ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 2 Issue 4; September-October-2015; Page No.01-06

Security issues and Cryptographic techniques in Cloud Computing

Radhika Patwari[1], Sarita Choudhary[2]

[1] Systems Engineer, Infosys JVWU

[2] M.Tech (Dept. of CS), JVWU

ARTICLE INFO

Received: 01 September 2015
Accepted 19 September 2015

Corresponding Author:

Radhika Patwari

[1]*M.Tech (CSE) student, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan*

ABSTRACT

Cloud computing is an emerging paradigm that provides cheap, on demand resources and services over a network. It has become primary distributed computing platform. It eliminates the need of maintaining costly computing facilities by companies and institutes. One of the barriers for cloud adoption is security. There are no proper laws which govern who own responsibility as data flows across cloud.

This article gives a quick introduction to cloud computing. Then it covers various threats and security issues in today's cloud and cryptographic ways for maintaining security in cloud.

Keywords: cloud computing, security threat, multi-tenant behavior, cryptographic techniques, standards and policies

I. Introduction to cloud

The concept of cloud is not new. Network based computing is evolving for more than 50 years. But the term 'cloud' originated in 1990s. Many believe the first use of "cloud computing" in its modern context occurred in 2006, when then Google CEO Eric Schmidt introduced the term to an industry conference.

It is a virtual environment that provides resources to users and charges only for services they consumed. Most of the things we see and use on internet are cloud, for example email services, google map, online file viewers, online file converter. In brief 'Cloud is metaphor for internet'. Its use is spreading rapidly because it captures a historic shift in the IT industry as more computer memory, processing power, and apps are hosted in remote data centers, or the "cloud."

NIST (National Institute of Standards and Technology) has given official definition for cloud computing according to which a cloud should have these characteristics:

a) Resource pooling - In cloud computing, resources are pooled to serve a large number of customers. Cloud computing uses multi-tenancy where different resources are dynamically allocated and de-allocated according to demand. The resource allocation should be elastic, in the sense that it should change appropriately and quickly with the demand. Sometimes, the terms elastic or utility computing are used to describe this ability of a cloud to provide additional resources when required.

b) Self service and on-demand service - The user should be able to access computing capabilities as and when they are needed and without any interaction from the cloud-service provider.

c) Broad network access - Capabilities are available over the network and accessed through standard mechanisms

d) Rapid elasticity - Capabilities can be elastically provisioned and released, in some cases automatically. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

e) Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

One more important feature of cloud is 'Pay as you go' - The user is billed only for the amount of resources they use.

Amazon's EC2 is one of the best examples. Amazon Elastic Compute Cloud (EC2) allows users to rent virtual computers on which to run their own computer applications. EC2 allows scalable deployment of applications. Each virtual machine, called an "instance", functions as a virtual private server. One EC2 Compute Unit provides the equivalent CPU capacity of a 1.0-1.2

GHz 2007 Opteron or 2007 Xeon processor. Amazon charges about $0.013/hour ($9.7/month) for the smallest "Micro Instance" (t2.micro) virtual machine running Linux or Windows.

AT&T also entered the cloud computing realm when it acquired USinternetworking (USi) in2006. USi was an application service provider for more than 30 countries. In 2008, AT&T introduced Synaptic, which combined USi's five Internet data centers in the US, Europe, and Asia to serve as regional gateways within its cloud. Today, the latest example of cloud computing is Web 2.0; Google, Yahoo, Microsoft, and other service providers now offer browser-based enterprise service applications (such as webmail and remote data backup).

Advantages -

First, expenses are lowered too much for companies. Now companies don't need to purchase computers or hire personnel for maintenance. Every computing facility (softwares), platforms, even whole infrastructure is provided as service virtually. This is especially useful for small startups which don't have much capital to invest.

Second, cloud architecture is very scalable. For example cloud storages can easily manage thousands of GBs of data due to its distributed architecture whereas this task is problematic locally. Finally, there is cloud for everything, storage cloud for storage services, data cloud for data management services and compute cloud for computational services.

Disadvantages -

First, Cloud faces latency and bandwidth related issues because of being remotely hosted. Denial of service is also a threat to cloud computing. DOS has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services. DOS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed.

Then comes the problem of interoperability among cloud services.

Finally security issues are there such as data being accessible to third parties. Possibility of security leakage due to multi-tenancy nature.

