# CLOUD COMPUTING SECURITY CHALLENGES AND SOLUTION

**Deepak Chopra, Dishant Khurana, K. Govinda**

*SCSE VIT UniversityVellore,*
*Tamilnade, 632014 India*

## ABSTRACT

*Cloud computing is another name used to describe "intergalactic computer network" in which the variety of services are offered, including storage, computers over the network of interconnected computers. As cloud computing involves storage and computation of data over the network, so it involves the issues of network security. Network security has become a major issue in these days because more and more people get involved with cloud applications which have sensitive information. Some of the applications of cloud computing like dropbox, private cloud of the firm has to send, receive and store the sensitive data over the network. The securityof cloud and communication systems becomes a major issue as society becomes increasingly dependent on the cloud computing technology. Cloud computing represents is the new evolution in the field of technology which has many demanding security concerns at every level, e.g., network, host, application, and data levels. Breaches of confidentiality, data corruption, man-in-the-middle attack are some of the risk issues related to cloud security.This paper describes about the different security algorithms, security issues and security attacks in cloud computing. Finally, as a result of this research, we propose a security model as a combination of the security algorithms.*

***Keywords****- Cloud computing, Infrastructure, Security Algorithms, Security Attacks, Security Issues.*

## INTRODUCTION

Cloud computing is another name used for describing distributed computing over the network. Cloud Computing is a set of IT services that are provided to the customer over the network which are owned and delivered by a third party. As the emergence of cloud computing, all types of companies started using their own private cloud to reduce the cost spent on the hardware. Companies like Google, IBM, and Amazon many more large scale industries started using this platform to store and compute their data. As use of this platform has been increasing day by day, then the security issues involved with cloud computing has become a major research topic. This paper describes the cloud computing platform, its security issues and security model used to mitigate the security issues.

## LITERATURE REVIEW

Cloud computing has become the latest topic in the field of Information & Technology and research today. It is often provided "as a service" over the Internet. In this computing model, resources are combined to provide service, infrastructure and platform to as many as possible users by sharing the resources. The services are mainly provided in the form of infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS)

### Service Models

Service models of cloud computing are deployed depending on requirements of business models. The primary service models being deployed (see Figure 1) are commonly known as:

1. **Software as a Service (SaaS)** — the applications or services are hosted in the cloud. Consumers have to buy the ability to access the hosted cloud services. A benchmark example of this is Salesforce.com, as discussed previously, where necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud [1]. Also, Microsoft is expanding its involvement in this area, and as part of the cloud computing option for Microsoft®Office 2010, its Office Web Apps are available to Office volume licensing customers and Office Web App subscriptions through its cloud-based Online Services.

2. **Platform as a Service (PaaS)** — Consumers purchase access to the platforms [2], enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed.

3. **Infrastructure as a Service (IaaS)** — Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity [3], but do not themselves control the cloud infrastructure. Also known are the various subsets of these models that may be related to a particular industry or market.

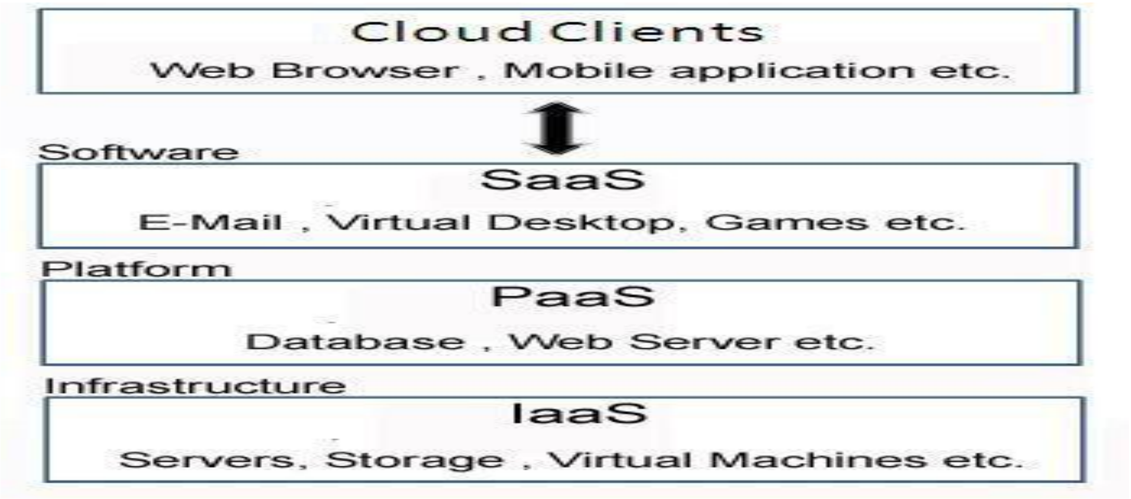
Cloud Clients
Web Browser , Mobile application etc.
Software
SaaS
E-Mail , Virtual Desktop, Games etc.
Platform
PaaS
Database , Web Server etc.
Infrastructure
IaaS
Servers, Storage , Virtual Machines etc.

