Securing the Cloud with Encryption and Key Management

Sahil Arora (Author)
Student – CSE 5th Sem
LNMIIT, Jaipur

Ashish Raj (Author)
Research scholar
MIMIT Malout

***Abstract*--Cloud computing is a metaphor for internet and provides services on demand and pay per use access to a pool of shared resources namely networks, storage, servers, and applications, without physically acquiring them.**
Cloud Computing Security refers to the policies, technologies, and methods deployed to protect data, applications and documents on the cloud.

Encryption basically is the method to turn information into unintelligible format using different algorithms, in cloud computing it is used for security purposes as it changes the data stored on cloud into an unintelligible form.

Key Management is a method with which we use special encrypted keys to access all the data.

Keywords: Cloud Computing, Encryption, Key Management, AWS.

I. Introduction

The term cloud computing is often associated with virtualized infrastructure or hardware on demand, utility computing, platform and software as a service.it is also referred to the use of computing resources that are delivered as a service over the network. It is also called cloud and is one of the magnificent shifts in information technology which can enhance collaboration, agility, scaling and availability. It allows anyone who owns a credit card to acquire virtual hardware, runtime environments, and services. These services can be used for as long as needed and no upfront commitments are needed.
A user can access all of these benefits through his browser any time once he has access to the Internet.
Cloud computing cuts operational and capital costs and lets IT departments to focus on projects instead of keeping the datacenter running all the time and to just pay for the resources and services they use to meet the needs of rapidly changing markets [1].
Cloud computing allows all the users to use all the applications offered by the cloud without the effort of installation and also offers access to their personal data from anywhere in the world through a device or a system with Internet access.
Cloud computing uses the internet and remote servers to maintain data and applications. This technology allows a much more efficient way of computing by centralizing the data,storage, memory and processing. Different from the existing technologies and computing approaches, cloud is defined on the essential characteristics of service models such as Software as a Service (SaaS), Platform as a Service (Paas), Infrastructure as a Service (IaaS), and deployment models such as Public, Private, Hybrid, Community [2].

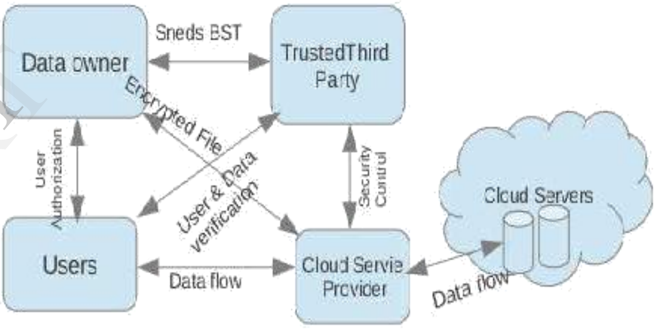

Fig. 1. Cloud Security Flowchart

A. Cloud Computing Services

- **Infrastructure as a service**

In IaaS the computing resource provided is that of virtualized hardware. In IaaS you are basically using the cloud provider’s machine by using a virtualized server and running software on it. The cloud providers provides the virtualized components or the infrastructure to the clients to build their own IT platforms [3]. Infrastructure as a Service offering can deliver features and benefits like Scalability,Utility style costing,Location independence,Physical security of data center locations.

- **Software as a service**

SaaS is simply the cloud vendors providing the software that we want to use, on their servers. It is popular for its ability to simplify deployment and reduce customer procurement costs; Using SaaS, a user can have access to any application from any computer that supports a browser [4]. SaaS offerings feature the biggest cost savings over installed software by eliminating the need for users to install and maintain the hardware, labor cost and the cost of maintaining applications. Examples of Saas include Google, Twitter, Facebook and Flickr with users able to access the services with the help of any device with internet enabled.