II. Interoperability in cloud

Frameworks are yet to be developed that would enable interoperability in cloud. Porting of applications from one cloud to another and interoperating between different cloud services is still a challenge. Users also don't want to get confined to a single cloud provider. Users want freedom to move from private to public cloud and back again.

When you decide to move an application between clouds, several challenges occur:

a) Rebuilding the application in the target cloud.

b) Setting up the network in the target cloud to give the application the support that it had in its original cloud.

c) Setting up security to match the capabilities provided by the source cloud.

d) Managing the application running in the target cloud.

e) Handling data movement and the encryption of data while it is in transit and when it gets to the target cloud.

All this is due to lack of standards for clouds. Every provider implements its own proprietary enhancements to differentiate its wares from other providers. Adoption of universal standards(such as open source) should be there.

Amazon's APIs (www.aws.amazon.com) have become the de facto standard for clouds that provide on-demand instances. Cloud-based applications that use this API enjoy portability and interoperability—for example, Eucalyptus uses these APIs, and applications that run on Amazon's EC2 service can in turn run on a Eucalyptus cloud.

III. Security issues in Cloud

With growing cloud capabilities, security is becoming a major challenge in wide adoption of cloud. Can users fully trust cloud? Is their data safe on cloud? These questions are emerging with no reliable solutions yet. Moreover cloud is becoming particularly attractive to cyber crooks. The cloud faces both internal and external security threats like media failures, software bugs, malware, administrator errors and malicious insiders.

Cloud services hold user's personal data and identity information such as photographs, calendars, address books, medical records, social security numbers, tax documents, financial transactions etc. These data if analyzed properly can tell every aspect of user's life. So significant safeguard is required to protect user's privacy. Consider banks and other financial institutions which process highly sensitive data, if they use cloud high degree of security is required for their data.

For hosted clouds, third party is responsible for storing and securing data. But are third parties trust worthy? Handing over sensitive data to other party is a serious concern. Trusting a third party requires taking the risk of assuming that the trusted third party will act as it is expected (which may not be true all the time). Data exposure risk stays from the level of one individual's data to the whole cloud level.

Data loss is also possible in cloud. The prospect of seeing your valuable data disappear into the ether without a trace. A malicious hacker might delete a

target's data out of spite or data can be lost because of a careless cloud service provider.

The scalable nature of cloud has posed another threat. Cloud service providers share infrastructure, platforms, and applications to provide services. There is no strong isolation. Two companies might be using same piece of hardware without knowledge. If an integral component gets compromised, a shared platform component, or an application, it can expose the entire environment to a potential of compromise and breach to malicious users.

Google was forced to make an embarrassing apology in February when its Gmail service collapsed in Europe, while Salesforce.com is still smarting from a phishing attack in 2007 which duped a staff member into revealing passwords. Still Google and Amazon have infrastructure to deflect a cyber-attack but every cloud doesn't have. When these tech-giants can face security breaches, it is difficult for users to have full confidence in cloud that there data is safe.

Another question comes who is responsible for security of data? Is it only cloud service providers duty or stake holders, business entities are also responsible for maintaining safeguards. Legal decisions will ultimately determine who owns the responsibility for securing information shared within clouds.

IV. Privacy Policies

The cloud is still very much a new frontier with very little in the way of specific standards for security or data privacy. In terms of legislation there is nothing. Although it might be too early yet for standards to fully emerge, several organizations are attempting them, including an effort by the Cloud Computing Interoperability Forum (www.cloudforum.org/) and by the Open Cloud Consortium (www.opencloudconsortium.org).

IBM, Cisco, SAP, EMC and several other leading technology companies announced that they had created an 'Open Cloud Manifesto' calling for more consistent security and monitoring of cloud services. But the fact that neither Amazon.com, Google nor Salesforce.com agreed to take part suggests that broad industry consensus may be some way off. Microsoft also abstained, charging that IBM was forcing its agenda.

Nevertheless till standards for cloud come into force, several measures can be taken by companies and cloud users on their part-

Service Providers:

a) Companies need to be vigilant, for instance about how passwords are assigned, protected and changed.

Cloud Users:

a) Cloud service providers typically work with numbers of third parties, and customers are advised to gain information about those companies which could potentially access their data.

b) Companies should ask to see service provider's reliability reports to determine whether these meet the requirements of the business.

c) Find out about the hosting company used by the provider and if possible seek an independent audit of their security status.