Figure 1- Service Models
(Source: http://en.wikipedia.org/wiki/Cloud_computing)

### Deployment Models

Deployment models can be deployed depending on the structure of the organization. Different organizations have different structure, so deployment models can be chosen according to the structure to ease up the working of organization. There are four types of deployment models, namely pu blic, private, community and hybrid cloud service.

1. **Public Cloud**

The resources like cloud applications and storage is being made as open source. General public can access these services by buying them from cloud service providers [5]. These services are free or payable depends upon situation. Examples of public cloud systems are Amazon Web Services (AWS) and the Google App Engine [7].

2. **Private Cloud**

The infrastructure consisting of the resources of cloud application and storage is operated and managed either by organization or a third party. It may exist on site or at remote place of the organization. It is difficult to manage, make and assemble alone for a single user [7].

3. **Community Cloud**

The infrastructure supports a specific community that has common concerns (example: policy, security requirements, mission, and compliance considerations). This type of infrastructure can be managed either by the organisation or by a third party and may exist on-site or at remote location [7].

4. **Hybrid Cloud**

This type of infrastructure consists of two or more clouds (private, community, or public) which are unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [7].

## SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing involves communication between client and server through a network. Large amount of time has been consumed to transfer big volumes of data through the network. This becomes a major concern for data-sensitive applications in cloud computing. The communication delay between client and server is responsible to add delay to response time. As the time taken by the traffic is sufficient to intercept the data between the client and server, so it is a major concern of security to secure the channel of network between the client and server. There are various security issues arises when data has been intercepted over the channel between client and server. Some of them are listed below:

- Breaches of confidentiality
- Potential loss of control/ownership of data
- Account hijacking
- Data Security
- Unauthorized secondary usage
- Network security

## SECURITY ALGORITHMS

There are various security algorithms available to provide secure communication over the network, out of them cryptographic algorithms play an important role. Cryptographic algorithms involve encryption and decryption of the data using key. Encryption algorithm encodes the data using key such that it is not vulnerable to third party attack. Decryption algorithm decodes the encoded data in the original form before encryption. There are two types of cryptography algorithms:

a) Symmetric key algorithm: Only one key is used to both encrypt and decrypt the message.
b) Asymmetric key algorithm: Two different keys (namely: public and private) are used to encrypt and decrypt the message. Public key is used to encrypt the message while private key is used to decrypt the message. Public key is known to everyone while Private key is known to only user who is going to decrypt the message.

Cryptography algorithms which are used in cloud computing are as follows:

### RSA (Rivest-Shamir-Adleman)

This algorithm is used for public-key cryptography. It is the first and still most commonly used asymmetric algorithm. It involves two keys- a public key and a private key [8]. The public key is used for encrypting messages and known to all. Messages encrypted with the use of public key can only be decrypted by using the private key. In this authentication scheme, the server implements public key authentication by signing a unique message with its private key, thus creating what is called digital signature. The signature is then returned to the client. Then it verifies using the server's known public key [10].

**MD5- (Message-Digest algorithm 5)**

A widely used cryptographic hash function algorithm with a 128-bit hash value and processes a variable length message into a fixed-length output of 128 bits. First the input message is broken up intochunks of 512- bit blocks then the message is padded so that its total length is divisible by 512. [9] In this, the sender of the data use the public key to encrypt the message and the receiver uses its private key to decrypt the message [10].

**AES- Advanced Encryption Standard**

It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the ciphers has a 128-bit block size, with the key sizes of 128, 192 and 256 bits, respectively. It ensures that the hash code is encrypted in a highly secure manner [10]. Its algorithm steps are as follows:

1. Key Expansion
2. Initial round
3. Add Round Key
4. Rounds
5. Sub Bytes
6. Shift Rows
7. Mix Columns
8. Add Round Key
9. Final Round
10. Sub Bytes
11. Shift Rows
12. Add Round Key.

**DES- Data Encryption Standard**

DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and Ri which are then passed into what is known as a **round** (see figure 2.3), of which there are 16 (the subscript i in Li and Ri indicates the current round). Each of the rounds is identical and the effects of increasing their number are twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the cipher text and either the plaintext or key6. At the end of the 16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the **pre-output**. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text [11].

