Journal of Biostatistics and Biometric Applications
Volume 3 | Issue 1
ISSN: 2455-765X

Research article Open Access

A Proposed Architecture for Data Security in Cloud Storage Space

Attar N*, and Shahin M

Consulting Company and Power Support Services, Mashhad, Iran

***Corresponding author:** Attar N, Consulting Company and Power Support Services, Mashhad, Iran, Tel: +989155130525, E-mail: Naser.Attar@Yahoo.com

Citation: Attar N, Shahin M (2018) A Proposed Architecture for Data Security in Cloud Storage Space. J Biostat Biometric App 3(1): 106

Abstract

Cloud computing is a new and evolving technology. Important feature of cloud computing is using storing, multi-users space and distributed and parallel environment. The cloud offers some services which reduce the cost and time, offering various types of services is possible through internet. One of important services of cloud is the possibility of storing data by users in cloud. In fact, the main challenge is that the users concern about how the data are stored on cloud servers because these data may be located in different zones of world and illegitimate users might access to these data and this insecurity is considered as one of the big concerns of users in cloud. Therefore, data security and privacy in cloud is a big problem. In order to solve data security in cloud computing, cryptography architecture is suggested that is effective for cloud data. The evaluation of proposed plan has shown that our plan is possible and efficient.

Keywords: Data; Data Security in Cloud; Cloud Computing; Data Encryption; AES Algorithm

Introduction

Cloud is associated with a great number of advantages for organizations and users such as reducing the costs, increasing flexibility, business and agility. The cloud gives users some common computing resources such as networks, servers and storing systems anywhere, cheap and appropriate based on demand [1].

Available virtual resources in cloud enable the organizations to save the resources and also speed up establishing functional programs which leads to business in the organization [2]. Although cloud proposes different services such as the possibility of using storing space in cloud but considering lack of appropriate security control system and weakness in protecting data, many users don't use these storing services. Generally speaking, security problems in cloud include the following issues:

Integrity

The user ensures that data cannot be changed by another illegitimate user in a distributed system such as cloud.

Availability

The user can access the data and information anywhere and anytime he wants.

Confidentiality

Illegitimate people don't access personal data and information.

Data security problems in cloud can be considered in two categories:

Privacy and confidentiality:

The user should ensure that illegitimate users don't access his personal information.

Data security and Integrity:

The data should be secured using cryptography techniques. The cloud service provider should consider a method to monitor the generality of data.

However, there are still some concerns such as confidentiality and Integrity of data [2]. Therefore, data security is a very fundamental problem is providing cloud services. Data security in cloud computing has security challenges due to several reasons;

the first reason is using traditional encryption method which is considered as a threat for data and the users cannot control it and the second reason indicates that data in cloud servers are stored distributed and the user may update, remove or add data thus an advance technology is required to prevent abusing data and losing them. Cryptography architecture has been offered in this paper which is very simple, efficient and appropriate for cloud computing and only legitimate user can access to data and information. In second section the architecture of cloud computing, in third section the related works, in fourth section proposed architecture and in fifth one analyzing and evaluating this proposed model have been discussed. Finally, the conclusion and future researches have been illustrated.

Cloud Architecture

Generally speaking, cloud computing is divided into two categories of service providing and establishment models [3]. Service providing models include three main layers which have been shown in Figure 1.

