IDENTITY BASED SECURE AND CONFIDENTIAL MECHANISM IN CLOUD COMPUTING ENVIRONMENT

Khin Lay Mon
University of Computer Studies, Mandalay
Khinlaymon.tk@gmail.com

ABSTRACT

Cloud computing is a typical example of distributed computing. Three broad categories of cloud service are infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or software-as-a service (SaaS). This paper focuses on the SaaS services provided by the Cloud service providers (CSP). The issue with SaaS is data security and confidentiality that makes the cloud user reluctant towards the cloud services. Data confidentiality can be achieved by encrypted outsourced content before outsourcing to cloud servers. This system provides a secure and confidential mechanism by using identity based session key generation and a hybrid cryptographic technique in cloud computing environment. This system especially includes two encryptions and two decryptions as a hybrid approach by using the combination of Tripe-DES and RSA public key encryption. The nature of the system is well suited for distributed nature of cloud servers for an efficient processing with greatly enhanced user's confidence in cloud computing.

Keywords: *Data security, Cloud computing, Distributed computing, Software as a service.*

1. INTRODUCTION

Cloud computing is emerging as a key computing platform for sharing resources that include software, infrastructure, application, and business process. Cloud computing has recently emerged as a new paradigm for hosting and delivering services over the Internet. With this emerging trend a organization can start with small resources and increase only when there is a increase in service demand [5] [6]. Thus, a cloud model promotes availability and is composed of five essential characteristics: (1) On-demand self-service, (2) Metered service (3) Ubiquitous network access, (4) Location-independent resource pooling, (5) Rapid expansion, [2].

Cloud is designed to be available everywhere, all the time. By using the feature like geo-replication and redundancy, services are available even during hardware failures including full data center failures. Cloud services offer three types of deployment models such as Public Cloud, Private Cloud and Hybrid Cloud [8].

Several IT experts have classified cloud computing vendors into three broad categories based on the fundamental nature of the cloud-based solution: infrastructure-as-a-service, platform-as-a-service, or software-as-a service.

The aim of this work is to focus on SaaS services (Software as a service) in which the owner's data is under the control of some third party cloud service provider (CSP). In order to make data confidentiality, a mechanism is proposed here that provide storage of encrypted data on remotely located servers with maximum possible security and with acceptable performance in group communication. In order to protect the access to data, the system proposes to combine both symmetric and asymmetric public key cryptography. In order to implement the system, RSA algorithm is used for key encryption and Triple-DES algorithm is used for file encryption. The key idea of the framework is that it combines symmetric and asymmetric data encryption to ensure data confidentiality and privacy while transferring distributed data files. This system can especially support data confidentiality in cloud computing environment.

2. RELATED WORK

A hybrid algorithm is proposed to combine both the symmetric key algorithm of AES and asymmetric key algorithm of Elliptic Curve

Cryptography (ECC). This hybrid algorithm provides the integrity of data using MD5 algorithm [4].

Qin Liu et al. investigate the characteristics of cloud storage services and propose a secure and privacy preserving keyword searching (SPKS) scheme, which allows the CSP to participate in the decipherment, and to return only files containing certain keywords specified by the users, so as to reduce both the computational and communication overhead in decryption for users, on the condition of preserving user data privacy and user querying privacy [7].

This paper includes the implementation of the hybrid approach: symmetric and asymmetric algorithms. This system can achieve fast encryption speed and provide data confidentiality.

3. CLOUD COMPUTING

In Cloud Computing, services providers will provide the storage for data along with services. Cloud is designed to be available everywhere, every time. Cloud services offer three types of deployment models and services:

Public Cloud: Public clouds or hosted clouds are external or publicly available environments that are accessible to multiple tenants.

Private Cloud: Private clouds are typically custom-made with dedicated virtualized resources for the particular organizations. It also refers to internal data centers, not available to general public.

Hybrid Cloud: Hybrid clouds are the combination of both public as well as private cloud and tailored for a particular group of customers. [1].

Software-as-a-Service (SaaS): In this type of a cloud computing model, a provider's made software runs on a hardware cloud infrastructure and it is allowed to access by the customers with the help of a thin client interface such as a Web browser.

Platform-as-a-Service (PaaS): PaaS allows customers to use programming environments of service provider to access and utilize additional application building blocks.

Infrastructure-as-a-Service (IaaS): This type of service is very useful for small enterprises that are not in position to invest for infrastructure. When a vendor rents out infrastructure components on demand—such as servers, storage components, file systems, virtualization technologies, and network hardware—the vendor is delivering an IaaS service.

