Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

# A Review on Cloud Security and its Issues using various Symmetric Key Encryption Algorithm

Deepika Jalhotra
M Tech (CSE)
DCSA, KU, Kurukshetra
Haryana, India

Dr. Pardeep Kumar
Associate Professor (CSE)
DCSA, KU, Kurukshetra
Haryana, India

Shalini Aggarwal
Assistant Professor
GCW, Karnal
Haryana, India

***Abstract:*** As with the growth of data on cloud, cloud security is considered more important than before. Now-a-days millions of users are using cloud. Cloud computing resolves many problems like balancing the load, scheduling the tasks, providing the software to users and many more. This paper includes the various security issues faced during the use of services provided by the cloud and securing the cloud by using various symmetric key encryption algorithm.

***Keyword:*** Cloud security, Encryption, Security issues, AES and DES

## 1. INTRODUCTION

In this era, cloud computing is most widely used technique. It allows the cloud user to enjoy the on demand services and applications from the pool of computing resources through storing their data on the cloud[1]. Cloud computing is the computing where the computer resources are shared instead of they are stored on local servers or some personal devices for handling a particular application.

For example, the smart phones that are being used today use their internal memory and are having their storage capacities like 16GB to 32GB or even more. So the memory is needed on each device to save the applications and data. The cost of the phones especially smart phones depends upon the memory storage like if you buy a phone with memory space 16GB costs Rs25,000 and another smart phone with memory space 32GB costs Rs 45,000 i.eRs 23,000 extra for 16GB memory space. So, if cloud computing is used the extra memory space is not required and which saves the cost for that extra memory. This also provides the security to the data of the user and applications also in case if the device or phone is damaged and data of the user remain safe.[2]

**Types of Cloud**

There are basically three types of cloud

a) Public Cloud
b) Private Cloud
c) Hybrid Cloud

**a) Public Cloud:** In public cloud, cloud services are available to users via the service provider over the internet. It provides the control to the user to use the services offered by the cloud to that user. These services are either free or on the basis of pay-per-use. Public clouds are available to large organizations that are owned by third party organizations which offers cloud services. Amazon Elastic Compute Cloud (EC2), Google App Engine, and Microsoft are some of public cloud provider.[1]

**b) Private Cloud:** Private Cloud is also known as "Internal cloud" or "Enterprise cloud". In this type of cloud data is managed properly within the organization only and without the limits of network bandwidth. The main Purpose of this type of cloud is to offer services within the organization and more security and privacy is provided by it than in public cloud.[3]

**c) Hybrid Cloud:** This type of cloud is the combination of both public and private cloud. It provides the benefits of cost with security concerns.

**Models of Cloud**

There are basically three models of cloud computing

a) Software as a service(SaaS)
b) Platform as a service(PaaS)
c) Infrastructure as a service(IaaS)

**a) Software as a Service:** SaaS is the type of delivery model through which cloud computing makes software available to the end users as a service. These software services are delivered to the user through web browsers as a service on demand (either free or pay according to their use). The client user has not to worry about the licence and cost and other issues related to it.[4] This is a big advantage for customer as it reduces the cost for software development, maintenance and operations. Dropbox, Google and Microsoft office web are some examples of SaaS.

**b) Platform as a Service:** PaaS is the type of delivery model which delivers the computing platform as a service via internet. PaaS eliminates the cost and complexity of evaluating, buying, configuring and managing the hardware and software needed for enterprise application[2]. PaaS may include services such as application design, development, security, scalability and versioning. Navi suite is the example of PaaS.

**c) Infrastructure as a Service:** It is the delivery model in which a cloud owner provides the Infrastructure (equipment) which are necessary for the support of operations, including storage, hardware, servers and networking components. The

© 2015-19, IJARCS All Rights Reserved

cloud service provider takes the authority of the equipment and is responsible for storing, running and maintaining it.[5] The end user always pays on per use basis. Access to infrastructure includes complete operating system access, routers and firewalls etc. Google, Amazon and Microsoft are good examples of IaaS.

