International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Privacy Preserving and Ownership in Cloud Computing Using Symmetric Key Encryption

Deepika Jalhotra[1], Dr Pardeep Kumar[2], Ms Shalini Aggarwal[3]

[1]M Tech scholar, DCSA, Kurukshetra University, Kurukshetra, Haryana, India
[2]Assistant Professor, DCSA, Kurukshetra University, Kurukshetra, Haryana, India
[3]Assistant Professor, GCW, Karnal, Haryana, India

Abstract: - *There are several issues related to security in cloud computing. In cloud computing various resources and data are accessed via a network. An authorized user can access the network easily. This paper focuses on various data protection and security issues in the cloud environment and design a model for solving various issues like authentication, authorization and confidentiality using symmetric key algorithm like Advanced Encryption Standard(AES) and Data Encryption Standard(DES). In the designed model data is encrypted using AES 128 bit, 192 bit and 256 bit. The proposed model provides the security from unauthorized access to the data.*

Keywords: - Cloud Security, AES, DES, Symmetric Key Algorithm

I. Introduction

In Cloud Computing there are various issues which deal in performance of the cloud. The main issue is the security of data in the cloud. According to the users who are using the cloud find that the data which is present on the cloud is not protected from unauthorized access. With the help of cryptography, data security can be achieved. [1] [2] There is encryption and decryption process in cryptography and these processes are done with the help of symmetric and asymmetric keys. In the symmetric keys, both client and server use the same key for their encryption and decryption. And in the asymmetric keys, both client and server use the different keys for their encryption and decryption of processes. Now a days, most of the companies are shifting towards the AES (Advanced Encryption Standard) based encryption in the cloud for the security of data. There are basically 3 types of encryption keys in AES that is 128 bit encryption, 192 bit encryption and 256 bit encryption which are using 10, 12 and 14 rounds. The data which is to be stored in the cloud is encrypted by using the encryption process. [3]

As with the growth of technologies all big and large no of organizations like Amazon, Google, Yahoo and IBM etc are already using the cloud. From all over the world a large no of users store or share their data on the cloud. In the real cloud environment the existing solutions related to data security are not secure. The approaches which are used today don't ensure data security in the cloud. But in the proposed model data of end user is encrypted by using the AES 128, 192 and 256 bit encryption which is secure as compared to other encryption techniques and shows the time which is taken by the technique for the encryption and decryption of data [2]. And authorized user can share their data to other authorized user. A comparative study based on analysis of simulation time for encryption and decryption of data is done and found that AES algorithm is better than DES and all other encryption algos.

II. Related Work

This section discusses about the AES and DES algorithms and why AES is important from other encryption algorithm.

A. Encryption Algorithms:

There are basically two types of encryption algorithm that is symmetric key encryption algorithm and asymmetric key encryption algorithm. The symmetric key encryption algorithm uses a single private key for both encryption and decryption. Advanced Encryption standard (AES) and Data Encryption standard (DES) both are the examples of symmetric key encryption algorithm. And asymmetric key encryption algorithm uses a public key for encryption and a private key for decryption of data.

a) Advanced Encryption Standard (AES):

It is also known as RINNDAEL algorithm. It is the type of Symmetric key encryption algorithm. AES was established by US NIST (National Institute of Standard and Technology). It was developed by two Belgian cryptographers John Daemon and Vincent Rijmen [3]. These cryptographers submitted their proposal to NIST during the selection process of AES. The block size that is the plain text size of AES algorithm is 128 bits. And the key length of AES varies in three sizes that are 128 bit, 192 bit, and 256 bit. The number of rounds depends upon the key length.

Table 1 Relation between No of rounds & key length

Key length	128 bits	192 bits	256 bits
Number of Rounds	10	12	14

Table 1 shows the relationship between the key length and no. of rounds

b) **Data Encryption Standard (DES):**

It is the type of symmetric key encryption algorithm. It was developed at IBM in the early 1970s. This algorithm encrypts data in the blocks and the size of each block is 64 bits. That is the DES algorithm takes the input of 64 bits plain text and converts that input into 64 bits cipher text [7] [6]. The key length of this algorithm is 56 bits which is very small as compared to that of AES algorithm. In the first step of encryption the data in the block of 64 bit passes through initial permutation. And after the initial permutation 16 rounds of permutation and substitution is performed [1]. And the last step is of 64 bit output which is obtained by reversing the initial permutation and applied to the last step of 16 rounds and the results obtained is the 64 bit cipher text. . After the development of AES, DES was considered not so secure because the key length of this algorithm is small as compared to that of AES algorithm. [3] [9] DES is mostly exposed to brute force attack because of its small key length.

