Survey of Security Algorithms in Cloud

Swaranjeet Kaur
M.Tech Research scholar
Sri Guru Granth Sahib World University
Fatehgarh Sahib,Punjab

Amritpal Kaur
Assistant Professor
Sri Guru Granth Sahib World University
Fatehgarh Sahib,Punjab

ABSTRACT

Cloud Computing refers to the delivery of computing resources over the web. Computing resources are shared rather than having personal devices to handle applications. Information is accessed simply at anywhere, anyhow by connecting our device with web. Cloud Computing is predicated on web services used for storing, transferring and lots of alternative operations associated with information. Security is the major issue in cloud computing. The different algorithms have been proposed to provide security to critical data. This paper gives a brief introduction to some existing security algorithms in Cloud Computing.

General Terms

Cloud Computing, Security issues and Security algorithms.

1. INTRODUCTION

The term cloud refers to a network of remote servers hosted in the internet to store, manage and process data instead of local servers. Cloud Computing is a model for enabling simple, on-demand network access to a shared pool of computing resources (storage, applications and services). Rather than keeping information on your own hard drive for your needs, you tend to use a service over the net, at another location, to store data or use its applications. For e.g. when you store photos on-line rather than on your own data processor or use web-mail or a social networking website, then you are employing a “cloud computing” service. Data owners can easily access and store their data on cloud. Cloud computing is a set of IT services that are provided to a client over a network on a hired basis and with the flexibility to scale up or down their service necessities. Cloud computing is the use of a computing resources (hardware and software) that are delivered as a service over a network.

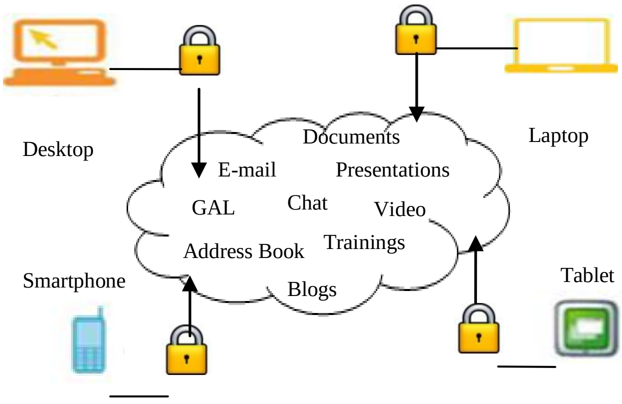

Fig 1: Showing access to Cloud Services from any device [1]

Cloud Computing allows people to share data, no matter where they are and what type of device they are using. Examples of cloud services are:

Social Networking Sites, e.g., facebook, twitter etc,

E-mail communication,

Google Docs (word, spreadsheets etc),

Amazon MP3 (to keep music in cloud),

Apple iCloud (works with Apple products) and

DropBox

There is an absence of actual definition of cloud computing. Certainly, the dearth of a regular definition of cloud computing has generated a good quantity of confusion. There appears to be several definitions of cloud computing. The United States National Institute of Standards and Technology (NIST) has printed a working definition that appears to have captured the normally united aspects of cloud computing. This definition describes cloud computing using:

Five characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Four deployment models: private clouds, community clouds, public clouds, and hybrid clouds.

Three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

With the fast development of processing and storage technologies and therefore the success of the net, computing resources became cheaper, more powerful and obtainable than ever before. This technological development has enabled the realization of a brand new computing model known as cloud computing, within which resources (e.g., mainframe and storage) are provided as general utilities that may be chartered and hired by users through the net on-demand. In a cloud computing atmosphere, the standard role of service supplier is split into two [2]:

Infrastructure suppliers-- who manage cloud platforms and lease resources consistent with a pay-per-usage model, and

Service suppliers–who lease resources from one or several infrastructure suppliers to serve the end user.

1.1 Cloud computing building blocks

The building blocks of cloud computing can be categorized as follow [3]:

Deployment Models:
Deployment model is that the cloud may be displayed for private, public or community uses. It consists of Private

cloud, Public cloud, Community cloud and hybrid cloud.