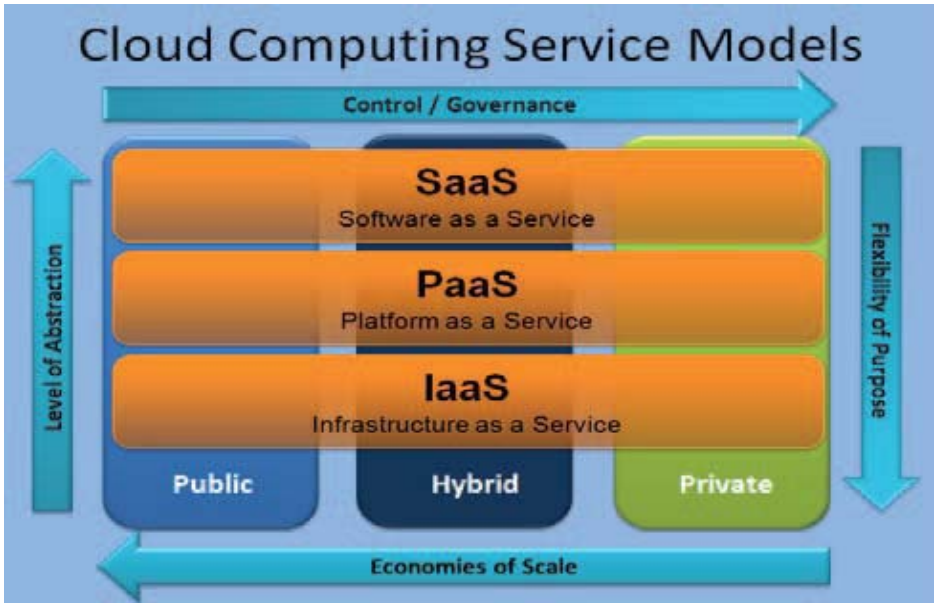


Fig 1-Models of Cloud Computing

## 2. LITERATURE OVERVIEW

This section includes the issues in securing the cloud and algorithms used in securing the cloud.

**Security Issues**

**1.) Confidentiality**

Confidentiality refers to only authorised users or systems can access the data present on the cloud. The threat to data increases in the cloud due to increase in the number of users or system and applications involved in it.[6]

**2.) Multitenancy**

Multitenancy refers to the sharing of resources. It means multiple users use the same resource simultaneously[7].

**3.) Integrity**

Integrity means the data or information present on the cloud is modified only by the authorised users that is the users who have the authority to modify the data or information.

**4.) Availability**

Availability is the property of a system being accessible on demand by the authorised users.

Availability refers to data, software and also hardware available to authorised users on demand.[8]

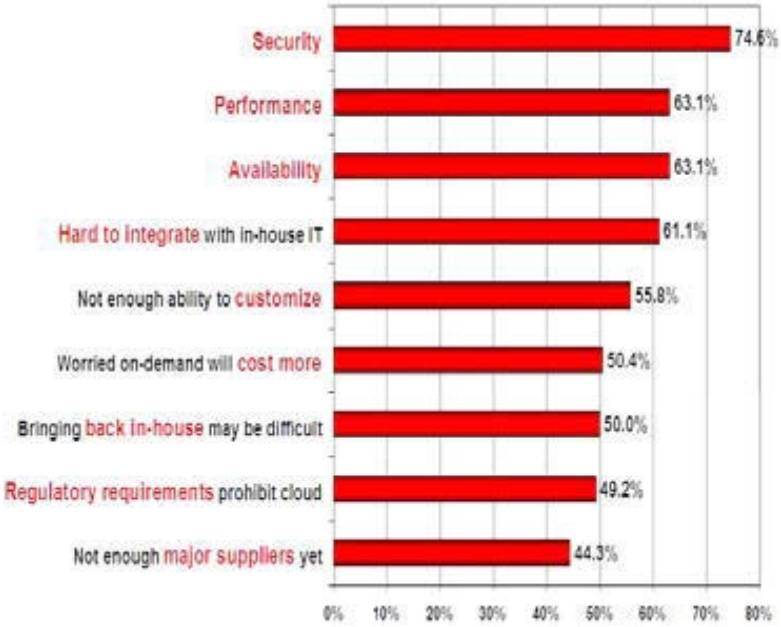


Fig 2- Issues of Cloud Computing

**Symmetric Key Algorithm**

Symmetric key algorithms are used for encryption and decryption of data. These types of algorithms uses the same key that is both the keys are same for encryption of plain text and decryption of cipher text.

