Journal of Information Engineering and Applications www.iiste.org
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.3, No.6, 2013- Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications

Brief Analysis of Methods for Cloud Computing Key Management

Sneha Soni
Sagar Institute of Research & Technology –Excellence, Ayoudha by Pass Road, Bhopal
Tel: +91 9907096956 E-mail: soni.snehaa@gmail.com
Amit Soni
Saroginin Naidu Govt Girls PG (Autonomous) College, Near 7 Number Stop, Bhopal
Tel: +91 9893448577 E-mail: stoneuntitled@yahoo.com

Abstract

In this paper basic of cloud and possible methods for its key management is discussed. Now a days cloud computing is good arena in the field of research. In cloud computing cloud customer and cloud provider needs to secure data against loss and theft. Encryption with key management is a technique for securing the personal and enterprise data. It is mainly used to protect data. In this paper how key management can be performed to protect cloud data is discussed. So that risks of data loss and theft can be reduced.

Keywords: Cloud computing, Cloud architecture, Encryption, Key management

1. Cloud Computing and Its Architecture

Cloud computing is a new business model. It is a way of delivering computing resources, Cloud computing is not a new technology. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

If we think about the why cloud computing is needed then there are N number of reason, it does not require any software or hardware to install, cloud computing is equipped with dynamic allocation, pay per uses, platform independent, massive , web scale abstracted infrastructure and no long term commitments.

Characteristics of cloud computing is as follows:

It uses virtualization systems, which will reduces hardware cost and there maintenances, it also provide on demand self service, scaling feature on the basis of demand, it also include storage devices, memory, processing units and networks for communication. It also provides automatic control monitoring of resources and optimization, it can access in heterogeneous plateforms, change back, show back and metering back features.

The cloud computing has three basic deployment model named as Private cloud, Public and Hybrid Cloud, let's see what they are Private cloud plateform is used on individual need basis. In this service model business essential is turn into information technology environment and uses it to deliver service to their uses. It provides virtualization, multi-tenancy, consistent deployment; change back, pricing and security and access control.

Public cloud : In this serive model a business rents the capability and businessman or any client will pay for what they use on demand. This plateform is avaiable to public users . any public user can register in it and can enjoy the service of avaiable infrastructure. Public cloud is the most taggated area for malicious users. In this cloud nothing is avaiable as free of cost, its vendors providean access control mechanism for their uses. It is avaiable through third party service provider. It shows the cloud features i.e. pay per uses and on demand uses.

Hybrid cloud: It combines the elements of the public and private clouds. It is the extension of both the clouds. In hybrid cloud user can keep control on data and business- critical services by simultaneously outsourcing non-business–critical information and cloud process. It offer advantages of both the public and private clouds i.e scale and conveniences of public cloud, control and realibility of on premises software and infrastructure.

There are three types of cloud service model i.e IaaS, PaaS, Saas let's see what does it mean, IaaS is Infrastructure-as-a-service, it provides access to computation resources , network, hardware, or virtual computers which enable an internet based services. It uses the concept of the virtualization, one of the example Amazon EC2.

PaaS is platform-as-a-service, it provide provisioning of hardware and operating system. With the help of PaaS support customer writes custom application. Where cloud providers deliver platforms, tools and other business services that enable customers to develop, deploy, and manage their own applications, without installing any of these platforms or support tools on their local machines. The PaaS Model is hosted on top cloud infrastructures directly. Mostly used PaaS are Google Apps and Microsoft Windows Azure.

SaaS is Software-as-a-service (SaaS), hosting of the cloud providers applications on the cloud infrastructure is done. End users are internet based service user. Application installation is not needed at the customer computers. It is hosted on top of PaaS, IaaS or can directly host on cloud infrastructure. Various examples of the SaaS include customer relationship managements, management information systems, human resource management and many more.

2. The Cloud Computing Key Management

Key management is a huge, complex issue now in the land of cloud computing. Encrytion is generally used technique for implementing ckey management . now a days encyption is universally recognized method to protect data .

Management of cloud comuting along with the key management is very complex issue. In public cloud particularly in IaaS, it is an complex task to implement because it has most of the pitfalls . if we think about the key management then the biggest point that needs to be consider is not that how encryption is implemented but main issue is the requirement of the ownership of the key. Also one other point to be noted is that where to keep the encryption key either in cloud infrastructure or in customer premise.

Security is one of the main problem in cloud computing structure. Cloud service providers perform task for monitor the cloud and data usage. In this Users end is not responsible for maintaining back end data storages and its exact storage location. Security of this user end data can be ensure by implementing key management.

Various key management interoperability protocols are used to ensure effective ness of the key management. enabling encryption on the virtual machine is challenging task because it is not possible to encrypt everything. Use of virtual machine increases the amount of the data, its working is not same as the physical machine.

Cloud customer is only responsible for maintaining key management . Key provisioning and storage is not mainatained by them. Virtual machines generally stores key. There are various stages for key management i.e. generating keys, using keys, storing keys, distributing keys revoking keys, verifying keys and destroying keys, some of the assumption are two basic scenarios.