Also there are a handful of existing web standards which companies in the cloud should know about. Chief among these is ISO27001, which is designed to provide the foundations for third party audit, and implements OECD principles governing security of information and network systems. It provides requirements for an information security management system (ISMS).

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure.

The SAS70 auditing standard is also used by cloud service providers. A service auditor's examination performed in accordance with SAS No. 70 represents that a service organization has been through an in-depth examination of their control objectives and control activities, which often include controls over information technology and related processes.

National Institute of Standards and Technology (NIST) has taken step in standardization of cloud related policies. It has given official definition, characteristics of cloud to some extent. NIST aims to foster cloud computing systems and practices that support interoperability, portability, and security requirements that are appropriate and achievable for important usage scenarios. NIST scientists are involved in cloud-related international standards committees and lead a number of public working groups to solve cloud-related challenges. For further information on security standards by NIST see (http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf)

V. Cryptographic techniques for security in cloud

Many security methods for cloud use various cryptographic techniques. Cryptographic techniques have become essential for security in cloud. A key is used for data encryption and decryption. This helps in protecting confidentiality and integrity of data. It ensures security of data being shared in cloud and also allows data to be stored securely.

Cryptography refers to the science of designing ciphers. Encryption refers to the method of converting plain text to secret text (cipher text) which can only be read by owner of secret key. At present various cryptographic algorithms are there which belong to two major categories -

a) Symmetric algorithms such as DES, AES, Triple DES
b) Asymmetric or public-key encryption algorithms such as RSA, Diffie-Hellman, ECC, etc.

The difference is in the way the keys are used. In symmetric key encryption, the person who is sending the data and the person who is receiving the data share a key which is kept secret. This is then used to encrypt and decrypt the messages. In asymmetric key encryption, two keys are involved wherein one is used for encryption (this is publicly available) and the other is used for decryption (this is kept secret).

Identity based encryption -

Identity-based encryption (IBE), is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). It allows any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. This kind of encryption reduces the complexity of the encryption process for both users and administrators.

