys which can't be in the cloud because of its dynamic nature so it demands the key to be with the consumer to avoid overweening computations for the decryptions in the database for the data retrieval.

The following are the universal prerequisites for the key management:

- The companies which are performing the key management need to be authenticated and to affirm their empowerment to perform these functions.
- The affiliated commands and their information must be resistible to the spoofing.
- Capable of precluding the undiscovered and unauthorised alterations to shell the integrity
- Secret and private keys are auspices from the wildcat revelation.
- Keys and the data about their logs also are protected from the spoofing.
- The security strength of the protection mechanism used for the key management.

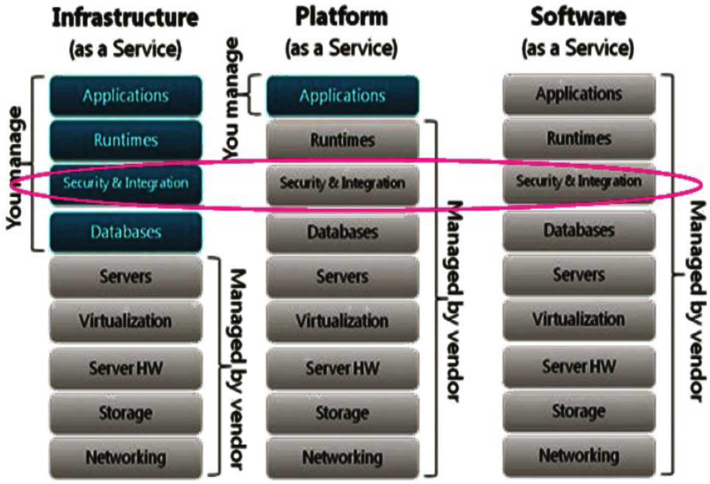

Fig: Cloud service models and their security handling

From figure, out of these three services, both security and integration is managed by the vendor itself in the Paas and Saas, but coming to the Iaas it is completely different because it has to manage by consumer itself.

The secure direction of the cloud and its resources is a vital expression for the cloud computing and cryptography is the one main thing which directs the cloud towards security and in the perspective of the cloud consumer it implicates two necessary operations

- Assure fundamental interaction of the Cloud consumer and it's avails.
- Assuring the safety of the metadata storing.

Key Management system plays a vital role in the extending the hand to the cryptography to maintain the cloud security and the keys which are explained above will be logically distributed to the consumer and provider.

### *Disputes in Key management and Security operations for the cloud services:*

*For Iaas*: In this service where the security and integration is taken care by the consumer and as it is very flexible so that consumer positions the resources in the form of VM's or there is a chance of using leased VM's which lets in the checking by default and the assured Vm's must be attested to ensure the assured access to it. As soon as Vm is parameterised and it is launched on provider platform to service the consumer by becoming the running instance. To create a running VM instance it should proceed after the VM creation .There are different predefined levels for the security in Iaas

*IaaS-SC1*: This levels mainly concentrate on the ability to attest the determined VM image templates which are made usable by the provider to its consumers to parameterise them to meet their own requirements.

*Architectural Solution*: The main fear of the consumers while taking the predefined VM images from the provider either it is veritable or not so to resolve this fear the templates must be digitally ratified so that it needs public and private keys to do so and again it is provider responsibility to store them securely while in use also which is by using the FIPS 140-2 validated module for cryptography by NIST and it makes provider responsible for the providing of public key in a attested manner

*IaaS-SC2*: It is completely on the power to certify the API calls from the consumer to the provider's Hypervisor system through the VM Management interface

*Architectural Solution*: The responsibility of the provider is to certify the VM image and provide the public key pair and to tie the customer individuality to it and it is the task of the consumer to parameterise the VM to meet its own requirements and the provided key pair is the key to initiate the calls from the consumer to the VM or the other round way is to collaboration of the consumer with SSH or TLS to establish a session with VM direction interface.
IaaS-SC3: Capability of providing secure communication during executive operations on the available VM instances.