Private cloud: Private cloud is employed by a company and its customers, who own it. It may be managed by the organization or a third party. Resources and virtual applications that are provided by the cloud merchant are pooled together. Only the organization and its members have access to work on a particular private cloud.

Public cloud: Public cloud is for the utilization of public. It is chiefly based on a pay-per-use model that was just like paid electricity metering system. Public cloud is less secure than private cloud. All applications and information on the general public cloud are not safe from malicious attacks.

Community cloud: Community cloud is for a community of users who are having same mission or goal. The infrastructure is shared by many organizations for a shared cause. It can be managed by them or a third party service supplier.

Hybrid cloud: Hybrid cloud shares the properties of any of the above mentioned models. It is a private cloud connected to one or additional external cloud services. It is a combination of each public and private cloud. This Cloud provides safer management of the information and applications.

Service Models: The assorted service models are as follow [4]:

Software as a Service (SaaS)
Software as a Service is the uppermost layer that features an entire application that was offered as a service on demand. It can be represented as a process by which Application Service Provider (ASP) offers various software applications over the web. This service enables the client to get rid of installing the application on own computer. It is also referred to as Application as a Service Cloud. The user utilizes the software out of the box without any integration or patching up with any infrastructure.

Platform as a Service (PaaS)
Platform as a Service offer computational resources via a platform upon which applications and services may be hosted. In different words, it provides all the required resources to build an application and service via the web, without downloading or installing it. PaaS makes use of APIs to organize the performance of a server hosting engine that completes and replicates the execution consistent with consumer requests. An operating system, hardware and network are provided and user installs its own software and applications.

Infrastructure as a Service (IaaS)
Infrastructure as a Service also referred as Resource Cloud provides resources which are managed and may be scaled up, as services to a variety of users. It refers to the sharing of hardware resources for executing services. It can be done by using Virtualization technology. Moreover, the resources that are used are usually billed by the providers on the premise of the computational usage by the users. However, users should monitor their IaaS environments closely to avoid being charged for unauthorized services.

2. SECURITY ISSUES IN CLOUD

Security is to secure sensitive or critical data from unauthorized access or users. In other words, security is to protect sensitive information from harmful forces and the unwanted actions of unauthorized users. The main focus behind security is to ensure privacy while protecting personal data.

There are number of security problems for cloud computing because it contains several technologies as well as networks, databases, operating systems, virtualization, resource scheduling, dealing management, load balancing, concurrency management and memory management. Therefore, security problems for many of these systems and technologies are applicable to cloud computing. As an example, the network that interconnects the systems in a cloud needs to be secure. Moreover, virtualization paradigm results in many security problems. For instance, mapping the virtual machines to the physical machines needs to be administered firmly. Information security involves encrypting the information as well as making certain that appropriate policies are used for data sharing.

There are six particular areas of the cloud computing environment where equipment and software need substantial security attention. These six areas are [5]:

(1) Security of information at rest,

(2) Security of information in transit,

(3) Secure authentication of users, applications.

(4) Robust separation between data belonging to different customers,

(5) Cloud legal and regulatory problems, and

(6) Incident response.

In particular, we examine the following issues:

1) The threats against information residing in cloud computing environments.

2) The categories of attackers and their capability of attacking the cloud.

3) The safety risks related to the cloud, and where relevant concerns of attacks and countermeasures.

4) Rising cloud security risks.

Security is the main drawback in cloud computing. The usage of cloud is increasing day-by-day due to increase in number of users. Thus the numbers of attackers, attacking on the cloud to gain insight into sensitive information, are also increasing. A number of the potential attacks, criminals may try, include:

Denial of Service (DoS) attack: Denial of Service attack is an effort to create a machine or network resource inaccessible to its certain users. It consists of efforts to temporarily or indefinitely interrupt services of a host connected to the Internet. Attackers flood the cloud by flooding service so as to perform a full loss of accessibility on the meant service.

Cloud Malware Injection Attack: Cloud malware injection attack refers to a manipulated copy of victim’s service instance, uploaded by assaulter to the cloud, so that some service requests to the victim’s service are processed inside that malicious instance. An assaulter can get access to user information through this attack.

