Indian Journal of Science and Technology, Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/100221, August 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Approach for Data Security from Malicious Attacker in Cloud Computing

Satish Kumar* and Anita Ganpati

Department of Computer Science, Himachal Pradesh University, Shimla – 171005, Himachal Pradesh, India;
skumar.hpu@gmail.com, anitaganpati@gmail.com

Abstract

Objectives: Cloud computing allows clients to access various IT resources online without much expenditure and investment. Although there are various advantages of cloud computing, but still various security threats exist in the cloud environment, e.g. data security, account hijacking, privacy and users' authenticity. **Methods/Statistical Analysis**: In this research paper, an empirical approach has been applied which is based upon the program implementation of the proposed model for data security in the cloud environment. The applied approach shows that the proposed model for data security will prevent the cloud data from the fraudulent activities that can be performed at both ends (i.e. cloud provider and cloud user). **Findings/Conclusion:** In this research paper, a model for data security has been presented which will protect cloud data from malicious insider attacks as well as fraud cloud user simultaneously. It is concluded that a single combined approach is enough to tackle the fraud at both ends i.e. at cloud user end and at cloud provider end. Implementation for above model is also done under compiler "Turbo C" and results are also shown in the form of screenshot for each case. It is also concluded that the cloud provider will have always a proof that he is not responsible for the corruption of cloud user's data unless he has cloud user's decryption key. **Application/Improvements:** The proposed model is applicable as a remedy for repudiation problems and providing better data security in cloud environment. The implemented program can be enhanced using high bit encryption method to improve and provide more data security to the cloud.

Keywords: Cloud Data, Cloud Security, Data Security, Encryption, Malicious Attacker, Repudiation

1. Introduction

Cloud computing is an elastic approach to utilize computing resources among different IT users to enable them to deploy computer processing power according to the users' needs. It makes convenient for cloud services' clients to set up and use cloud services, allowing the size of the computing infrastructure to raise when a cloud user needs to acquire more processing power while allowing them to scale down the resources when the users do not have requirement for extra cloud services. The overall usage of a cloud services leads to the optimization of computing resources so that it makes them cheaper for everybody involved[1]. Elasticity and Multi-tenancy are two vital characteristics of the cloud model. Elasticity enables scaling up and scaling down resources allocated to a service or cloud user based on the current service demands. Multi-tenancy enables sharing the same service instance among different cloud users (tenants). Both characteristics focus on improving resource utilization, cost and service availability.

In cloud computing, it is very important to examine data security at both ends i.e. at cloud end user site as well as at cloud provider site to prevent any fraudulent activity. At cloud provider site, there may exist a malicious person to misuse the cloud users' data and at the same time there may be a malicious person as well as on the cloud user site to misuse the capabilities of cloud services. There may be a scenario where the malicious person at cloud provider site has tempered the cloud users' data and repudiate at

*Author for correspondence

later time. The same case may also be applicable to the cloud user too after sending suspicious data to the cloud provider's site and then he repudiates There must be some mechanism to ensure that neither cloud provider nor cloud user repudiates.

1.1 Definition of Cloud Computing

National Institute of Standards and Technology (NIST) introduced cloud computing model[1] as "a model for enabling convenient, on-demand network access to a collective pool of configurable computing resources (e.g. computer networks, IT servers, storage space, applications and IT services) that can be quickly provisioned and released with least management effort or cloud provider interaction".

According to Amazon Web Services (AWS), cloud computing refers to the provision of computing resources to the cloud users on demand basis which are delivered to the clients over the network/internet while following pay-per-usage pricing model[2].

Gartner defined cloud computing as a technique of computing in which capabilities of cloud computing i.e. scalability and elasticity are provided to the clients using internet and web technologies[3].

1.2 Characteristics

Shared Infrastructure: All the cloud resources can be shared among multiple cloud users due to multi-tenant nature of the cloud computing[4].

Network Access: All the cloud services can be accessed through a web browser which allows thin clients to access cloud services over the network[4].

