Investigation of Security in Cloud Computing

Annu Devi

MERI College of Engineering & Technology, Rohtak, MDU, Haryana, India

Abstract: ***Cloud computing becomes more widely prevailed storage for outsourced data which may contain more sensitive information such as credit card numbers, passwords, e-mails, personal health records etc. As the data owners cannot risk their unencrypted outsourced data so as the cloud servers. The cloud server may fail to keep up the integrity of the cloud data due to hacking or entry of unauthorized entities. The increased attack surface in a in a Cloud environment allows for other vulnerabilities to be exploited, thereby increasing the organization's risk. While Cloud services offer flexibility, scalability and economies of scale, there have been commensurate concerns about security. As more data moves from centrally located server storage to the Cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at risk if appropriate measures are not put in place prior to selecting a Cloud vendor or implementing your own cloud and migrating to Cloud services. Cloud services such as Software as a service, Platform as a service or Infrastructure as a service will each have their own security concerns that need to be addressed. This paper reviews the best practices to secure Cloud services and data, including conventional security techniques and working with vendors to ensure proper Service Level Agreements exist.***

Keywords: Cloud Computing, Encryption, Decryption, Threats, Public key, Private key, Cryptography

1. Introduction

In computer networking, cloud computing is computing that involves a large number of computers connected through a communication network such as the Internet, similar to utility computing. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time.

Network-based services, which appear to be provided by real server hardware and are in fact served up by virtual hardware simulated by software running on one or more real machines, is often called cloud computing. Such virtual servers do not physically exist and can therefore be moved around and scaled up or down on the fly without affecting the end user, somewhat like a cloud becoming larger or smaller without being a physical object.

Cloud computing exhibits the following key characteristics:

- ○ **Agility** improves with users' ability to re-provision technological infrastructure resources.
- ○ **Application programming interface** (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs.
- ○ **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
  - ○ **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.
  - ○ **Multitenancy** enables sharing of resources and costs across a large pool of users thus allowing for: centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
  - ○ **Peak-load capacity** increases (users need not engineer for highest possible load-levels)
  - ○ **Utilization and efficiency** improvements for systems that are often only 10–20% utilized.
- **Performance** is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Productivity** may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed.
- **Reliability** improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- **Scalability and Elasticity** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, OS and cloud providers), without users having to engineer for peak loads.
- **Security** can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels.
- **Virtualization** technology allows sharing of servers and storage devices and increased utilization. Applications can be easily migrated from one physical server to another.

2. Existing Security System for Cloud Server

The methods to ensure information security that apply to the traditional data center consisting of racks of physical servers also apply to the virtual world.

Platt defines three categories of information security:

1) Logical Security
2) Physical Security
3) Premises Security (Platt, 2009)

- Physical security protects the infrastructure, building and physical access to the data center.
- Premise security protects the people and property within the data center.
- It is important to ensure adequate physical security in is in place.

Encrypting Data in Motion

Data in motion to and from the CSP is no different than data in motion when using the Internet for other business needs when data in transit needs to remain confidential. However, it is incumbent upon the consumer to ensure data within the CSP infrastructure moves within and between their data centers in a secure manner.

Cryptography

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)
2) **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3) **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4) **Authentication** (the sender and receiver can confirm each other’s identity and the origin/destination of the information) Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