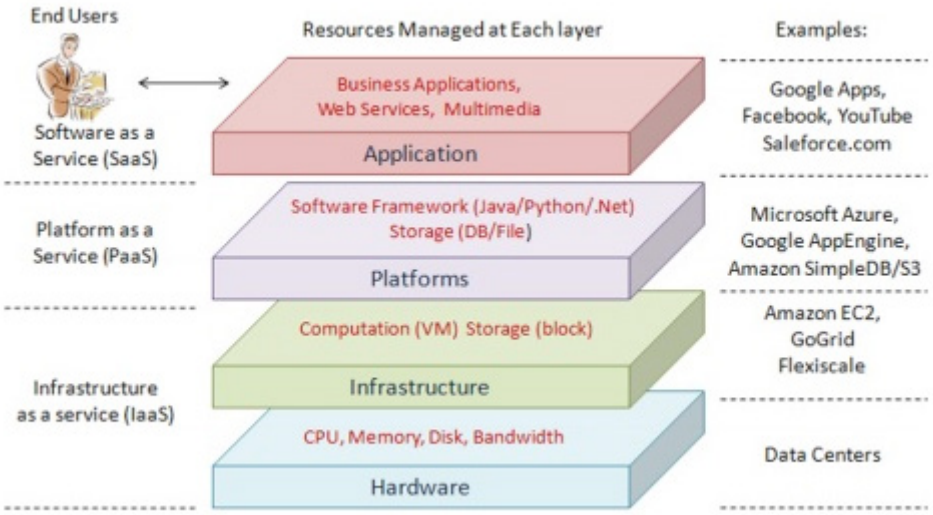


Figure 1: Different types of cloud service

Providing Model

Infrastructure as a Service (IaaS): The user can rent some infrastructures such as storing space, network and band width and use its services [4].

Platform as a Service (PaaS): The user can create software and locate in this layer and introduce it to others.

Software as a Service (SaaS): Using software such as web browser, the user can use cloud services. In this operational layer such as bill, the number of users and volume of resource consumption are identified.

The models of establishing cloud involve four types which have been shown in Figure 2.

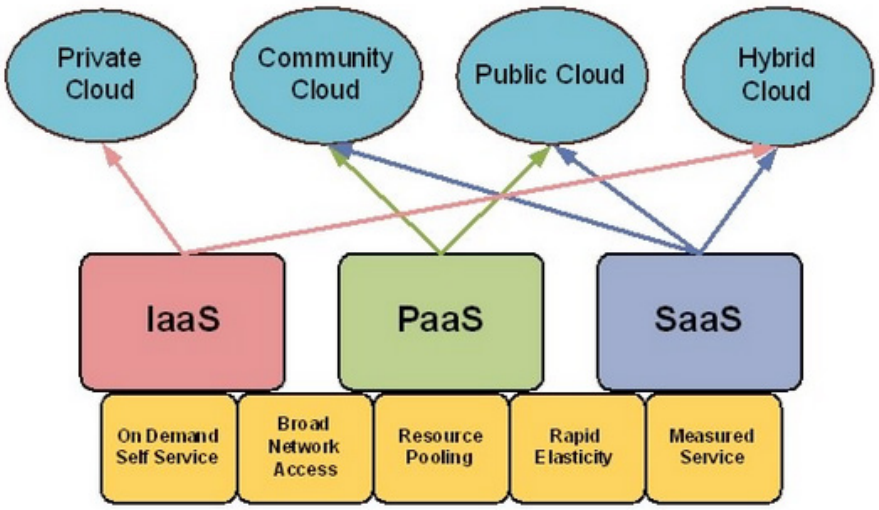


Figure 2: The model of cloud establishment

Different Types

Private cloud: It has been allocated to particular organizations. In private cloud, infrastructure computing is allocated the organization and won't be shared with other organizations [5].

Public cloud: This cloud is available for all users and everybody can use the infrastructures.

Hybrid cloud: It is a private cloud that can be expanded to public cloud. It is in fact a combination of public and private cloud. An organization can put private software with high security in its private cloud and a software with public application in public cloud.

Community cloud: Cloud infrastructures are shared for exclusive and conditional use by a particular population of consumers of an organization.

Related Researches

In a paper three steps are used for data security [6]. The first step produces the key using Hellman elliptic curve algorithm model. In the second step, the user confirms using digital signature and finally using HASH algorithm the file is encrypted. In the author proposes a framework for security on side of service receiver using AES cryptography algorithm [7]. In cloud providers' services are used for data security and IaaS layer is divided into two parts; one for maintaining cryptography algorithm with key and the other for encrypted files [8]. The user sends his request to PaaS layer. As the result the layer PaaS with two layers of IaaS are interacting, encrypting and decrypting user data. In the author considers a life cycle for data which consists of 6 sections [9]. 1- creating data 2-storing data 3- using data 4- sharing data 5- archiving data 6- removing data and security problems in these 6 levels have been investigated. As an instance in storing level, cryptography algorithms should be used for protecting data security and in transferring data that is sharing level, a secure protocol has to be used. In cryptography algorithms of AES and RSA have been proposed to protect data security in cloud computing [10].