Major issue that comes in key management is key geeneration and key application, security of the keys and master key, failure recovery, key expirationand key uses. , there is poor integeration between key management systems and application of the encryption and data lifecycle.

3. Methods for Cloud Key Management

Description of each method is as follows.

3.1 First methods

In this method, encryption is provided by the cloud provider. Cloud provider plays an important role for providing security of data. It kept customer encryption keys. Virtual wall is created around cloud data so that data can be protect from threats. With the help of encryption plain and sensitive data transforms to protected format. Whenever data is transfer from one place to another place it is protected by cloud provider encryption.

When encryption is performed in the cloud database two important aspects is need to remember first is separation between data, what data is used in the cloud and what data needs to be secured. Second is who the authorized person is who can access and control data. What data is sensitive and what data is encrypted.

As far as sensitivity of the data is concerned i.e. social security numbers, account number, patient healthcare records, etc. can be consider. Cloud provider encrypts data when it is stored in databases or transferred through a web browser. Overall encryption is under the control of the cloud service provider and it is not segmented by the customer.

Only authorized users and organization with access to right cryptographic keys, can access that data. Accessing permission of reading and writing is also given by the cloud provider. By implementing this type of method cloud data and backup tape cannot hacks by unauthorized user.

This method can be assured when taking care of these points and doing practice securely storing of the encryption key. Distribution of keys on requirement basis, selection and use of encryption algorithm, management of the key lifecycle, and maintenance of access privileges, proper documentation of status of key management and encryption. With the help of such habits greater security can be maintained regardless of who is the owner of cloud infrastructure and what is its location.

3.2 Second *method*

The second method involves trust on third party with user encryption keys. In this method your trust on third party is the base for assuring security of the cloud database. The major disadvantage of this method is that it is mostly targeted method for hacker.

3.3 Third method

The third method includes implementation of key management server in the physically located data center.

4. Pros and Cons of the Methods

In section III we have briefly discussed the possible approach for key management in cloud computing environment, let's see the basic advantage and the disadvantage of the approaches. First method is easy to deploy and manage because very comfortably it integrates layers of cloud data. But it is very costly to implement.

Second method is not very secure if third party is not reliable then your key can be disclose. But overhead of the customer is reduced because now customer is not responsible for maintaining key management and other aspect of the clouds computing.

Third method without a doubt is secure, but it eradicates various advantages of the cloud. It also forces customer to reverse back to data center where you have stored your data.

Conclusion

After briefly discussion of key management methods in cloud computing we can conclude that for ensuring cloud computing data security it is up to the cloud customer an d cloud service provider that which methods is suitable for them by analyzing advantages and disadvantages of each method. As future work is concerned we can do research for developing cloud key management protocols that can overcome cons of above discussed methods at certain level.

References

Dr. Kumar Saurabh (2012) technical book on " Cloud Computing " second edition, Wiley – India Publication, June.

Xin Yang, Qingni Shen , Yahui Yang and Sihan Qing (2011) ," A way of key management in cloud storage based on trusted computing", NPC'11 Proceedings of the 8th IFIP international conference on Network and parallel computing, ACM Digital Library, 2011, pp.135-145.

Sun Lei, Dai Zishan and Guo Jindi (2010) on "Research on key management infrastructure in cloud computing environment", IEEE 2010, Grid and Cooperative Computing (GCC) International Conference, pp. 404- 407.