Side Channel Attack: An assaulter could attempt to compromise the cloud by inserting a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a form of effective security threat targeting system implementation of cryptographic algorithms [6].

Authentication Attack: Authentication is a liability in hosted and virtual services and is usually targeted. Authentication attacks target and decide to exploit the authentication method a website uses to verify the identity of a user, service or application. Types of authentication attacks are as follow:

Brute Force: It permits a wrongdoer to guess a person's user name, password, and credit card number by using an automatic method of trial and error.

Insufficient Authentication: It permits an assaulter to access a website that contains sensitive content without having to properly authenticate with the website.

Weak Password Recovery Validation: It permits an attacker to access a website that provides them with the ability to illegally acquire modification or recover another user's secret.

Man-In-The-Middle Cryptographic Attack: This attack is carried out once a wrongdoer places himself between two users. Anytime attackers can place themselves within the communication's path, there is the chance that they can intercept and modify communications.

3. SECURITY ALGORITHMS

The main focus is on cryptography to make data secure when transmitted over the network. Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries. In cryptography, encryption and decryption techniques are used. An encryption converts plaintext or message into cipher text and decryption extracts original message or plaintext from the same cipher text. Firstly, the information should be encrypted using the encryption algorithm in cryptography. Secondly, by using decipherment technique the receiver can read the original information. The figure shows some of the symmetric and asymmetric algorithms [7]:

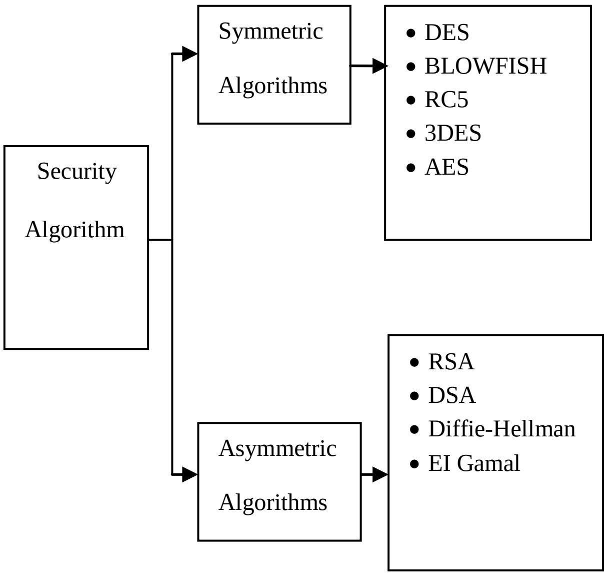

Fig 2: Showing security algorithms

3.1 Symmetric Algorithms (private)

In Symmetric keys encryption or secret key encryption, one same key is used to encrypt and decrypt the data. Hence the key is kept secret. These algorithms do not consume an excessive amount of computing power. Symmetric algorithms are of two types: Block cipher (block of plaintext is encrypted) and Stream cipher (one bit at a time).