In to protect data security in cloud, the author has proposed AES cryptography algorithm with a third party auditor [11]. The main task of third party auditor is identifying data security and confirming storing using HASH code. In fact, third party auditor prevents damaging data and identifies likely dangers for data which leads to reliability of data in cloud.

Proposed Method

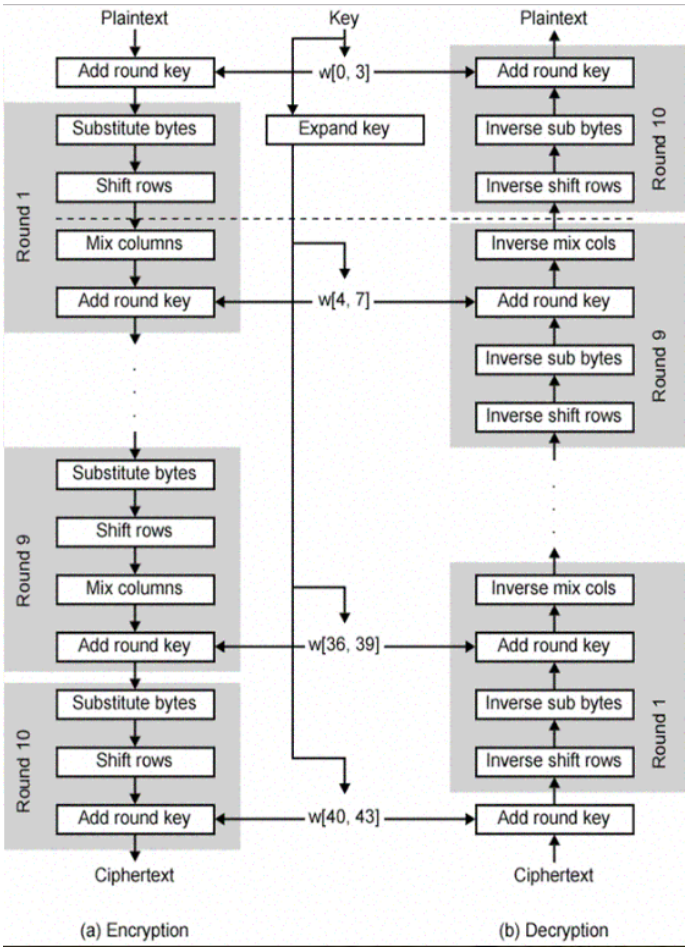


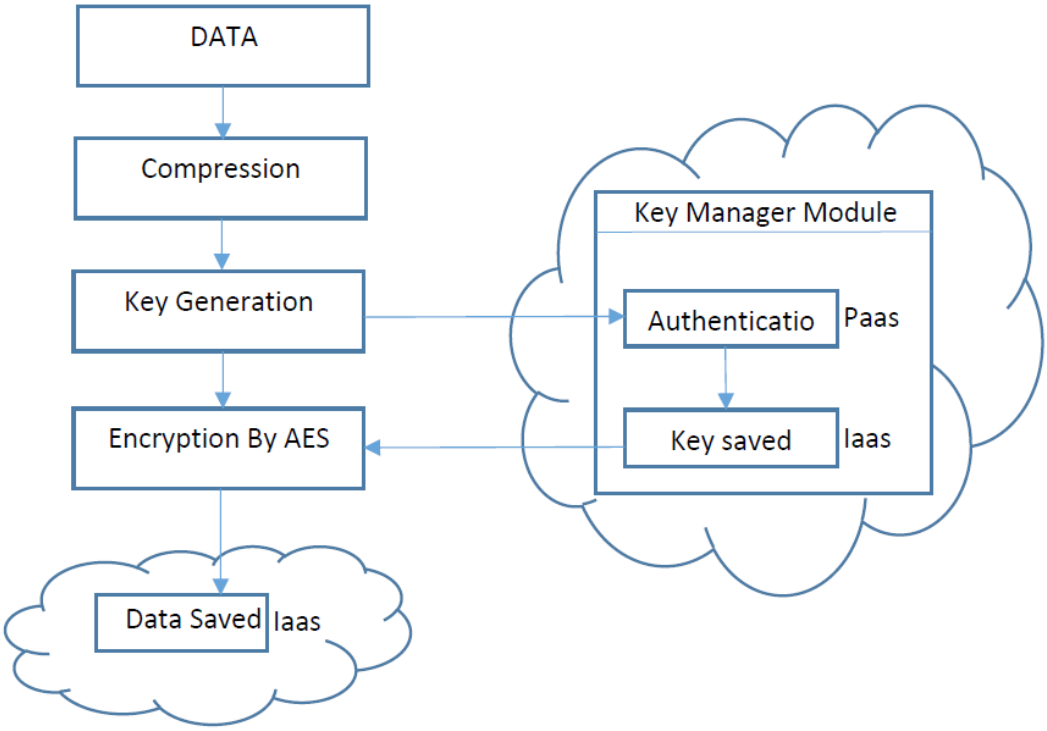
Figure 3: AES encryption algorithm [12]

In order to maintain the security, Integrity and confidentiality of data, symmetric encryption algorithm AES has been used. Symmetric encryption algorithm AES is a symmetric piece encryption algorithm with data format length of 128, 192 and 256 bits. Key length is also independent from format length of 128, 192 and 256 bits. Depending on the length of data format and the length of independent key, algorithm will be on 10, 12 and, or 14 rounds. AES contains the structure of key expansion that produces some sub-keys from the main key depending on the number of rounds that each round is added to the format of data. AES algorithm includes three important shifts of SubByte, ShiftRow and MixColumn [12] that the first one is an alternative non-leaner function providing the security of system and two last functions are linear functions for increasing the expansion and mix of algorithm (Figure 3). AES encryption algorithm with format length of 128 bits is used in proposed method. The reason of using AES encryption algorithm is the possibility of instructions and high security parallelism and as result high speed for cloud big data. The key of AES encryption algorithm is made using a module called the module of managing key based on combining username and password of user and stored in storing space of cloud.

The proposed method consists of two parts. The first one is loading data on cloud server and the second one is downloading data from cloud server on user's computer. In both two parts the security of user's data has been considered.

Loading data

Loading data consists of three phases (Figure 4).



First phase (Compression): First before encryption, the data should be compressed. Compression operation is Conducted using WINRAR software. Through this, the volume of data is reduced and encryption will be conducted with high speed and the data also occupy less volume on cloud servers .

Second phase (Producing key): While interacting cloud service provider (PaaS), the user should be authenticated. In this part the module of key management produces the key for encryption using the combination of username and password. This key is produced for any data which is supposed to be encrypted and stored in cloud securely by the module of key management [13].

Third phase (Encryption): In this section, the user's data are encrypted using AES encryption algorithm with produced key in key management module and then stored in cloud space.

Downloading data

Downloading data from cloud environment in proposed model consist of three phases (Figure 5).

(The first phase) extracting the key: The compressed data is first stored from cloud space on user's computer and then related key to the data is extracted by key management module and in next step decryption operation starts.

(Second phase) decryption: In this step, data decryption is conducted using extracted key from key management module with AES algorithm [14].