- **Platform as a service**

PaaS is the platform to build applications and have them hosted in the cloud by the cloud provider. It provides an infrastructure with a high level of integration in order to implement and test cloud applications allowing a user to deploy applications without having to spend money on the server on which to host them and controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

II. Network Topology

There are three kinds of network topology in cloud computing:

- **Public Topology:**A cloud infrastructure which is provided to many customers and is managed by a third party i.e. it relates to datacenters owned by IT companies where all cloud services are offered by the cloud providers. For these clouds the cloud provider is fully responsible of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use based on the billing option offered by the cloud provider. Public cloud providers like Google or Amazon offers access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine.

- **Private Topology***:* Private cloud can be owned and managed by the organization and exist at on-premises or off-premises. It is more secure when compared to public cloud.These clouds are virtual distributed systems that depend on private infrastructure and instead of pay-as-you-go model like in public clouds, there can be any other scheme in place which sees the usage of the cloud and does the billing. One of the best examples of a private cloud is Eucalyptus Systems [5]. Private clouds provide advantages like data privacy for the customer and compliance with standard procedures and operations.

- **Hybrid Topology:**Hybrid clouds allows the exploitation of existing IT infrastructures. Hybrid clouds are a combination of both private and public cloud. All cloud computing services should offer services of different degree of efficiencies but public cloud services are often more cost efficient than private clouds. For this reason many organizations maximize their efficiencies by using public cloud services for all non-sensitive work and only using public cloud when needed, thus ensuring that all their platforms are flawlessly integrated. A hybrid cloud configuration offers its users features benefits like scalability, cost efficiencies, security and flexibility.

III. Key Security Issues in Cloud Computing

Security and privacy issues are major issues on massive adoption of cloud computing. Traditional cryptographic techniques are used to prevent data and access to information on cloud. Nowadays, security has become the number one issue when it comes to cloud computing. Since a third party stores your data, there is always a risk of privacy and unethical use of your data. The given below are the various security concerns in a cloud computing environment:-

- **Data Loss or Leakage:**Data loss, which means a loss of data that occur on any device that stores data. Data Leakage is an incident when the privacy of information or data has been tampered. In data leakage the data that is leaked can be of private in nature whereas Data Loss is the loss of data due to deletion, system crash etc. Totally both the term can be referred as data breach, has been one of the biggest fears that organization face today. Data Loss Prevention is a term which is used to identify, monitor, and protect data in use, data in motion, and data at rest [6].
- **Compliance:** The security issues that an organization faces are the same sorts of issues that SaaS providers face. If a cloud service provider does not adhere to these security audits, then it leads to an obvious decrease in customer trust. Enterprise experiences a significant pressure to agree with a wide range of regulations and standards like Payment Card Industry Data Security Standards (PCI DSS), Gramm-Leach-Bliley (GLBA), and HIPPA, in addition to auditing practices like SAS70 and ISO. Enterprises need to agree with security standards, regardless of the systems required to be in scope of regulation, be that on premise physical servers, on premise VM's or off-premise VM's running on cloud computing resources. Compliance can be managed by identifying users and their access privileges, sensitive data, its location and how it is encrypted.
- **Data Privacy:**The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your

organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about data exposure and privacy. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks [7].

- **Identity management**: Every cloud provider uses its own to techniques to control access to information and computing resources provided by it. The cloud providers integrates the customer's identity management system into their own or provides their own solution for identity management. [8].
- **Cloud Forensics:**Cloud forensic is necessary in cloud security because of attackers trying to access our cloud services. We need to be notified when hackers try to gain access to our cloud. If there is a breach, the cloud provider can respond to it with less downtime than if you has investigated locally. Forensic server is easy to build and costs almost nothing until it comes to use.

IV. SECURING DATA IN CLOUD

Protecting Data in the Cloud: By definition, al cloud computing relies on is an internet connection if that is compromised by hackers or exposed to the world then the security of the cloud service being accessed fails, Ia cloud vendors data is not well protected or if it behaves in an unscrupulous manner, then again there will be a cause of concern. Cloud computing is often perceived as somewhat risky and therefore the data kept on the cloud should be well protected on customer as well as vendor's level. The following plays a vital role in helping ensure that your data is safe and that your encryption keys are protected, both when in storage and when in use in the cloud.