3.1. Cloud Storage Techniques

Cloud computing is a typical example of distributed computing paradigm where the data are stored on cloud servers. In cloud data storage, a user stores his data through a Cloud Service Provider (CSP) into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Instead of storing information to computer's hard drive or other local storage device, data owner saves it to a remote database. Cloud storage has several advantages over traditional data storage. For example, data stored on a cloud storage system, user can get that data from any location that has Internet access. No need to setup a new infrastructure to cater the increasing demand of a user. It brings convenience to the user at the same time and removes threat to the privacy of data. A common approach to data protection is to encourage users to store their encrypted data on servers. However, as the amount of encrypted data in the cloud grows, retrieval becomes problematic. One component of cloud infrastructure is the data center, which provides safe, reliable data services. Searching over the distributed nature of data is not an easy task and requires special attention. It may be stored in multiple computers located in the same physical location, or may be dispersed over a network of interconnected computers. In such a system, responsibility for data management is delegated to the distributed file system such as NFS, Netware, LAN-Manager, and AFS (Andrew File System) and its operational staff.

3.2. Software as a Service

SaaS is a model of software deployment whereby a provider licenses an application to customers for use as a service. The SaaS model of software application delivery has a multi-tenant architecture that allows numerous customers to operate out of a single software application. SaaS offers companies potential options to reduce internal resources and

expenses reserved to application maintenance, version updates and patching. Once an existing application is moved to the vendor, the overall IT spending can be reduced. The newly available internal resources are then free to be allocated toward other internal operations priorities [5].

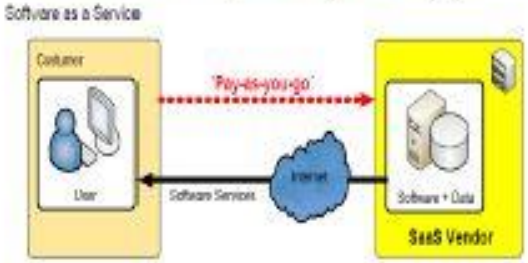

Figure 1: SaaS

3.3. Architecture Of a Cryptographic Storage Service

To ensure the privacy and confidentiality of sensitive data, a user herself may encrypt the sensitive data before uploading the data into cloud data storage. In order to store user's encrypted data, cryptographic storage required in a cloud environment. The advantage of cryptographic storage is that no unauthorized users would be able to access the data until some kind of permission is granted by the owner of data.

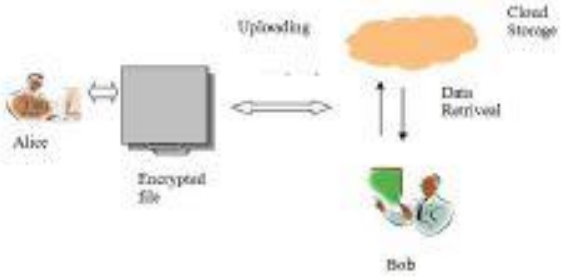

Figure 2: Cloud Cryptographic Architecture

The architecture consists of the following components: a Session key generation, Key encryption, Data Encryption (DE), that process and encrypt data before it is sent to the cloud, and Data Decryption (DE), that enables to download files from cloud providers. Cryptographic storage is an important aspect of cloud services for building trust in cloud vendors. Secure encryption and distributed data make documents random, unreadable and difficult to search by users of cloud.

4. DATA SECURITY

Data security is the core of cloud computing security problems. Data security is mainly about the data confidentiality, integrity, availability and so on. As cloud computing brings with it new deployment and associated adversarial models and vulnerabilities, it is imperative that security takes center stage [7].

This is especially true as cloud computing services that are being used for e-commerce applications, medical record services, and back-office business applications, which require strong confidentiality guarantees with secure and efficient retrieval mechanism. The infrastructure provider, in this context, must achieve the following objectives [2]: Confidentiality and Audibility.

4.1. Davies Meyer Hash Function

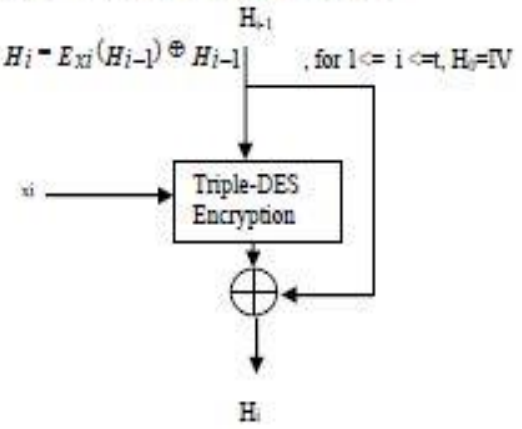

Figure 3: Davies Meyer Hash Function

The Davies Meyer compression function makes a simple use of the underlying block cipher Triple-DES in figure (1). The input block x_i serves as the key to Triple-DES. Thus, the block size of x_i must match the expected key size of the specific block cipher.

The previous hash-value H_i serves as the plaintext to be handled with appropriate bit-length.