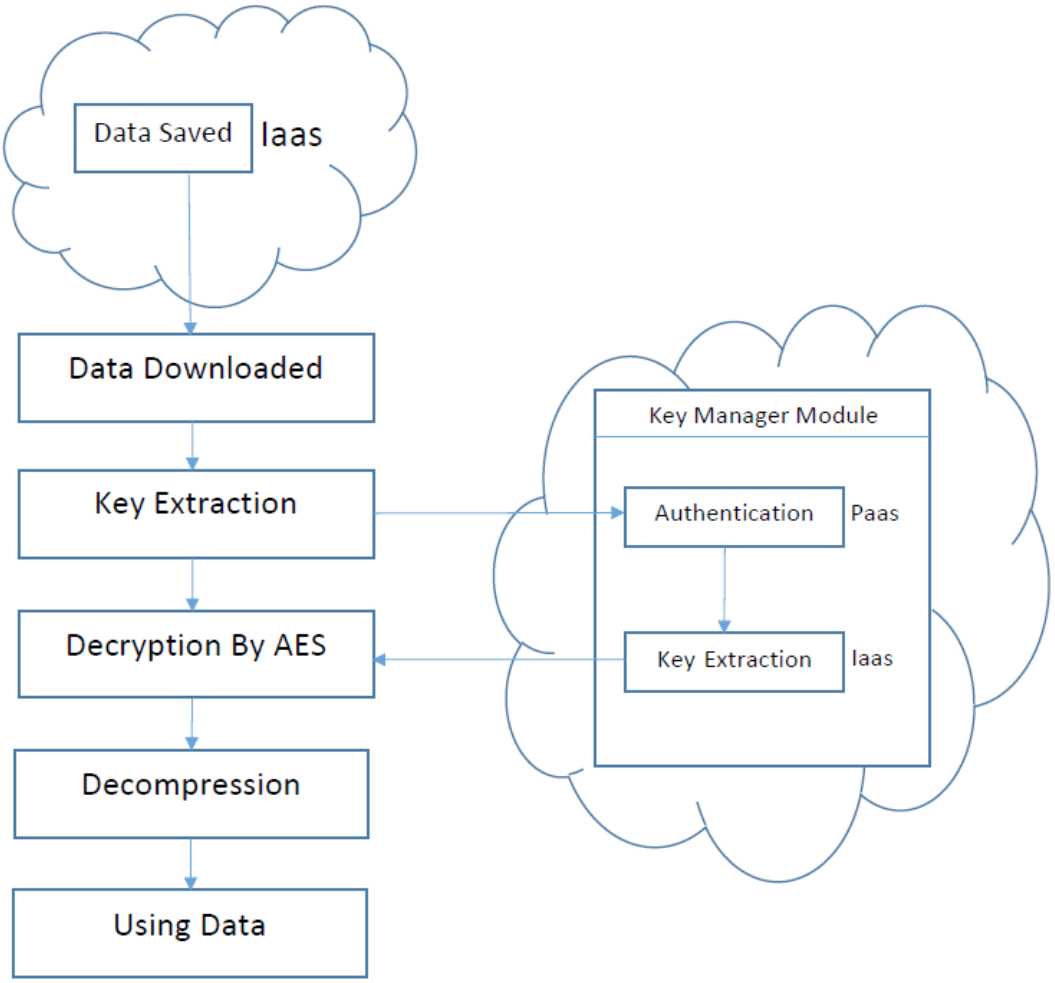


Figure 5: Proposed method of downloading data from cloud

Evaluation and Analysis

The evaluation of proposed model was investigated through two attitudes. The first one is comparison based on storing space of data in cloud and the second one is considered as comparison based on the speed and efficiency of proposed model. To do the experiments, a machine with properties of dual-core Intel processor with speed of 2.5 GHZ and RAM 4GB and HARD 500GB and Linux operating system has been used. First, comparison based on storing space is conducted. Three files with different sizes are compressed using compression software of WINRAR. The results are obvious that is encryption is conducted on compressed data; it occupies less space compared to encryption on uncompressed data (Table 1). In terms of speed and efficiency, encryption on compressed data has higher speed than uncompressed data [15].