Handle Metering: The usage of all the cloud services are monitored and audited by the cloud providers so that cloud users have to pay for only that what they use[4].

1.3 Cloud Computing Models

There are two broad categories of cloud computing which depends upon the way how these models are deployed and services they provide. These are known as deployment models and service models. Each of these models is described below:

1.3.1 Deployment Models

According to NIST[1], deployment models refer to those models which are based upon the deployment of different computing resources. There are following type of deployment models defined by NIST[1]:

1.3.1.1 Private Cloud

A private cloud refers to that one in which the cloud services are provided only for a specific group of people within a single organization or private organizations.

1.3.1.2 Community Cloud

In community cloud the cloud services and infrastructure are provided for many different organizations which have some common goals and objectives.

1.3.1.3 Public Cloud

In public cloud, the services are provided to the general public. Most of the services are provided free of cost and some services are provided according to the pay-per-usage model. Security remains the main concern in case of public cloud.

1.3.1.4 Hybrid Cloud

A hybrid cloud consists of more than one cloud. The composition may include any of the private, community or public clouds. A hybrid cloud provides the facilities of all other clouds mutually to a cloud client.

1.3.2 Service Models

The cloud service models refer to those models which defines the kind of services provided by a cloud provider. There are three types of cloud services model discussed below[5]:

1.3.2.1 Cloud Software as a Service (SaaS)

In SaaS model, only software services are provided to the cloud user e.g. email facility, word processing power, portal facilities, virus scanning software's etc. In SaaS model, a cloud client pays as per time he uses the software services[6].

1.3.2.2 Cloud Platform as a Service (PaaS)

In PaaS model, the cloud infrastructure is provided as a platform to the cloud users i.e. computing tools and set of programming languages may also be serviced to the cloud user in PaaS model[7]. The cloud customer do have control only over the applications deployed by them but

do not have any control over the infrastructure provided by cloud provider[8].

1.3.2.3 Cloud Infrastructure as a Service (IaaS)

In IaaS model, the cloud infrastructure e.g. processing power, storage space and bandwidth etc. are provided to the end user.In IaaS, a lot of the services are delivered to the cloud user via a virtual terminal known as Virtual Machines (VMs). The entire infrastructure like memory space, CPU cores, system firewalls etc. are provided to the end users in IaaS service model[9].

2. Need and Scope of the Study

In a cloud computing environment, internal threats have steadily increased over the past few years[10]. Internal threat refers to those threats which occur within the organisation. A malicious user within an IT organisation often keeps more knowledge regarding the location and type of data stored within that organization and hence it is easy for them to hack and illegally access the data stored. Although there is no assured mechanism to eliminate internal threats completely, some effective methods can be developed to eliminate them. There must be a strong data protection mechanism to ensure the security of data stored at cloud and hence to prevent the unauthorised access to the stored information on the cloud.

3. Objectives of the Study

The objective of this research paper is to define and implement a secure mechanism for the protection of data stored at cloud from the malicious insider at cloud provider site as well as malicious cloud user at cloud user site. The given approach for data security also ensures that neither cloud user nor cloud provider can repudiate from the malicious activity committed by them.

4. Literature Review

There are many researchers who have discussed about various cloud data security issues. In this section, various literature reviews of some of these researchers are presented.

In[11] discussed the cloud security Service Level Agreements specifications (SLA's) regarding data recovery of data in case of data loss, location of the cloud and separation of data from different tenants. They concluded that the cloud users do not have any control over their own data and the processes using that a data in cloud environment.

In[12] discussed the issues regarding the security of cloud computing model. They concluded that with the advent of new and fast technologies, the risk for sensitive information like payment information etc. are also increasing at the same pace.

In[13] proposed an architecture for data security which was based on diffiehellman and elliptical curve cryptography algorithm. In their architecture they showed that it can be implemented in cloud environment by taking the advantages of cryptographic methods.