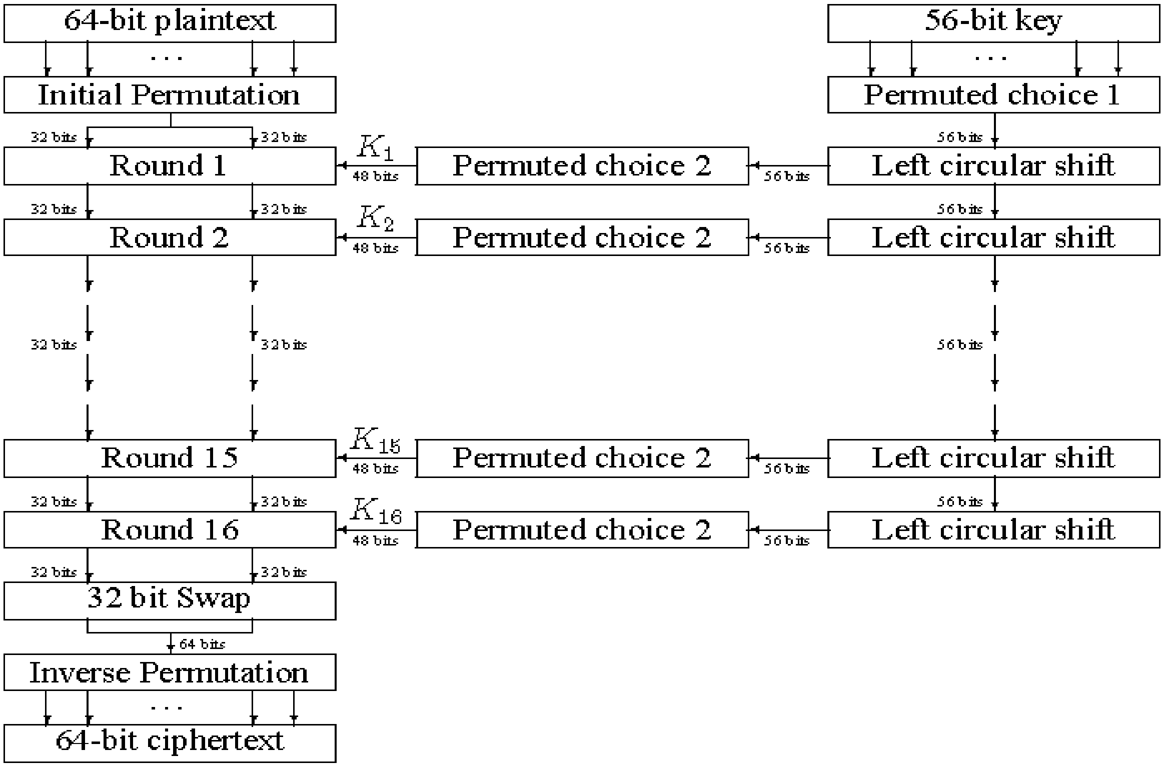

Figure 6: Flow diagram of DES algorithm for encryption algorithm

*Comparison between time complexities of cryptographic algorithms:*

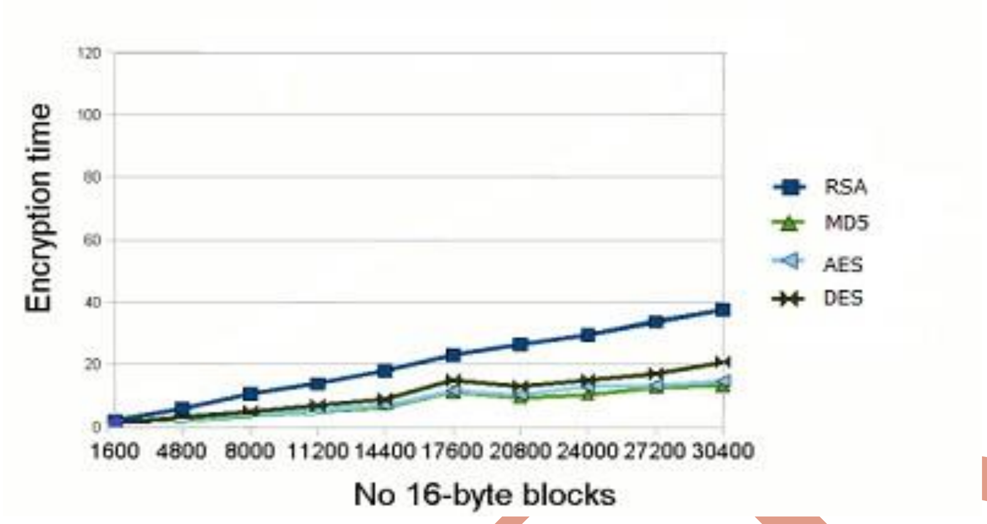

Figure 7: Comparison of time taken to encrypt the data by DES, Bloefish-256, AES-128 and AES-256 [12]