- Standards-based data encryption with a simple management interface.
- Key management using Split-Key Encryption.
- Homomorphic key encryption technique.
-

A. Data Encryption

In simple language data encryption is the method of translating data into a secret code or the process of encoding information to make it unreadable without the special knowledge of decryption techniques. Encryption of data is achieved using an encryption algorithm. For each message, the key is chosen randomly from a large number of keys. After the keys are used both sender as well as receiver must use the same private key.

B. Key Management Using Split-Key Encryption.

Split-Key encryption technique protects the keys and guarantees that they remain under customer control and never exposed in storage. This technique requires two keys. The data objects are split into two and the first part is common to all the data objects in the application called the Master Key. Second part is different for all the objects and stored by the Key Management Service provided by the system. System uses both the parts to encrypt and decrypt the data [9].

C. Homomorphic Key Encryption.

Homomorphic encryption is a technique of converting data into cipher text that can be worked upon as if it were still in original form. It allows mathematical operations to be implemented on encrypted data without tampering the encryption allowing the program to do some work on the unreadable data [14].Since in homomorphic encryption the data retains its original structure, identical mathematical operations will yield the same results whether they are performed on encrypted data or decrypted data.

V. ENCRYPTION AND KEY MANAGEMENT

A. THROUGH VMWARE.

Before doing any task you have to make the platform. In same way you need to install VMware workstation [10] and VMware vSphere Client [13]. After installing these two follow the step to get your key for the encrypted data in the cloud.

- Install VMware ESXi server on your Vmware workstation by following the basic steps of its installation [11].
- After installation you will get a DHCP server Id of the ESXi server use this IP address to and username and password of root user entered during ESXi server installation to log in to Vmware vSphere client.
- When the vSphere client is connected to your server go to File > Deploy OVF Template of Porticor vpd and on the next step select the IP address provided and in IP address allocation select DHCP option and click next.
- Once you have created the VM, power on the VM, wait until you see its IP address and then access the URL: *https://VM-address/* (note the use of HTTPS)
- You will now be redirected to the Porticor management application at *pvkm.porticor.com.*
- Create your account if you are not a user or sign in with your existing account. On the next page name your project and click next to initialize your new instance and after finishing a Master key would be generated as show in the following image.

- Save the Master Key and complete your project setup and click on continue to create an encrypted disk.
- Select Network File Storage then Rescan Disk Volumes. After this select the storage type and click protect.
- Click on 'use it' next to storage type selected. To mount the newly created encrypted disk to your application simply copy the mount command.
- Block access to encrypted data by clicking on Lock option.

B. Through Amazon Web Services (AWS) Using Porticor

Amazon is the solely responsible for the infrastructure they provide. However, anything we put on the AWS infrastructure is our responsibility to secure. This is called the shared responsibility model: Amazon provides the infrastructure and secure it, we use the infrastructure and must secure that [15]. For encryption of your data in your own personal cloud environment in amazon web services you should have an account in AWS [12] and follow the following steps to secure your data:

- Open URL *http://porticor.com* create an account if you are not already registered or sign in with your existing account.
- As soon as you login you will see the porticor wizard fill the project name and description and move on to the main wizard page.
- The wizard will assume that you are a current AWS user. Select the Quick Launch option and enter your Amazon credentials and preferred geographical region, as well as instance size.
- After clicking the Next button you will see a progress bar. When the instance is ready you will see the last page of the wizard.
- Press Finish, and it will be redirected to your new appliance. Where you will be provided the project master encryption key for your project instance, save it and porticor project setup will finish, click continue.
- After this you will be redirected to virtual appliance main management screen then click on "Protected File Systems" to create an encrypted disk.
- Enter the disk name and size of the disk and then select the disk type as Network File System (NFS).
- To mount you encrypted disk in your application simply click use it and copy the code into your app server CLI.