B. Why AES Encryption Algorithm?

A comparison has been made between the various key sizes of AES algorithm and the DES algorithm on different key sizes and finds out that AES performs better and which variation of AES performs better in all file size is shown in table 2.

Table 2 Comparison of AES & its variations with DES

File Type	File Size	AES 128	AES 192	AES 256	DES
.txt	1 KB	1685	1450	1216	1794
.jpg	61 KB	1894	1779	1669	1990
.jpg	3.15 MB	4958	4820	4103	5463
.pdf	11MB	10982	9991	8384	11481
.pdf	57.6 MB	24507	19095	18735	37034
.mp4	1.15 GB	1015168	976930	816156	1173966

From the above table, it is found that Advanced Encryption Standard (AES) performs better than the Data Encryption Standard (DES) and also the variation of AES that is AES 256 performs the encryption and decryption in less time as compared to its other variation and other algorithm. Now a days there is a problem of fast and

secure release of services to the cloud users. And AES solves this problem of fast and secure release of services to the cloud users. Because AES is fast and secure as compared to other encryption and decryption algorithms

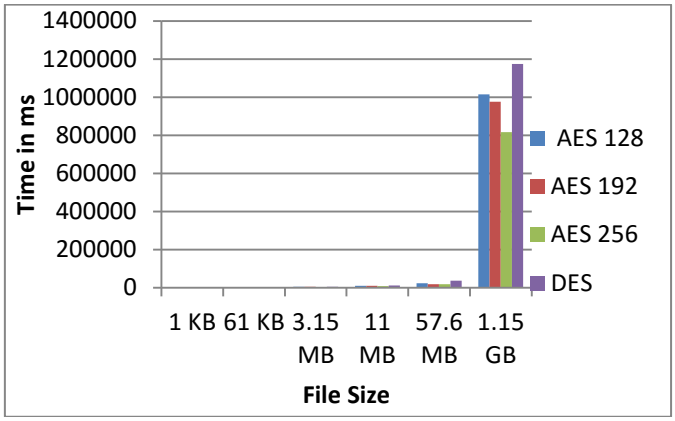

Fig 1 Comparison Graph of DES, AES & its Variations

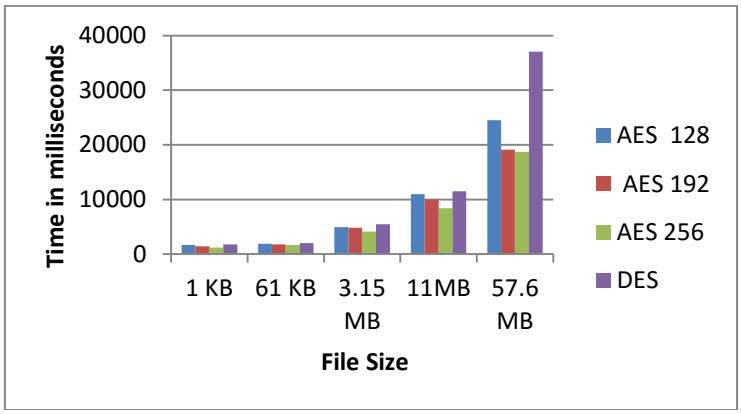

Fig 2 Comparison Graph of DES, AES & its Variations excluding 1GB file

III. Proposed Solution

This section discusses about the proposed solution which contains the model. In that model there are various phases which will be discussed and this model also maintains the security because security is the major concern. There is the basic need of security and privacy in the cloud environment.

1) User Registration Phase:

In this phase each and every user has to register them before accessing to the cloud system. The registration of the user is done by creating a user name and password. After registering the user can access the cloud system by login to the cloud system to access the services provided by the cloud.