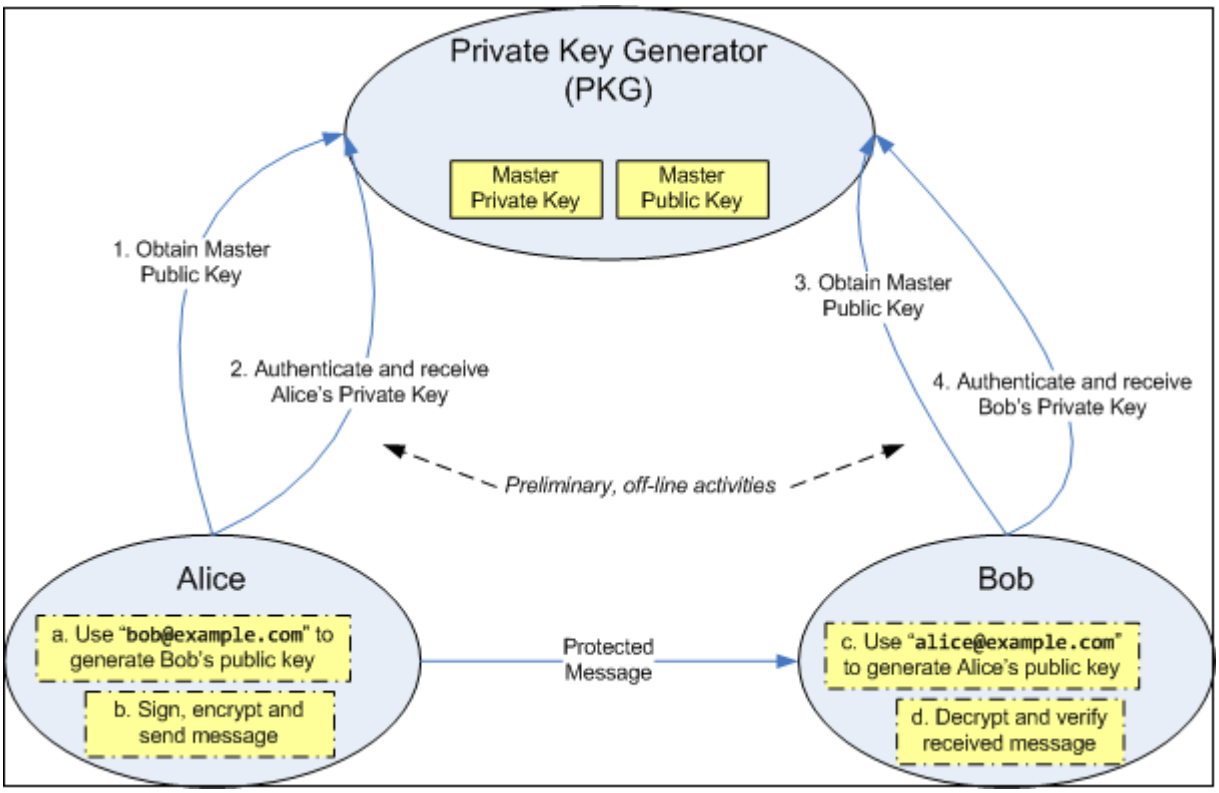

Figure 1: Identity based Encryption

Attribute based encryption -

It is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). A user can encrypt a message under a public key and a policy. Decryption will only work if the attributes associated with the decryption key match the policy used to encrypt the message.

Fully Homomorphic Encryption -

Homomorphic encryption ensures privacy of data in communication, storage or in use with tools similar to conventional cryptography, but with extra features of computing over encrypted data, searching an encrypted data, etc. Search and manipulation of cipher text was difficult with traditional encryption techniques.

Intelligent Encryption -

Conventional public-key and shared-key encryption systems rely on standard protocols and a pre-established public key certification infrastructure (public key infrastructure), allowing people all over the world to use encryption according to standard methods. But in conventional cryptographic methods only one person, i.e., owner of the key can view original data. This creates problem in case of cloud where number of users are there to access same data. Intelligent encryption works on basis of various conditions. It allows various users to view encrypted data based on certain conditions rather than only single authorized user. It is similar to attribute based encryption but conditions are extended for multiple users.

Consider a situation where access to confidential information is managed within a company. Conditions for viewing the information are incorporated into the cipher text, and attribute information is applied to the decryption key so that decryption is possible only with a

key that matches these conditions. If the data is encrypted with embedded conditions such as "[Director] OR [Personnel department AND Section manager]", then it can be decrypted with a key containing the attributes [Personnel department, Section manager], but not by a key containing the attributes [Personnel department, Section #1, Employee]. In this way number of users satisfying condition can get view original text.