H. Sato et al.[14] focused on matters related to social insecurity of cloud and propose a model to overcome the insecurity issues. The proposed model is capable of creating the trust factor for both service provider and service users.

In[15] stated that there is a need of Third Party Auditor (TPA) for trusted storage and retrieval of data on the cloud.TPA makes task of cloud users (clients) easy by verifying the integrity of information stored on behalf of the cloud client. In cloud, there is support for data dynamics which means that cloud users can insert, delete or update the information stored onto a cloud.So there should be strong security mechanism which ensures integrity of the information stored on a cloud. They stated that TPA can not only see the information but he can also access that information or he can modify also, so there should be some secure mechanism against such activity.

In[16] studied the case of data leakage in famous cloud service provider Amazon's Elastic Compute Cloud (EC2). They presented an in-depth analysis that showed a variety of strategies that virtual machine owners might use if they were interested in engaging in malicious behavior in a cloud environment

In[17] used Advanced Encryption Standard (AES) cryptographic method for data security and provided the file level security to end users of cloud. They proposed a technique to encrypt the files with encryption keys and by those keys, all the information will be in encrypted manner. This approach to encrypt information is very useful because only authorized persons could read analyze the information stored in the cloud.

In[18] in their paper presented the significance of cloud data security and the existing security techniques for the cloud. They emphasized on the reliability and trusted

relation between the cloud provider and cloud user. They also stated that the cloud provider's and the cloud users must provide mechanisms to keep cloud environment safe from the outside threats.

In[19] investigated the problem of byzantine failure, modification attack due to malicious data and even server colluding attacks. They also discussed security issues for storing data onto the cloud if the system is distributed. They stated that insertion, deletion and updation operation in the database in cloud environment may lead to the inconsistency and insecurity for cloud users.

In[20] has developed the secure cloud data center framework and emphasized that the security mechanism to cloud environment must not be implemented in isolation but they must be implemented all the layers of cloud architecture to ensure the safety of information.

In[21] discussed four trust factors for securing cloud namely control, ownership, prevention and security. Further, the challenges for faith and trust are identified as diminishing control and lack of transparency. They concluded that these four factors play an important role for maintaining trust among the cloud users.

5. Proposed Model for Cloud Data Security

The proposed model ensures that no fraudulent activity can take place on the behalf of both malicious insider (at cloud provider site) as well as malicious outsider (at cloud provider site). To explain the data security model, let us take an example. Suppose "A" is cloud user who wants to store his data on the storage provided by cloud provider denoted by "B". There is an agreement signed between both the cloud user and cloud provider which states that "in case of data corruption or loss to the cloud user's data, the cloud provider has to pay compensation (e.g. 1000 dollars)".

Now let us take two cases in which first cloud user is fraud and the other one in which cloud provider (malicious insider) is fraud.

5.1 Case 1: Cloud User is Fraud

According to above example, if cloud user is fraud and sent the corrupted data himself to the cloud storage provided by cloud provider intentionally and blame that someone at cloud provider's site has corrupted his data and claim for money, then in that case provider must have some mechanism to show that the cloud user was fraud and he had already sent the corrupted data. Otherwise, the cloud provider has to pay compensation to the cloud user. The proposed model for data security to prevent this fraudulent activity will not allow this to happen. Because first the data sent by the cloud user is encrypted by cloud provider's encryption key and then by cloud user's own encryption key. So the cloud provider will not be able to access the cloud user's data unless he has the cloud user's decryption key. So it will be a proof for the cloud provider that he has not corrupted the cloud data.

5.2 Case 2: Cloud Provider is Fraud

In the second case, the cloud provider can itself be the source of malicious activity. A malicious insider in a cloud provider's site is a mischievous threat to the cloud provider as well as cloud clients. That malicious insider maybe an employee within the cloud provider premises, It maybe any current employee, former employee, company contractor or any business associates, who have knowledge regarding the metadata, location of data and metadata, security policies, practices and documentation manual of the organization. These malicious insiders can be involved in any of the malicious activities like fraud, theft of confidential information or any intellectual or sensitive property, or may damage the computer systems. In the proposed data security model it is not possible to access the data stored at the cloud because for that the malicious insider requires both decryption keys i.e. one of cloud user's decryption key and another one is cloud provider's confidential decryption key.