2) File Uploading and Downloading Phase:

In this phase only the authorised user that is the user who has successfully registered with the cloud system can upload and download their file on the system. While uploading the content of the file is encrypted using the AES algorithm and is saved on cloud system. While downloading the content of the file is decrypted using the same key which is used for the encryption. So that the file of user remains secure.

3) Data Security Phase:

In this phase 256 bit Advanced Encryption Standard (AES) is used to secure the uploaded data of the user. It is used because AES 256 bit encryption is fast and secure
as compared to its variations and DES algorithm as shown in the fig 1 and table 2.

4) Trusted Party Phase:

In this phase there is a trusted user who is also registered with that cloud system and if any other registered user wants to access files of other registered user. The user can access files of the user by sharing the file with that user so that the security is maintained

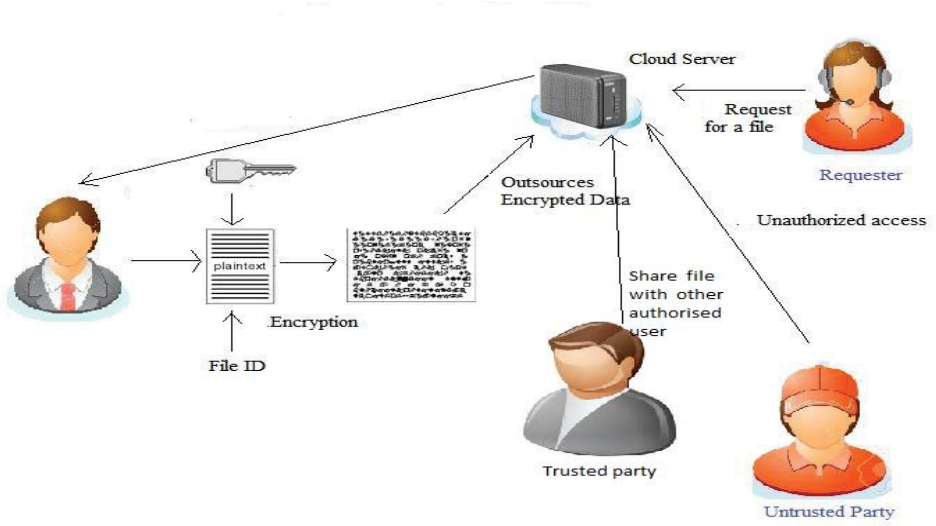

Fig 3 Proposed Model

IV. Experimental Results

The model is proposed using the java programming language and swing API. In this model there is one system that is cloud server which stores the files of users securely. Fig 2 shows the proposed model. The proposed model stores the files of cloud users safely and also shares the files with other authorised user. An authorised user can share secret files with the other authorised user.

Fig 4 Security Model of Cloud

For example, assume a user wants to store his/her secret file on the cloud, for performing this action that user has to register on the cloud by using the user name and password. The user name and password is set by the user itself not by the system. After successful registration the user can upload his/her secret file on the cloud. After uploading the file is encrypted using AES 256 bit encryption and if the user wants to see the encrypted file the user can see that file and also the decrypted file. A file id is generated for every file which is uploaded by the user and is stored in encrypted form on the cloud.