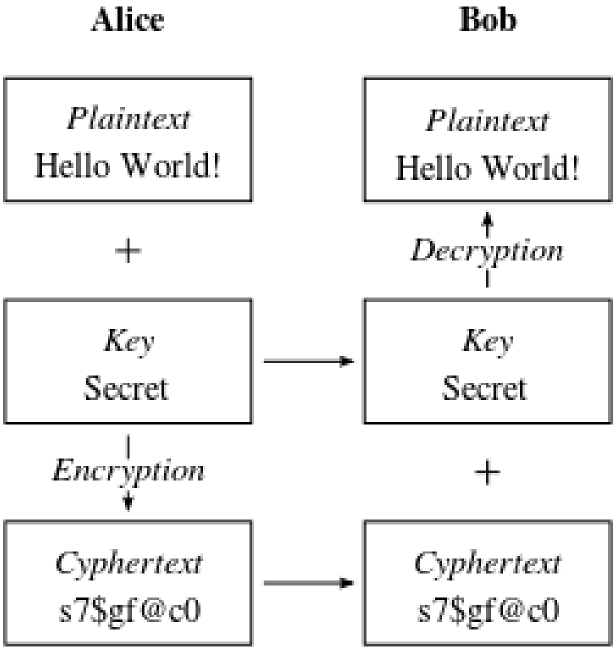

Figure 1: Cryptography

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

Common Cryptographic Algorithms

There are two basic kinds of encryption algorithms in use today:

- Private Key cryptography, which uses the same key to encrypt and decrypt the message. This type is also known as symmetric key cryptography.
- Public key cryptography, which uses a public key to encrypt the message and a private key to decrypt it. The name public key comes from the fact that you can make the encryption key public without compromising the secrecy of the message or the decryption key. Public key systems are also known as asymmetric key cryptography.

Private Key cryptography is most often used for protecting information stored on a computer's hard disk, or for encrypting information carried by a communications link between two different machines. Public key cryptography is most often used for creating digital signatures on data, such as electronic mail, to certify the data's origin and integrity.

This analysis gives rise to a third kind of system:

- Hybrid public/private cryptosystems. In these systems, slower public key cryptography is used to exchange a random session key, which is then used as the basis of a private key algorithm. (A session key is used only for a single encryption session and is then discarded.) Nearly all practical public key cryptography implementations are actually hybrid systems.

Private Key Systems

The following list summarizes the private key systems in common use today.

DES: The Data Encryption Standard (DES), an encryption algorithm developed in the 1970s by the National Bureau of Standards and Technology (since renamed the National Institute of Standards and Technology, or NIST) and IBM. DES uses a 56-bit key.

Commonly Used Private and Public Key Cryptography Algorithms	
Algorithm	**Description**
Private Key Algorithms:	
ROT13	Keyless text scrambler; very weak.
crypt	Variable key length stream cipher; very weak.[12]
DES	56-bit block cipher; patented, but freely usable (but not exportable).
RC2	Variable key length block cipher; proprietary.
RC4	Variable key length stream cipher; proprietary.
RC5	Variable key length block cipher; proprietary.
IDEA	128-bit block cipher; patented.
Skipjack	80-bit stream cipher; classified.
Public Key Algorithms	
Diffie-Hellman	Key exchange protocol; patented.
RSA	Public key encryption and digital signatures; patented
ElGamal	Public key encryption and digital signatures; patented.
DSA	Digital signatures only; patented.

IDEA: The International Data Encryption Algorithm (IDEA) developed in Zurich, Switzerland by James L. Massey and Xuejia Lai and published in 1990. IDEA uses a 128-bit key, and is believed to be quite strong. IDEA is used by the popular program PGP (described later in this chapter) to encrypt files and electronic mail. Unfortunately,[11] wider use of IDEA may be hampered by a series of software patents on the algorithm which is currently held by Ascom-Tech AG, in Solothurn, Switzerland. Ascom-Tech supposedly will allow IDEA to be used royalty free in implementations of PGP outside the U.S., but concerned users should verify the terms with Ascom-Tech or their licensees directly.

Public Key Systems

The following list summarizes the public key systems in common use today:

DSA: The Digital Signature Algorithm developed by NSA and adopted as a Federal Information Processing Standard (FIPS) by NIST. Although the DSA key may be any length, only keys between 512 and 1024 bits are permitted under the FIPS. As specified, DSA can only be used for digital signatures, although it is possible to use DSA implementations for encryption as well. The DSA is sometimes referred to as the DSS, in the same manner as the DEA is usually referred to as the DES.