The output H_i is then concatenated with the previous output H_{i-1} with the aid of the Exclusive-OR operator. Triple-DES serves as encryption function. The final output H_i is defined by the iterated formula [9].

4.2. Identity Based Session Key Generation

In this paper, Davies Meyer hash function is used to generate one time session key. The user ID is used as the input key of the Triple-DES encryption. The content will be applied to Hash function as the initial value. The resulting output is 128-bits session key for secure system.

4.3. Triple-DES Encryption Algorithm

Triple- DES variant was developed after it became clear that DES by itself was too easy to crack. Triple-DES is a symmetric cryptosystem. Triple-DES is designed to operate on 192 bit blocks of data. A block is transformed into an encrypted (192 bit) block of output in 48-rounds. The required key length is 192 bits. Triple-DES has an effective key length of 168 bit [10].

Triple-DES is a block cipher and is widely used in various cryptographic techniques. It operates on the Encryption- Decryption –Encryption (EDE) modes, which uses sequentially first DES encryption, the DES decryption, and last DES encryption, which the support of three different keys. This system follows encrypt-decrypt-encrypt. It is so called EDE sequence and is defined as follow:

$$C = E\,k_1\,[D\,k_2\,[E\,k_1\,[P]]]$$

$$P = D\,k_1\,[E\,k_2\,[Dk_1[C]]]$$

The total keys length is 3 * 64 = 192 bits. The Decryption operation of the Triple – DES is performed such as DED mode [3].

4.4. RSA Public Key Algorithm

Ron Rivest, Adi Shamir, and Leonard Adleman invented the RSA algorithm in response to the ideas proposed by Hellman, Diffie, and Merkel. This algorithm was the first publicly available public-key cryptosystem in the world and despite its security being unproven; confidence in it has risen over years of cryptanalysis. Because of this, it has subsequently become the most widely used cryptosystem in the world [10].

The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. RSA uses two separate keys for encryption and decryption. One key is made public, enabling anyone to send the message to the holder of the corresponding private key and allow the holder to decrypt the message with this private key. RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n. A typical key length of RSA for a secure transmission is 1024 bit or 309 decimal digits.Here are RSA algorithm.

For encryption Plain text message M,

$$C = M^e \bmod n$$

For decryption Cipher text C,

$$M = C^d \bmod n = (M^e)^d \bmod n$$

Key generation algorithm

- Choose two distinct prime numbers p and q and compute $n = p * q$
- Compute $\Phi = (p-1)(q-1)$
- Choose an integer e, $1 < e < \Phi$, such that $\gcd(e, \Phi) = 1$
- Compute the secret exponent d, $1 < d < \Phi$ such that $ed = 1 \pmod{\Phi}$
- The public key is (n, e) and the private key is (n, d).

The values of p, q and Φ should also be kept secret. Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus , this is a public key encryption algorithm with a public key of $KU = \{e, n\}$ and a private key of $KR = \{d, n\}$.

In this system, RSA algorithm is used for encryption session key.

5. THE SYSTEM'S ACTIVITIES

In Cloud Computing, services providers will provide the storage for data along with services. But due the lack of proper security policies, many business companies are reluctant to adopt the Cloud Computing technology.

This paper has been written to highlight cloud security. In the framework of the system, the user will firstly encrypt the sensitive data before

uploading the data. In order to store user's encrypted data, cryptographic storage require in cloud environment and will include the session key generation, key encryption and data encryption and decryption for data confidentiality as follow:

1. **Session Key Generation**: The first step is to generate one time session key by using Meyer hash function.
2. **Key Encryption**: The next step is to encrypt the session key using RSA public key algorithm.
3. **Data Encryption**: The given file will be encrypted before uploading to a third party service provider using the Triple-DES secret key encryption.
4. **Data uploading**: Encrypted data (Text and secret key) can be uploaded to the remote servers. Encrypted data in the control of service provider are now safe from the service providers and malicious users.
5. **Decryption**: Only legitimate users can download and decrypt the desired file the remote servers.