© 2015-19, IJARCS All Rights Reserved

**Types of Symmetric key Algorithms**

a) Stream cipher: It is a type of symmetric key cipher where plain text digits are combined with a pseudorandom cipher digits stream.

b) Block cipher: It is a type of symmetric key cipher where a large number of bits are combined and encrypt them as a single unit. Blocks of 64 bits have been commonly used.

The Cryptographic Algorithms which uses the Symmetric Key Algorithms are as under:

**a) Advanced Encryption Standard(AES):**The original name of AES algorithm is RIJNDAEL. This algorithm was established by the US NIST(National Institute of Standard and Technology) in 2001[9]. AES was developed by two Belgian cryptographers Joan Daemon and Vincent Rijmen. They submitted a proposal to NIST during the AES selection process. The block size of AES algorithm is 128 bits and Key length of AES are 128,192 and 256 bits.[4]

**b) Data Encryption Standard(DES):** This type of algorithm uses the symmetric key algorithms for encryption of data[10]. It was developed in the early 1970s at IBM. .Now a days DES algorithm is considered as insecure for many applications because the key size is very small[6].

**c) Triple DES:** This algorithm also known as Triple Data Encryption Algorithm (TDEA). It also uses the symmetric key block cipher and applies the DES cipher algorithm three times to each data block[8]. The key size of this algorithm is 168,112 or 56 bits.

**d) Blowfish:** It is the type of cryptographic algorithm which uses the symmetric key block cipher. This algorithm was designed in 1993 by Bruce Schneier. This algorithm gives good encryption rates in software. The key size of this algorithm vary from 32 bit to 448 bits and has a block size of 64 bits.

**e) RC2:** This algorithm uses a symmetric key block cipher. It was designed by "Ron Rivest". RC stands for either Ron's code or Rivest Cipher. It was developed in 1987. The block size of this algorithm is 64 bits and key length vary from 8 to 1024 bits and by default it is 64 bits.

**f) Skipjack:** This algorithm uses the symmetric key block cipher for the encryption of data. It was developed by the US National Security Agency(NSA). The key length of this algorithm is 80 bits and block size is 64 bits.

## 3. COMPARATIVE ANALYSIS

A comparison of above explained Algorithms which uses Symmetric Key has been done in the table 1.

| Algorithm Name | Structure | Key Size (in bits) | Rounds | Cipher Type | Introduced in | Attacks | Block Size (in bits) |
|---|---|---|---|---|---|---|---|
| **AES** | **Substitution-permutation N/w** | **128<br>192<br>256** | **10<br>12<br>14** | **Block** | **1998** | **Brute force** | **128** |
| **DES** | **Balanced Feistel N/w** | **56** | **16** | **Block** | **1977** | **Brute force** | **64** |
| **Triple DES** | **Feistel N/w** | **112<br>168** | **48** | **Block** | **1998** | **Meet in middle** | **64** |
| **RC2** | **Source heavy Feistel N/w** | **40-1024** | **18** | **Block** | **1987** | **Related key** | **64** |
| **Blowfish** | **Feistel N/w** | **32-448** | **16** | **Block** | **1993** | **Birthday attack like http** | **64** |
| **Skipjack** | **Unbalanced Feistel N/w** | **80** | **32** | **Block** | **1998** | **-** | **64** |

From the above table, it can be observed that AES algorithm uses less time to execute the datapresent on the cloud while the DES algorithm has less key size as compared to other algorithms. Blowfish algorithm has less memory size. The AES algorithm has varying key size and takes less time for encryption and decryption .

Comparison Table II of AES and DES Encryption and Decryption Time in Milliseconds

| File Size | AES Enc and Dec Time in MS | DES Enc and Dec Time in MS |
|---|---|---|
| 1KB | 1560 | 1601 |
| 61KB | 1794 | 1981 |
| 3.15MB | 2148 | 4197 |