Following table lists all of the private and public key algorithms we've discussed:

Threats and opportunities of the cloud

Critical voices including GNU project initiator Richard Stallman and Oracle founder Larry Ellison warned that the whole concept is rife with privacy and ownership concerns and constitute merely a fad.

However, cloud computing continues to gain steam with 56% of the major European technology decision-makers estimate that the cloud is a priority in 2013 and 2014, and the cloud budget may reach 30% of the overall IT budget. According to the TechInsights Report 2013: Cloud Succeeds based on a survey, the cloud implementations generally meets or exceeds expectations across major service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Privacy

The increased use of cloud computing services such as Gmail and Google Docs has pressed the issue of privacy concerns of cloud computing services to the utmost importance. The provider of such services lies in a position such that with the greater use of cloud computing services has given access to a plethora of data. This access has the immense risk of data being disclosed either accidentally or deliberately.

Privacy Solutions

Solutions to privacy in cloud computing include policy and legislation as well as end users' choices for how data is stored. The cloud service provider needs to establish clear and relevant policies that describe how the data of each cloud user will be accessed and used. Cloud service users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.

Security in the Cloud

Security in the world of information technology has become a popular topic within the industry and within the media. It is not uncommon to read about successful hacker exploits against consumers, business or government. The standard definition of risk by the ISO is, “the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. The increased attack surface in a in a Cloud environment allows for other vulnerabilities to be exploited, thereby increasing the organization’s risk.

3. Proposed Model and Its Implementation

An Digital library (colloquially referred to as a electronic library) is a focused collection of digital objects that can include text, visual material, audio material, video material, stored as electronic media formats (as opposed to print, microform, or other media), along with means for organizing, storing, and retrieving the files and media contained in the library collection. Digital libraries can vary immensely in size and scope, and can be maintained by individuals, organizations, or affiliated with established physical library buildings or institutions, or with academic institutions. The electronic content may be stored locally, or accessed remotely via computer networks. An electronic library is a type of information retrieval system.

Digital books would be encrypted. Encrypted files would be stored on Server. When used download it then user has to decrypt file before reading it. The decryption key would be available to user after making payment.

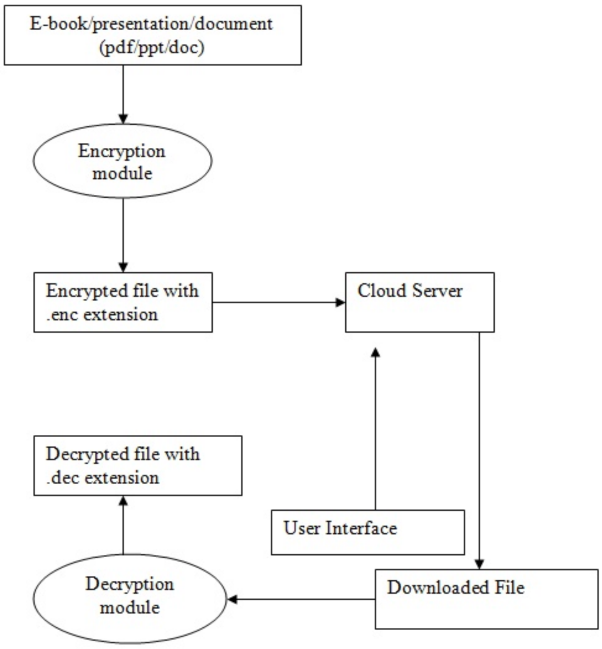
E-book/presentation/document (pdf/ppt/doc)
Encryption module
Encrypted file with .enc extension
Cloud Server
Decrypted file with .dec extension
User Interface
Decryption module
Downloaded File