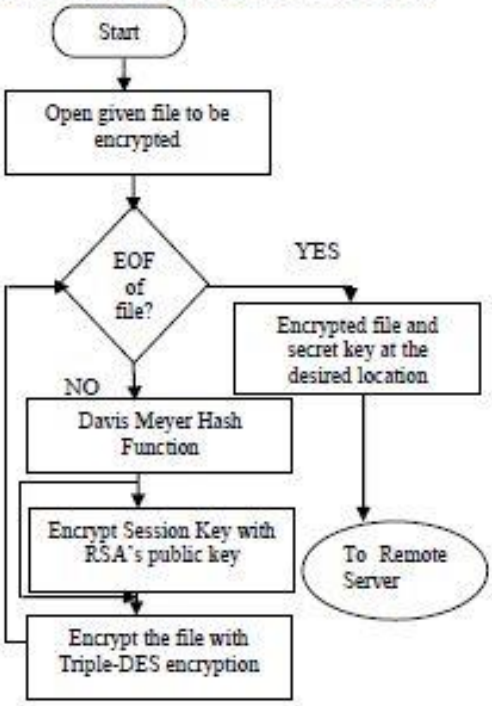

Figure 4: Encryption and file uploading process

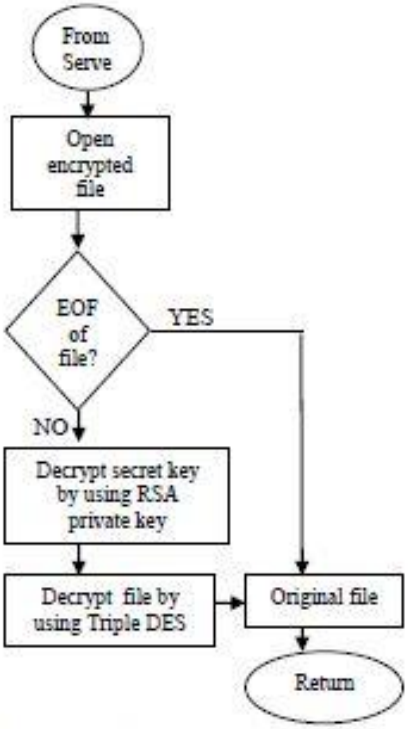

Figure 5: Decryption of encrypted file downloaded from the cloud server

Figure 5: Encrypted data with the hybrid cryptographic techniques

The system provides data confidentiality while solving the key distribution problem of symmetric encryption. The system consists identity-based session key generation, double encryption and decryption components. The issue of Cloud computing is Data confidentiality.

The system is a secure and robust cryptographic technique from inside or outside intruders. To operate with the system, the user has to do key generation, data encryption and key encryption before uploading files to the cloud.

6. CONCLUSION

In order to achieve the confidentiality, encryption techniques are used in a cloud environment. The system provides to enhance data security and confidentiality in a secure manner.

Symmetric cipher has key distribution problem. Public key cryptography solves that problem. All known public key algorithms are much slower than symmetric key algorithms. It would not be practical to use a public key algorithm to encrypt large amount of information. However, that problem can easily be overcome by the combining public key cipher with a fast symmetric cipher. Therefore, the system can especially support an effective encryption technique for the cloud computing environment.

7. FUTHER WORK

Data confidentiality can be achieved by encrypted outsourced content before outsourcing to cloud servers. But due to excessive computation of existing cryptographic algorithms and distributed nature of cloud computing, there is a need of a light weight cryptographic technique that has less computational overhead and high throughput. In the future, overall performance of existing encryption techniques for a small amount of data is comparatively less due to long key size and high degree of calculations. The methods need to provide an equal challenge as other encryption algorithms with less number of bits used for the secret key. The encryption technique is less computational and provides higher speed in a secure manner. The key management for the sharing of the secret key between the two parties can be also efficiently handled. The enormous overhead due to the large key size has been effectively ruled out. Due to a small key size and gained knowledge from literature survey the power consumption very less as compared to existing algorithms.

REFERENCES

[1] Anthony T. Velte, Toby J. Velte Robert Elsenpeter —Cloud Computing A Practical Approachl Tata McGRAW-HILL EDITION, pp 35.

[2] Bo Zhang et al., —An efficient public key encryption with conjunctive-subset keywords searchl, Elsevier Journal of Network and Computer Applications 34 (2011) 262–267.

[3] Behrouz A Forouzan, "Cryptography and Network Security." Mc GRAW-HALL International Edition(2008).

[4] Janakiraman V.S, Ganesan.R, Gobi M, "Hybrid Cryptographic Algorithm for Robus Network Security," PSG College of Arts and Science, Coimbatore, (July, 2007).

[5] Mehmet Yildiz et. al., —A Layered Security Approach for Cloud Computing Infrastructurel, 10th IEEE International Symposium on Pervasive Systems, Algorithms, and Networks, pp 763-767.

[6] Qi Zhang, Lu Cheng, Raouf Boutaba,l Cloud computing: state-of-the-art and research challengesl, J Internet Serv Appl (2010) 1, Springer, pp 7–18

[7] Qin Liu et al., —Secure and privacy preserving keyword searching for cloud storage servicesl Journal of Network and Computer Applications, Elsevier, 2011.

[8] S. Subashini, V.Kavitha, —A survey on security issues in service delivery models of cloud computingl, Elsevier Journal of Network and Computer Applications 34, 2011, pp 1-11

[9] Timo bartkewitz,"Building Hash Functions from Block Ciphers, Their Security and Implementation Properties," Ruhr-University Bochum,(February 23,2009)

[10] Willion Stallings, "Cryptography and Network Security", Principles and practices, Fourth Edition, (2007).