Notes

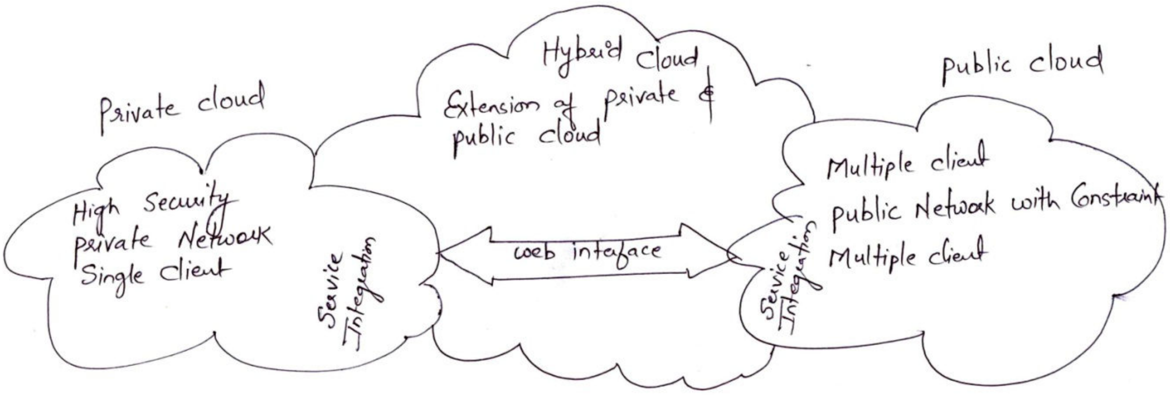

Figure 1. Cloud Computing Architecture

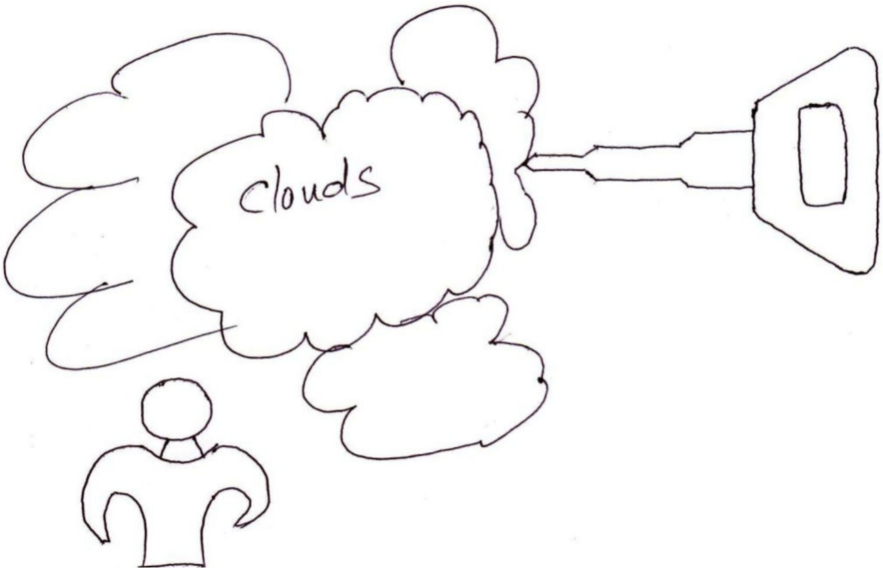

Figure 2. Cloud Computing Key Management

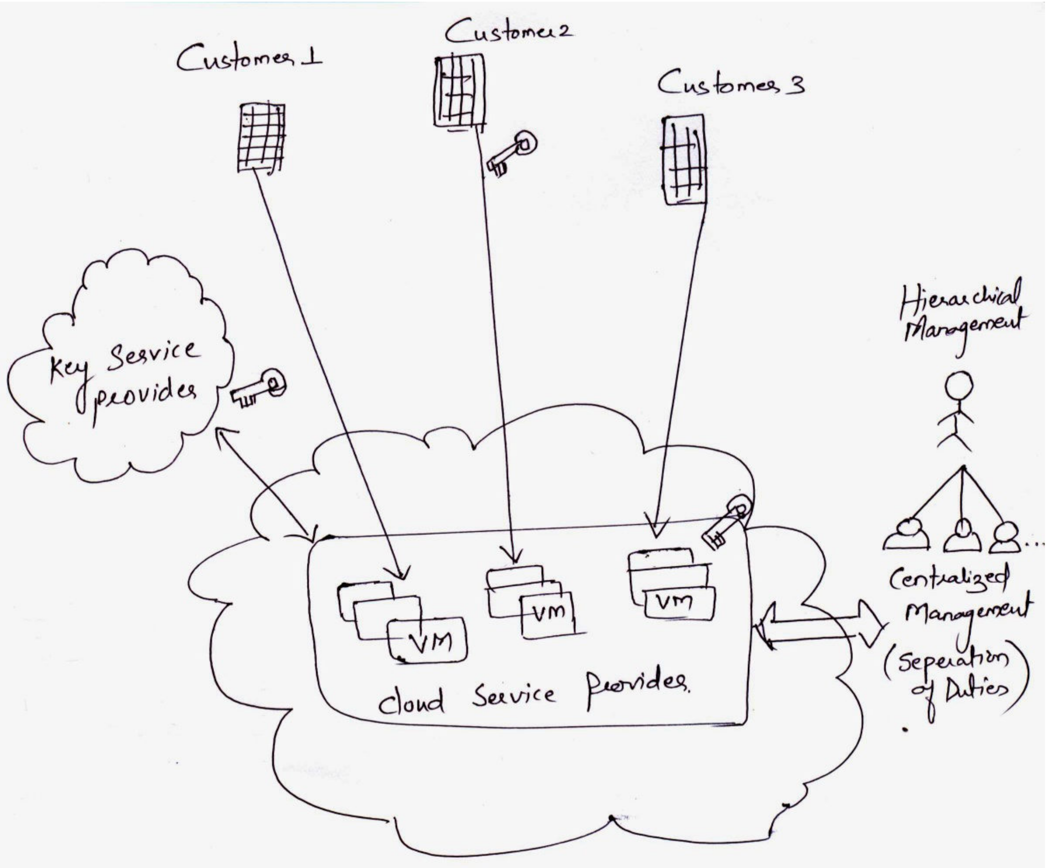

Figure 3. Cloud Computing Key Management Working