Input File Size	File Size After Encryption	File Size After Compression And Encryption
50 KB	50 KB	34 KB
35 MB	35 MB	20.3 MB
70 MB	70 MB	44.5 MB

Table 1: Comparing the encryption of compressed data with uncompressed ones based on storage space in cloud Considering that in proposed method, AES encryption with format length of 128 bites has been used, figure 6 shows the comparison among various types of key size in AES encryption algorithm [11]

As it is clear from figure 6, there is less complexity in 128 bites key than 192 and 256 bites keys. To test the speed, the proposed encryption method was compared with other symmetric encryption algorithms such as DES and BlowFish (Figure 7). The results show that proposed algorithm encrypts the files faster and more secure than other algorithms

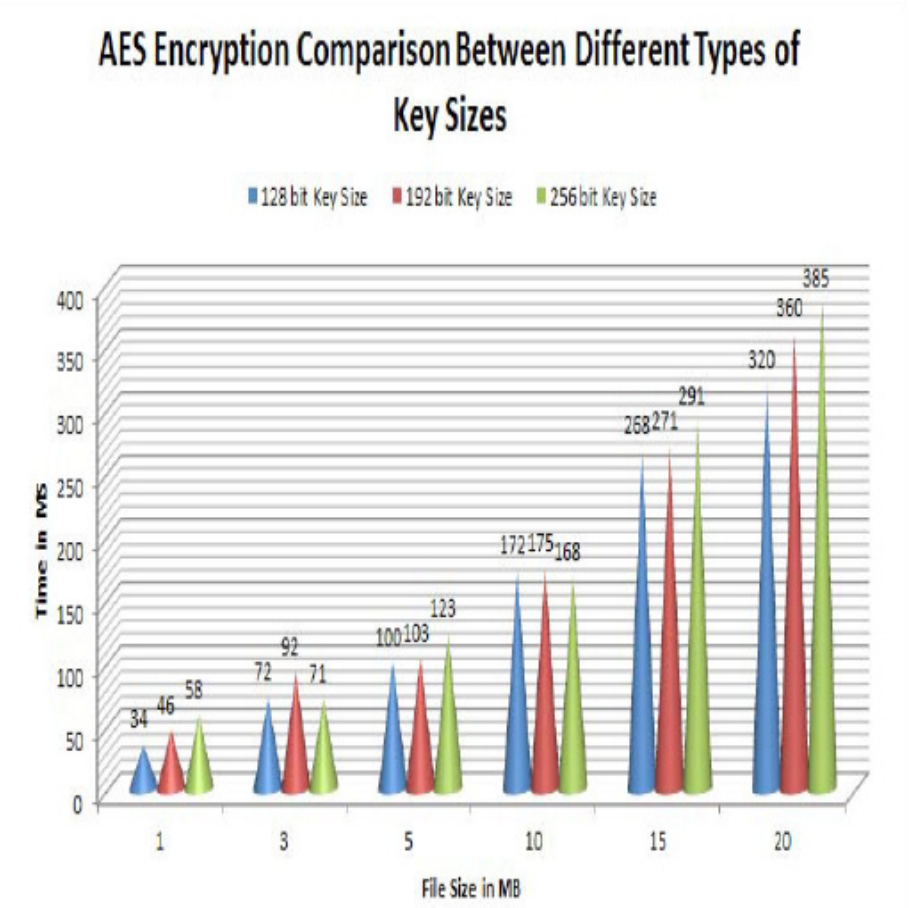


Figure 6: Comparing AES algorithm among various keys with different sizes

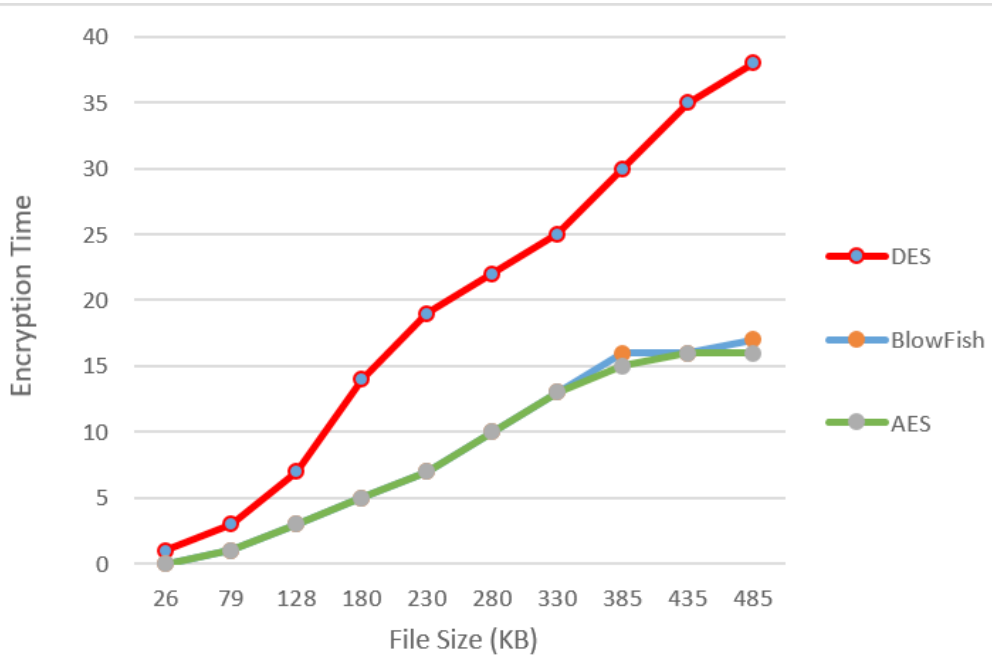


Figure 7: Comparing the speed of AES algorithm with symmetric encryption algorithms

Conclusion and future work

Using cloud computing services in future is a need for organizations and considering cloud storing space is necessary. Data Integrity and confidentiality are two main principles in organizations' data security. The security has to be considered either on the side of service receiver or cloud server. A method for providing the security of data before storing in cloud as well as reducing storing space

was proposed in this research and using key management module, the security of keys and their management were considered. We have proposed a plan in this paper which is very effective and efficient in order to ensure user's data in cloud storing space. The experiments showed that proposed plan leads to reduce cloud storing space and maintain the Integrity and confidentiality of user's data. We have also showed that proposed algorithm has a good speed. In case of hacking user's authentication, user's data and information