*Architectural Solution*: Administrator of Iaas customer needs high level root access to modify or the operating instances that are rented for the customer as mentioned in the above security level by the SSH which provides a secure structure for the public/private key pair. This sturdy cryptographically authentication prevents anonymous affiliation makes an attempt to the VM instance, likewise as preventing authentication attacks (such as secret guessing). Moreover, the SSH protocol permits uneven keys to be accustomed perform Associate in nursing echt transitory Diffie Hellman (DH) key institution. The regular session keys calculated throughout this method are accustomed encipher the payload and to get hash-based message authentication codes, therefore providing each confidentiality and integrity security services. once SSH is employed, not solely is that the administrator echt, however all the commands, responses, and payload ar protected in each directions from eavesdropping and against unobserved modifications, and are cryptographically etch.

*For Paas*: The goal of a Platform as a Service (Paas) offering is to give a computational stage and the fundamental set of use advancement devices to Consumers for creating or sending applications. Despite the fact that the hidden OS stage on which the improvement apparatuses are facilitated is known to the Consumer, the Consumer does not have control over its design capacities and consequently the ensuing working environment. Shoppers communicate with these devices (and related information, for example, advancement libraries) to create custom applications. Purchasers might likewise require a stockpiling base to store both supporting information and application information for testing the application usefulness.

*Paas SC1*: The capacity to set up secure connection with conveyed applications and/or improvement apparatus occasions

*Paas SC2*: The capacity to safely store static data.

*Paas SC3*: The capacity to safely store application information in an organized structure for example in DBMS

*Paas SC4*: The capacity to safely store application information in an unorganized structure.

*For Saas:*

Saas offerings give access to applications facilitated by the cloud Provider. A Saas cloud Consumer might want to collaborate with these application cases safely (through setting up secure sessions and solid validation) and activity the different application peculiarities, contingent on the set of relegated authorizations or by expecting their doled out parts (which give the consents). Moreover, a few Saas Consumers might likewise want to store the information produced/handled by those applications in a scrambled structure for the accompanying reasons: (a) to counteract presentation of their corporate information, because of loss of the media utilized by cloud Providers; (b) surreptitious review of their information by a Saas co-occupant or by a cloud Provider executive. In spite of the fact that the previous peculiarity (secure connection with application) is given by the Saas Providers, the second gimmick (putting away information in an encoded structure) right now must be given altogether by the Saas Consumer.

*Saas-SC1***:** The capability to establish a fundamental interaction which is very secure.

*Saas SC2***:** The capability of storing all the data in a modulated way.

*Architectural Solution:*

There are two operational situations here. On the off chance that all fields in the database need to be encoded, then the encryption abilities need to live with the cloud Provider due to the sheer scale of. Then again, if each one cloud Consumer needs particular encryption of a subset of fields, and since this subset changes with every customer; all encryption operations need to happen at the customer (cloud Consumer). The key administration challenges for each of the two alternatives are examined beneath after a concise portrayal of the related design arrangement

## Conclusion:

The proposed key management has considered various parameters for the identification of the exact key mechanism which is suitable for providing the desired security. The key management functions has considered security, fast transmission of data and each and every key has different functionalities but embedding them in a single key function produce desired results. The consumer holding the key is much more suitable than producer having the key.

## References:

1) Cryptographic Key Management Issues & Challenges in Cloud Services ,Ramaswamy Chandramouli ,Michaela Iorga ,Santosh Chokhani , September 2013.
2) F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture (NIST SP 500-292), National Institute of Standards and Technology, U.S. Department of Commerce (2011).
3) P. Mell and T. Grance, The NIST definition of cloud computing (NIST SP 800-145), National Institute of Standards and Technology, U.S. Department of Commerce (2011) http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
4) L. Badger, D. Berstein, R. Bohn, F. de Valux, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, US government cloud computing technology roadmap volume 1: High-priority requirements to further USG agency cloud computing .
5) Rfc 2627, Key Management for Multicast: Issues and Architectures Author D. Wallner, E. Harder, R. Agee Date June 1999.
6) How Cloud Deployment Affects Compliance Safenet.com.
7) Key Management : A Cryptography Tutorial, cryptography world.
8) For transferring data units among storage elements US 5940507A .
9) What is Data Encryption Standard (DES)? - Definition from WhatIs.com searchsecurity.techtarget.com
10) Symmetric algorithms - Types of symmetric algorithms - Symmetric key algorithm www.encryptionanddecryption.com
11) Asymmetric algorithms examples - List of Asymmetric algorithms www.encryptionanddecryption.com
12) http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdfwww.facweb.iitkgp.ernet.in