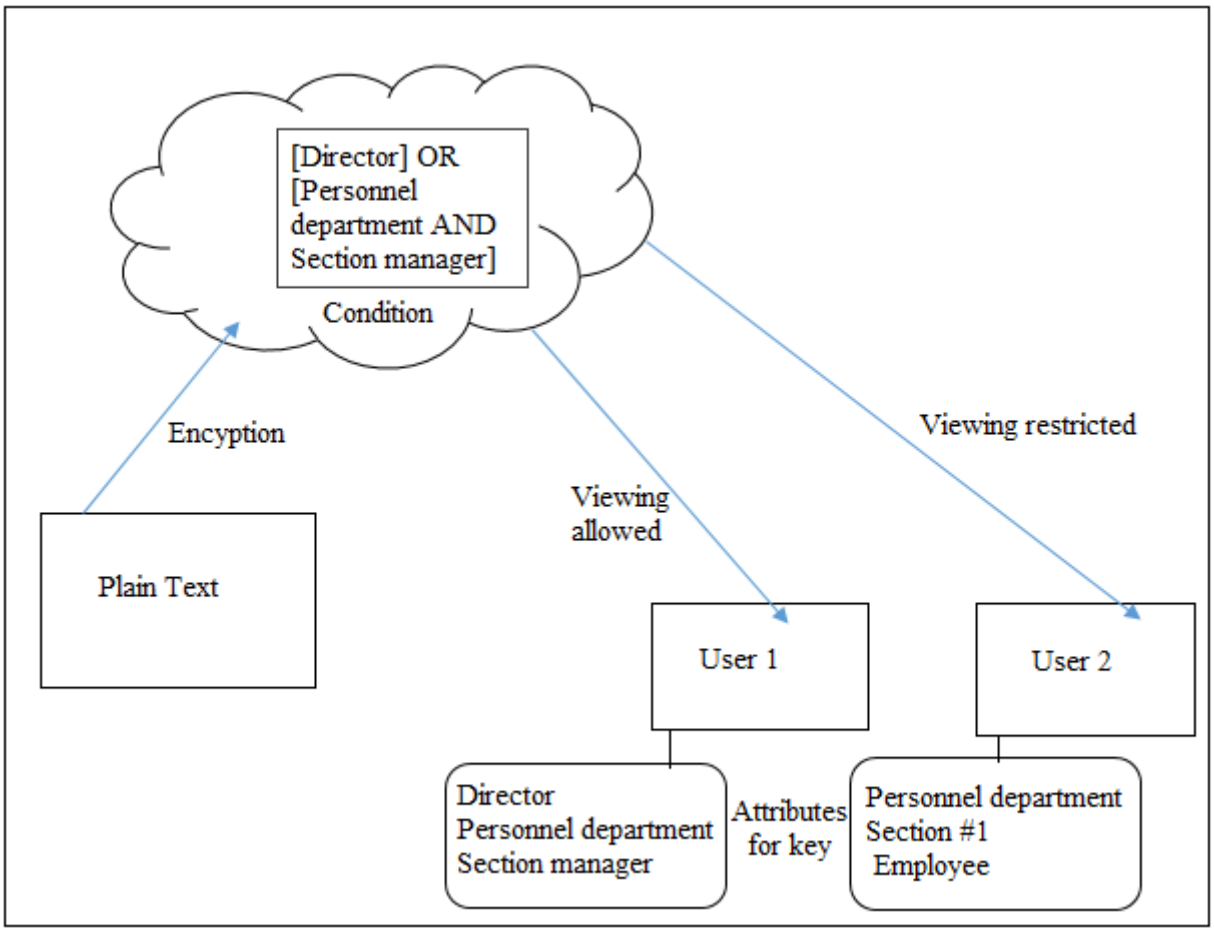

Figure 2: Intelligent Encryption

Cloud-managed-key -

The one more possible threat with conventional cryptographic methods can be letting users manage their decryption keys themselves. Further if a user has no longer permissions to access data, he still can decrypt data if he has key. A possible solution for this problem can be a cryptographic scheme where key is managed by cloud. It solves the issue of key management in public key cryptography. In this scheme decryption keys for public key cryptography are managed in the cloud and the decryption processing is securely outsourced to the key management cloud. This allows users to make use of encrypted data without having to manage the decryption keys. Since the decryption processes can be enabled or disabled on the basis of authentication by the key management cloud, it is also possible to enable or disable the reading of a previously distributed cipher text at a later time.

Benefits of cryptographic cloud storage and security -

a) In a cryptographic service, the data is encrypted on premise by the data processor(s). This way, customers can be assured that the confidentiality of their data is preserved irrespective of the actions of the cloud storage provider.

b) It can be difficult to ascertain exactly where one's data is being stored once it is sent to the cloud (i.e., many service providers have data centers deployed throughout the world). So some customers may be reluctant to use a public cloud for fear of increasing legal exposure for their data. In a cryptographic storage service data is only stored in encrypted form so any law that pertains to the stored data has little to no effect on the customer.

VI. Conclusion

Privacy and security in cloud can be said to be achieved when users have control over information they want to reveal to cloud and who can access their information. Without guarantee of security and privacy users can't make shift to cloud only on the basis of lower cost and faster computing. Certain cloud related standards and cryptographic methods for security are coming to

existence, still there is long way to go for public cloud to become a trustworthy computing environment.

References

1. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa3.html
2. https://en.wikipedia.org/wiki/ID-based_encryption
3. W. Sobel et al., "Cloudstone: Multi-Platform Multi-Language Benchmark and Measurement Tools for Web 2.0," *Proc. Cloud Computing and Its Applications*, 2008; www.cca08.org/papers.php.
4. http://msr-waypoint.com/pubs/112576/crypto-cloud.pdf?bcsi_scan_ac85d4f4ee253e53=0&bcsi_scan_filename=crypto-cloud.pdf
5. http://www.ijcsit.com/docs/Volume%206/vol6issue02/ijcsit2015060233.pdf
6. https://en.wikipedia.org/wiki/Attribute-based_encryption