can be hacked so as the future researches, a mechanism is recommended to be considered that authentication operation is conducted through a secure protocol and also parallel encryption is recommended to be used for cloud big data which increases the speed of encrypting data and proposed algorithm of AES is capable of parallelism which is absolutely effective for cloud big data.

References

1. Mell P, Grance T (2011) The NIST Definatin of Cloud Computing. NIST Spe Pub.

2. R Los, D Shackleford, B Sullivan (2013) The Notorious Nine Cloud Computing Top Threats in 2013. Cloud Security Aliance (CSA).

3. Amazon.com (2008) Amazon Web Services (AWS).

4. Cloud Computing Architecture (2015) Cloud, Networking & Data Analytics.

5. Anne Shields (2014) Must-know: Cloud computing services and deployment models.

6. Gupta A, Chourey V (2014) Cloud Computing: Security Threats & Control Strategy using Tri-Mechanism. IEEE Int Con ICCICCT Mill Valley, CA, USA.

7. Surv N, Wanve B, Kamble R, Mr.Sachin Patil, Katti J (2015) Framework for Client Side AES Encryption Technique in Cloud Computing. IEEE IACC.

8. Sarkar MK, Kumar S (2016) A Framework to Ensure Data Storage Security in Cloud Computing. IEEE UEMCON, New York, USA.

9. Sathyanarayana TV, Immaculate Sheela LM (2013) Data Security in Cloud Computing. Int Conf ICGCE.

10. Kaur M, Mahajan M (2013) Using Encryption Algorithms to enhance the data security in cloud computing. Int J Commu Comp Technol 1: No.12.

11. Shimbre N, Deshpande P (2015) Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm. Int Conf Compu Commu Cont Autom.

12. Pranav Agrawal, Short Tutorial on Advanced Encryption Standard.

13. Chouhan PK, Yao F, Sezer S (2015) Software as a service:understanding security issues. IEEE SAI Conference.

14. Serrano N, Gallardo G, Hernantes J (2015) Infrastructure as a service and cloud technologies. IEEE Software 2: 30-36.

15. Lindemann J (2015) Towards abuse detection and prevention in IaaS cloud computing. IEEE ARES Conference.