## PROPOSED SOLUTION FOR CLOUD SECURITY

Using the above discussed security algorithms; we proposed a simple way to tackle the threats from the hackers to stop them from intercepting the data. We know that data has been transferred in the form of packets through the network.

Steps to send the data from client side:

1. The cryptography algorithms have been stored on client side in particular order. For example: first is RSA, second is MD5 and third is AES and fourth is DES.
2. The encryption algorithm has been selected randomly at client site. It could either be achieved by the use of rand () function or by linear congruently method i.e.

$$r= (((a*r) +b)) \%m)\%z$$

Where: a,b are large prime numbers.

z = number of cryptography algorithms used in the model

m = 232 or 264.

Initial value of r = 32.

If you get over the same seed you get the same sequence of random variables. The choice of numbers being generated by rand () provides pseudo-random numbers while the latter technique is the most suitable way of generating random numbers.

3. After this the encryption of the data packet has been takes place with a given value of r, this value of r gets attached either at the end of the packet or at the starting of the packet.

4. The packet has been sent to the server and get stored over there.

Now reverse of the above mechanism takes place in the retrieval of the data from server.

1. The attached r value has been detected.
2. Corresponding cryptographic decryption algorithm starts decrypting the packet.
3. User can avail the information in simple format.

Advantages of the above proposed model for cloud computing security:

1. The channel of communication can be unsecured. No need to spend money on securing the channel because we are using randomly generated encryption algorithms for sending packets through the network channel. No one we get to know that which packet is encrypted by which algorithm.
2. This model uses less computer resources as compared to complex security algorithms
3. It is a cost effective model. It doesn't require much cost to implement this method.

## CONCLUSION

Although cloud computing plays a vital role in today's IT world. It revolutionizes the working structure of the companies. Cloud computing made easier to store and compute data over the network, but the revolution always comes with new problem. Cloud computing has their own security issues which risks user data privacy.

In this paper, we have discussed many security issues and their effects. The security issues faced by the users/providers over the communication channel have been discussed. To remove the data interception over the communication channel, encryption and decryption plays a vital role. As a result of this research, we proposed a new model to provide security to the data over the network. Cloud security has been provided by our model, because nobody knows at what time which encryption algorithm has been chosen up for encryption. As hacker don't know about the encryption algorithm, so it will not be easy for him to decrypt the data. For the time being, we have used only three cryptographic algorithms.

In future, we will extend this research by testing the efficiency of different cryptographic algorithms over the network and try to put more cryptography algorithms.

## REFERENCES

[1]Mr. D. Kishore Kumar, Dr.G.Venkatewara Rao, Dr.G.Srinivasa Rao, "Cloud Computing: An Analysis of Its Challenges & Security Issues", IJCSN Volume 1, 2012.

[2]Kuyoro S. O., Ibikunle F. & Awodele O., "Cloud Computing Security Issues and Challenges",IJCN, Volume (3) : Issue (5), 2011.

[3]Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, 2013.

[4]Satveer Kaur, Amanpreet Singh, "The Concept of Cloud Computing and Issues Regarding its Privacy and Security", International Journal of Engineering Research & Technology, Vol.1 - Issue 3, 2012.

[5]Florin OGIGAU-NEAMTIU, "Cloud Computing Security Issues", JoDRM Volume 3, Issue no. 2 (5), 2012.

[6]K.Valli Madhavi, R.Tamilkodi , K.Jaya Sudha, "Cloud Computing: Security Threats and Counter Measures", International Journal of Research in Computer and Communication Technology Advance Technology, Vol 1, No 4, 2012.

*[7] http://www.cloud-competence-center.com/understanding/cloud-computing-deployment-models*

[8]K.S.Suresh, Prof K.V.Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, 2012.

[9]Gurpreet Kaur,Manish Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms", IJERA : Volume 3 Issue 5, 2013.

[10] M. Vijayapriya M. Phil. Research Scholar, "Security Algorithm In Cloud Computing: Overview" International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4, 2013.

*[11] http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf*

*[12] http://www.javamex.com/tutorials/cryptography/ciphers.shtml*