VI. Advantages and Challenges of Cloud Security

Cloud Computing can have notable security and reliability advantages. Not least, having data on the cloud can provide significant level of back-up i.e. difficult and time consuming for many users to achieve by any other means. Another security advantage is that cloud computing may significantly reduce the risk of data falling into the wrong hands by encrypting the data stored on it. One of the best security benefit of cloud computing is that it may actually make the personal computing safer as it is far easier to hack a PC than a datacenter. The concerns that arise in cloud computing occurs largely due to lack of knowledge or lack of preparation. It also brings new set of challenges as the organizations storing their data are increasing and as data is stored in offsite locations. However, with proper planning and alertness in selecting a provider, risks can be reduced to a greater extent.

However, the rate at which cloud computing is increasing it may soon significantly increase the security of individual PC's and other devices that supports internet.

Table 1:List of advantages and challenges associated with cloud computing security.

Advantages	**Challenges**
Reduce spending on technology infrastructure.	Disaster recovery
Improve accessibility	Dependence on secure hypervisors.
Guards Your Data	Prone to Attack
Simplification of Compliance Analysis	Encryption needed for secure storage.
Data held by Unbiased cloud vendors	Procuring services on a consumption (on-demand) basis
More Focused Security	Trust and assurance
Security certifications	Isolation
Multifactor authentication	Access control

VII. Conclusion

One of the biggest security worries with cloud computing is the sharing of resources. Cloud providers must inform their customers about the level of security that they are providing in their cloud services. In this paper we discussed about cloud computing, it's various services, network topologies, security issues, methods of encrypting data and key management and finally advantages and challenges of cloud security.

Data security is one of the major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. In this paper we saw how data is encrypted and keys are generated for your application security on cloud through two methods, first through porticor's ovf template using VMware ESXi server and vSphere client and secondly, using your AWS account directly. Data encryption is critical in protecting the security of data at rest in the cloud. But when it comes to the cloud, managing and protecting the encryption keys effectively is as important as encrypting the data. An effective data encryption solution must include:

- Robust, fast, yet easy to use data encryption
- Reliable, cloud-based key management that is cost-effective, but trustworthy
- Key encryption technologies to protect your encryption keys as well as your data – both in storage and in use

We hope this paper helped in better understanding of how keys are generated and encrypted data disk are made for cloud security so that better techniques are developed for a more secure cloud experience for the users.

REFERENCES

[1] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy,"Cloud Computing: Security Issues and Research Challenges".

[2] P. Mell and T. Grance,"The NIST Definition of Cloud Computing Version 15", Information Technology Laboratory, NIST (National Institute of Standards and Technology), October 2009. Available at http://csrc.nist.gov/groups/SNS/cloud-computing

[3]. Cloud Computing articles. http://Interoute.com

[4] Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta, Sagar Bhavsar, Vibha Mittal "Enhanced Security for cloud storage using File Encryption"

[5] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[6] Ma Jun, Wang Zhiying, Ren Jiangchun, Wu Jiangjiang, Cheng Yong and Mei Songzhu," The Application of Chinese Wall Policy in Data Leakage Prevention" in International Conference on Communication Systems and Network Technologies,2012

[7] Ronald L. Krutz, Russell Dean Vines "Cloud SecurityA Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., 2010

[8] Wikipedia "Cloud Computing Security" http://en.wikipedia.org/wiki/Cloud_computing_security

[9] Y Lakshmi Prasanna, Dr.E.Madhusudhana Reddy, S Neelima "A NOVEL TECHNIQUE FOR TRUST DELIVERY IN THE CLOUD" in proceedings of Council of Innovative Research 2013.

[10] Installation of Vmware workstation. https://www.vmware.com/support/ws5/doc/install_ws.html

[11] Installation of Vmware ESXi server. http://blogs.vmware.com/smb/2013/11/back-to-basics-install-vmware-esxi-5-5.html.

[12] Create account on Amazon Web Services at: "http://aws.amazon.com/"

[13] Installation of VMware vSphere client http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2032890

[14] "Homomorphic Encryption and Cloud Security: The Practicalities" article available at: http://www.porticor.com/2014/06/homomorphic-encryption-and-cloud-security

[15] "AWS Security: The Shared Responsibility Model."article available at: http://www.porticor.com/2014/06/aws-security-shared-responsibility-model