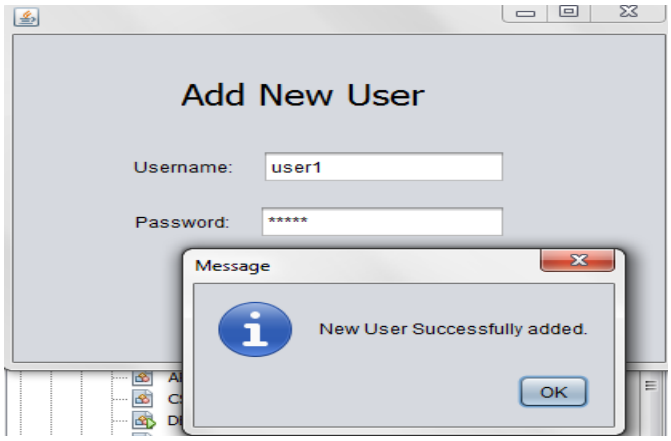

Fig 5 New user Registration phase

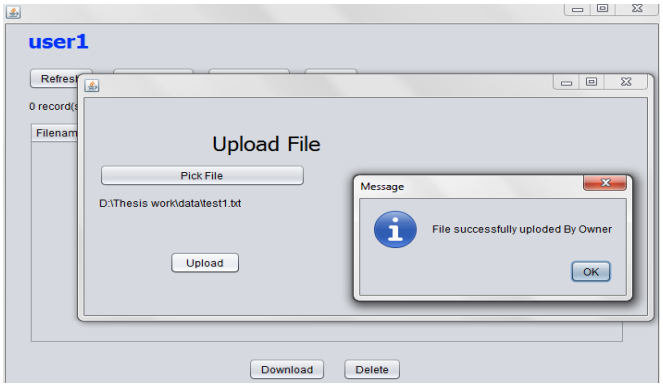

Fig 6 Upload File phase

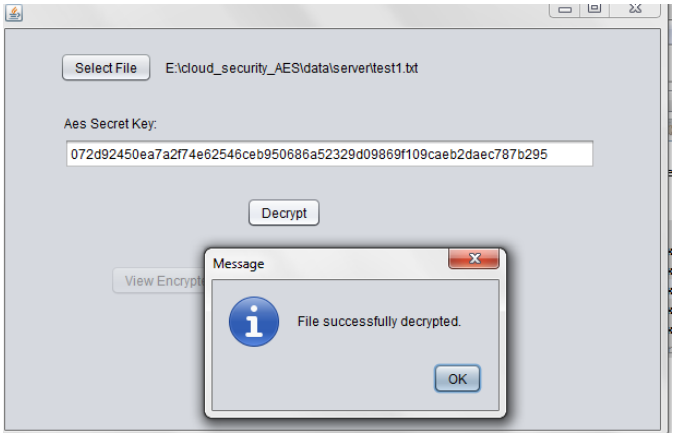

Fig 7 File Decryption Phase

V. Conclusion

This paper studied various symmetric key encryption algorithms which were proposed earlier and identified the best method for secure storing of files.AES 256 bit encryption is found to be best for fast and secure transfer and storage of files. AES 256 bit takes less time as compared to its variations. The test is performed on various format of different file sizes and found that AES 256 bit encryption and decryption is fast and secure. On the basis of this study a model for secure transfer, storing and sharing of files in the cloud is implemented which results in secure transfer of files.

VI. References

[1] T. Aravindh, S. Shyam Chander, R. Rukmani, and G. Kalaichelvi, "Secured Cloud Storage for Strategic Applications - A case study," IEEE, pp. 292-296, 2014.

[2] Mr. B.Thiyagarajan and Mr. Kamalakannan.R, "Data Integrity and Security in Cloud Environment Using AES Algorithm," IEEE, 2014.

[3] Ritu Gehlot and Prof. Nishant Sinha, "Enhancing Security on Cloud using Additional Encrypted Parameter for Public Authentication," IEEE, 2016.

[4] Monjur Ahmed and Mohammad Ashraf Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD," International Journal of Network Security & Its Applications (IJNSA), vol. 6, pp. 25-36, January 2014.

[5] Gaurav Raj, Ram Charan Kesireddiy, and Shruti Gupta, "Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256bit Encryption in Cloud," IEEE, pp. 374-378, 2015.

[6] Abhishek Goel and Shikha Goel, "Security Issues in Cloud Computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 1, no. 4, pp. 121-124, December 2012.

[7] Khalid EI Makkaoui, Abdellah Ezzati, Abderrahim Beni-Hssane, and Cina Motamed, "Cloud Security and Privacy Model for Providing Secure Cloud Services," IEEE, 2016.

[8] Babitha.M.P and K.R. Remesh Babu, "Secure Cloud Storage Using AES Encryption," IEEE, pp. 859-864, 2016.

[9] Vishnu Patidar and Makhan Kumbhkar, "Analysis of Cloud Computing Security Issues in Software as a Service," International Journal of Scientific Research in Computer Science and Engineering, vol. 2, no. 3, pp. 1-5, 2014.

[10] Bob Duncan, Alfred Bratterud, and Andreas Happe, "Enhancing Cloud Security and Privacy:Time for a New Approach?," IEEE, pp. 110-115, 2016.