Figure 2: Encryption and Decryption

3.1 File Encryption module in java

```
public void encrypt() throws Exception{
 //opening streams
 FileInputStream fis =new FileInputStream(file);
 file=new File(file.getAbsolutePath()+".enc");
 FileOutputStream fos =new FileOutputStream(file);
 //generating key
 byte k[] = "HignDlPs".getBytes();
 SecretKeySpec key = new
SecretKeySpec(k,algo.split("/")[0]);
 //creating and initialising cipher and cipher streams
 Cipher encrypt = Cipher.getInstance(algo);
 encrypt.init(Cipher.ENCRYPT_MODE, key);
 CipherOutputStream cout=new CipherOutputStream(fos,
encrypt);

 byte[] buf = new byte[1024];
 int read;
 while((read=fis.read(buf))!=-1) //reading data
 cout.write(buf,0,read); //writing encrypted data
 //closing streams
 fis.close();
 cout.flush();
 cout.close();
 }
```

3.2 File Decryption module in java

```
 public void decrypt() throws Exception{
 //opening streams
 FileInputStream fis =new FileInputStream(file);
 file=new File(file.getAbsolutePath()+".dec");
 FileOutputStream fos =new FileOutputStream(file);
 //generating same key
 byte k[] = "HignDlPs".getBytes();
 SecretKeySpec key = new
SecretKeySpec(k,algo.split("/")[0]);
 //creating and initialising cipher and cipher streams
 Cipher decrypt = Cipher.getInstance(algo);
 decrypt.init(Cipher.DECRYPT_MODE, key);
 CipherInputStream cin=new CipherInputStream(fis,
decrypt);

 byte[] buf = new byte[1024];
 int read=0;
 while((read=cin.read(buf))!=-1) //reading encrypted data
 fos.write(buf,0,read); //writing decrypted data
 //closing streams
 cin.close();
 fos.flush();
 fos.close();
 }
```

4. Result

Business and government will continue to move a Cloud environment in an effort to reduce costs, improve efficiencies and reduce administrative overhead. Delivering IT services via the Cloud portends to be a time saver, a money saver and allow for better efficiencies. This new paradigm of computing offers many benefits but it also increases security risks.

The delivery of computing resources in a Cloud environment is elastic, available on demand and convenient for the customer. While not mandatory, virtualization of the data center is important to achieve economies of scale that enable services to be provided at a lower cost than a traditional data center. While virtualization reduces some security risks, others are increased because the attack surface in a Cloud service increases. Traditional security methods are still relevant in the Cloud but are implemented in a virtual means.

Data is protected by traditional means such as physical security, encrypting the data at rest and data in motion. Data in motion is still sent across the wire using SSL but encrypting data in the Cloud's virtual data center presents challenges. Cloud Service Providers cannot process encrypted data in the virtual data center so the data must be encrypted locally then transmitted. However, homomorphic encryption may be a solution to the encryption challenge but is not likely to be a feasible solution for several years.

References

[1] Amazon. (2011). Amazon Web Services: Overview of Security Processes. Retrieved from
[2] http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
[3] Arora, P., Biyani, R. and Dave, S. (2011). To the cloud:Cloud powering an enterprise. McGraw-Hill. Buck, K. and Hanf, D. (2009).
[4] Mitre cloud computing series, Cloud SLA considerations for the government consumer. Retrieved from
[5] http://www.mitre.org/work/tech_papers/2010/10_2902/cloud_sla_considerations_government.pdf
[6] CBS News Staff. (2012, June 7). CBS News. Retrieved from:
[7] http://www.cbsnews.com/8301-501465_162-57448965-501465/eharmony-suffers-password-breach-on-heels-of-linkedin/
[8] Cisco. (2012). Cisco asa 1000V cloud firewall data sheet. Retrieved from
[9] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps12233/data_sheet_c78-687960.pdf

Author Profile

Annu Devi has done B. Tech from PTU in 2010 and now perusing M. Tech from MERI College of Engineering and Technology.