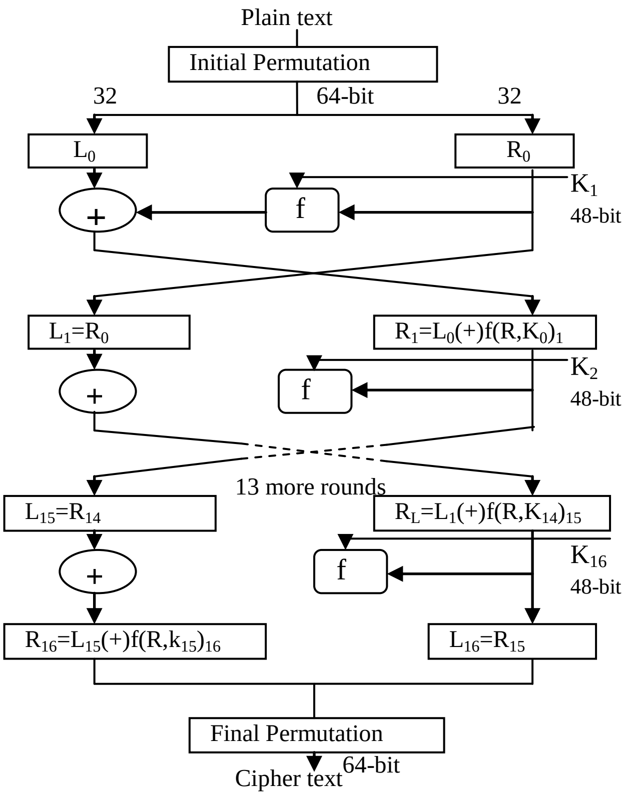

Fig 3: Encryption with DES

3.1.1 DES

DES stands for Data Encryption Standard and it was developed in 1977. It was the initial encryption standard to be recommended by authority NIST (National Institute of Standards and Technology). DES uses 64 bits key size with 64 bits block size. Since that time, several attacks and methods have witnessed weaknesses of DES that made it an insecure block cipher. Two elementary features of cryptography Diffusion (Substitution) and Confusion (Permutation) rounds. In every round key and information bits are shifted, permuted, XORed. 64 bit plain-text is bimanual to initial permutation (IP).Then IP generates two halves left plain-text (LPT)and right plain-text (RPT).Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are rejoined. At the encoding site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decoding site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encoding and decoding. The encryption process is made of two permutations (P-boxes), which we can call initial and final permutation, and sixteen Feistel rounds. The function f is made up of four sections [8]:

Expansion P-box

A whitener (that adds key)

A group of S-boxes

A straight P-box.

3.1.2 Blowfish

This was developed in 1993. It is one among the foremost common public algorithms provided by Bruce Schneier. Blowfish is a variable length key from 32 bits to 448 bits, 64-bit block cipher. No attack is thought to achieve success against this. Numerous experiments and research analysis tested the prevalence of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than alternative algorithms in output and power consumption. The block size for Blowfish is 64 bits; messages that do not seem to be a multiple of 64-bits in size have to be padded. It is applicable for applications where the key is not modified frequently. It is significantly faster than most encryption algorithms when executed in 32-bit microprocessors with large data caches. Data encoding happens via a 16-round Feistel network.

3.1.3 AES

AES stands for Advanced Encryption Standard**.** It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the cipher includes a 128-bitblock size, with the key sizes of 128, 192 and 256 bits, respectively. It ensures that the hash code is encrypted in a very extremely secure manner. Its algorithm steps are as follows:

1. Key Growth

2. Initial round

3. Add Round Key

4. Rounds

5. Sub Bytes

6. Shift Rows

7. Combine Columns

8. Add Round Key

9. Final Round

10. Sub Bytes

11. Shift Rows

12. Add Round Key.

3.2 Asymmetric Algorithms (public)

In Asymmetric keys, two keys are used: private and public keys. Public key is used to encode the data and private key is used to decode the data. Public key encryption is predicated on mathematical functions and intensive in computation. Encryption is the elementary tool for safeguarding the data. Encryption algorithm converts the data into scrambled form by using “the key” and solely user have the key to decode the information.

3.2.1 RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who publicly delineated it in 1977. The letters RSA are the initials of their surnames. It uses two different keys, one is public and one is private. The public key may be shared with everyone and private key is kept secret. It is predicated on the fact of problem in factoring large integers that are product of two massive prime numbers. The multiplication of these two numbers is simple but finding the original prime numbers from total factoring is troublesome task because it would take plenty of time even using today’s super computers. It uses two exponents: e as public key exponent and d as private key exponent and n as modulus. It involves three steps:

Key Generation: The keys for RSA algorithm are generated as follows:

Algorithm [12]:

```
Select two very large prime numbers denoted by p & q.
Set n=p*q
Select integer d such that GCD (d,((p-1)*(q-1))=1
Find e such that e*d=1(mod ((p-1)*(q-1)))
```

Encryption: If sender A wishes to send a message M to receiver B then A has to turn M into an integer m(padding scheme) and then computes the cipher text c using public key exponent e by computing:

$$c \equiv m^e \pmod n$$

Now A transmits c to B

Encryption key (e, n) is made public.

Decryption: Now receiver B can recover m from c using private key exponent d by computing:

$$m \equiv c^d \pmod n$$

Given m, B can recover the original message M by reversing the padding scheme.