© 2015-19, IJARCS All Rights Reserved

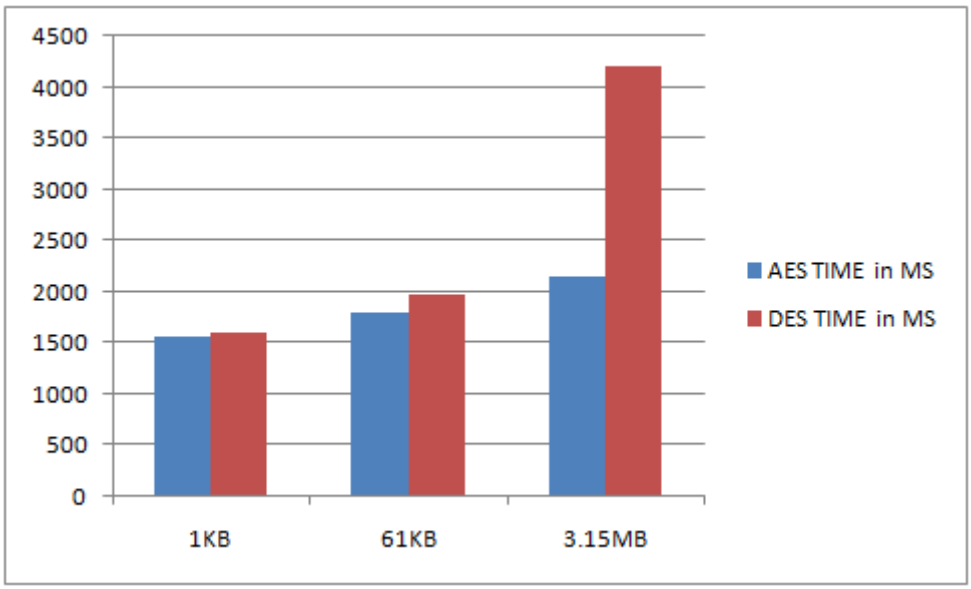


Fig 3 –Comparison of AES &DES Enc &Dec Time in ms

From the above Table and comparison chart it is shown that AES performs better for all types and sizes of files

## 4. CONCLUSION

This paper includes the various symmetric key algorithms which were proposed earlier and security issues which are faced during the use of data from the cloud. Comparsion have been made between the various symmetric key encryption algorithm and find the best algorithm from them. Encryption Algorithm plays very important role in securing the data on the cloud. According to comparison made on different symmetric key algorithms it is found that AES performs better as compared to other algorithms. DES has small key size which is not suitable for some of the applications used in the cloud. But AES requires less memory for performing actions using this algorithm. There are no differential and linear cryptanalysis attacks on AES. DES algorithm has weak and semi weak keys but this weakness is overcome in AES. The execution time of AES algorithm is less as compared to DES, 3DES, RC2, Blowfish etc.

## 5. REFERENCES

1. Bhale Pradeepkumar Gajendra, Vinay Kumar Singh, and More Sujeet, "Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption," IEEE, pp. 1304-1309, 2016.
2. Prof.R.R. Tuteja Shakeeba S. Khan, "Security in Cloud Computing using Cryptographic Algorithms," International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 1, pp. 148-154, January 2015.
3. Rachna Arora and Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Alggorithms," International Journal of Engineering Research and Applications(IJERA), vol. 3, no. 5, pp. 1922-1926, Jul-Aug 2013.
4. Ritu Gehlot and Prof. Nishant Sinha, "Enhancing Security on Cloud using Additional Encrypted Parameter for Public Authentication," IEEE, 2016.
5. T. Aravindh, S. Shyam Chander, R. Rukmani, and G. Kalaichelvi, "Secured Cloud Storage for Strategic Applications - A case study," IEEE, pp. 292-296, 2014.
6. Bob Duncan, Alfred Bratterud, and Andreas Happe, "Enhancing Cloud Security and Privacy:Time for a New Approach?," IEEE, pp. 110-115, 2016.
7. MANDEEP KAUR and MANISH MAHAJAN, "Using encryption Algorithms to enhance the Data Security in Cloud Computing," International Journal of Communication and Computer Technologies, vol. 1 NO-12, no. 3, pp. 56-59, January 2013.
8. Babitha.M.P and K.R. Remesh Babu, "Secure Cloud Storage Using AES Encryption," IEEE, pp. 859-864, 2016.
9. Mr. B.Thiyagarajan and Mr. Kamalakannan.R, "Data Integrity and Security in Cloud Environment Using AES Algorithm," IEEE, 2014.
10. Khalid EI Makkaoui, Abdellah Ezzati, Abderrahim Beni-Hssane, and Cina Motamed, "Cloud Security and Privacy Model for Providing Secure Cloud Services," IEEE, 2016.

© 2015-19, IJARCS All Rights Reserved