Decryption key (d, n) is kept private.

3.2.2 DSA

DSA stands for Digital Signature Algorithm. DSA is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST)in August 1991 to be used in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993.Four revisions to the initial specification has been released: FIPS 186-1 in 1996,FIPS 186-2 in2000,FIPS 186-3 in 2009and FIPS 186-4 in 2013.In DSA, key generation has two phases: the primary phase is to select algorithm parameters which can be shared between different users of the system and the second phase is to compute public and private keys for a single user. The entropy, secrecy, and uniqueness of the random signature value *k* are crucial. It is so crucial that violating any one of these three requirements can disclose the entire private key to an assaulter.

3.2.3 Diffie Hellman Key Exchange (D-H)

Diffie Hellman key exchange was discovered by Whitfield Diffie and Martin Hellman. It is a technique for securely exchanging cryptographic keys over a public network and was the primary specific example of public-key cryptography. It permits solely two users to exchange a secret key over an untrusted network. These two users do not need any prior knowledge of each other or secrets. It is predicated on the difficulty of computing discrete logarithms of huge prime numbers. It requires two large numbers, one prime (P) and other is (G), a primitive root of P.

3.2.4 ElGamal

ElGamal encoding system is an asymmetric key encryption algorithm for public-key cryptography that relies on the Diffie-Hellman key exchange. It was delineated by Taher Elgamal in 1985.ElGamal encryption is used in the free GNU Privacy Guard software. The Digital Signature Algorithm is an alternative of the ElGamal signature scheme, which should not be confused with ElGamal encryption. The practical use of ElGamal cryptosystem is in a hybrid cryptosystem, i.e., the message itself is encoded with a symmetric cryptosystem and ElGamal is then used to encode the key used for the symmetric cryptosystem. This is done because asymmetric cryptosystems like Elgamal are slower than symmetric cryptosystems for the same level of security, so it is faster to encode the symmetric key (which most of the time is tiny if compared to the size of the message) with Elgamal and the message (which is randomly large) with a symmetric cypher. In this, each user has a private key x. Each user has three public keys: prime modulus p, generator g and public Y. ElGamal encoding is probabilistic encoding, i.e., the utilization of randomness in an encryption so that when we encrypt the plaintext, it can be encrypted to several potential cipher texts.

4. CONCLUSION AND FUTURE SCOPE

In today’s world, Cloud computing is rising as a new brand factor. There are several issues in cloud computing but the major issue concerns security issue. Many of the organizations are moving their data on the cloud but are concerned about security of their data. Thus cloud security is must which will be able to break the hindrance to the acceptance of the cloud by the organizations. In this paper, some existing security algorithms have been discussed which can be implemented to the cloud to provide security. As discussed there are many security algorithms which are currently available in cloud computing. Apart from these there is a great need to develop many more efficient algorithms to increase the security level of cloud computing. A further enhancement can be done in the existing algorithms so that security of data in cloud

can be increased. As the number of users is increasing rapidly in cloud computing with the passage of time so it becomes major issue to make their data completely secure. In future, more work can be done in making the cloud more secure or to increase its security level as high as possible.

5. REFERENCES

[1] Rajendra Kumar Dwivedi,, 2012. From Grid Computing to Cloud Computing & Security Issues in Cloud Computing

[2] Qi Zhang, Lu Cheng, Raouf Boutaba, 2010. Cloud computing: state-of-the-art and research challenges

[3] M. Vijayapriya, 2013. Security Algorithm in Cloud Computing: overview

[4] Ms. Disha H. Parekh, Dr. R. Sridaran, 2013. An Analysis of Security Challenges in Cloud Computing

[5] Jaydip Sen, 2011. Security and Privacy Issues in Cloud Computing

[6] Ajey Singh, Dr. Maneesh Shrivastava, 2012. Overview of Attacks on Cloud Computing

[7] Randeep Kaur,Supriya Kinger, 2014 Analysis of Security Algorithms in CloudComputing

[8] Rashmi Nigoti, Manoj Jhuria, Dr. Shailendra Singh, 2013. A Survey of Cryptographic Algorithms for Cloud Computing