Hence in this way, the proposed model for data security ensures to prevent any fraudulent activity to take place simultaneously by the fraud cloud user as well as any malicious insider at cloud provider's site.

5.3 Step-Wise-Step Working of Proposed Framework

Step 1: Cloud User (denoted by CU) enters the URL of cloud provider website in his browser. Login GUI is loaded in the browser.

Step 2: After Successful login, User wants to send the data to cloud provider for storage. Suppose original data is denoted as 'D'.

Step 3: First cloud user asks an encryption key from cloud provider to encrypt data.

Step 4: Upon receiving encryption key (denoted by CP_{EK}) from cloud provider, cloud user encrypts his data with that key (denoted by $D_{PE)}$as shown in Figure 1.

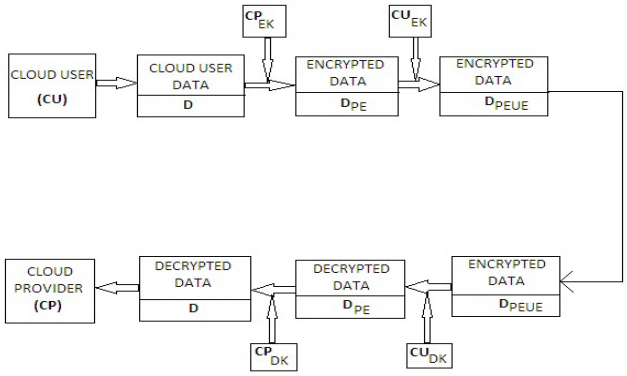

Figure 1. Working sequence of proposed model for data security

Step 5: Cloud user, then, encrypts again the data with his own encryption key (denoted by $CU_{EK)}$ and hence final data is prepared which is to be sent to the cloud provider, denoted by $D_{PEUE.}$

Step 6: Now at Cloud Provider Site, If there is a malicious user who wants to access the cloud user's data must require cloud user decryption key (denoted by CU_{DK}) to decrypt that data and access that, so the malicious user can't perform any fraudulent activity without cloud user permission or cloud user decryption key.

Step 7: Then cloud provider asks cloud user for his decryption key. The cloud user sends his decryption key to the cloud provider (denoted by CP).

Step 8: Cloud provider applies cloud user decryption key (CU_{DK}) to the received data and then finally applies his own decryption key (denoted by CP_{DK}) to the data and access the original data (D) sent by the cloud user.

6. Coding and Implementation

In this section, the implementation and coding of above scheme is given. The code for above scheme is written in C language. "Turbo C" Compiler has been used for writing and compiling the given code which is given as following:

6.1 Coding

In the program given below, there are three strings declared namely message, fcipher and scipher. Fcipher and scipher stands for first cipher and second cipher respectively. Original message is stored in "message" string and then after encrypting it with the cloud provider key (denoted by cpkey), the output is stored in "fcipher" string. Finally "fcipher" string is again encrypted with the cloud user key (denoted by cukey) and the final output is stored in "scipher" key which represents the string to be sent to the cloud user. It is a symmetric type of algorithm for encryption which uses the same decryption key as encryption key, so no different variables for storing decryption key are declared.

```
/*Program for Implementing Data Security Model using encryption*/

    #include<stdio.h>
    #include<conio.h>
    void main()
    {
    int message[10],fcipher[10],scipher[10];
    inti,cpkey=0,cukey;
    clrscr();
    printf(«\t<-----PROGRAM FOR USING TWO-KEY METHOD FOR CLOUD DATA SECURITY----->» );
    printf(«\n\nAT CLOUD USER SITE :»);
    printf(«\n\nEnter the message : «);
    for(i=0;i<10;i++)
    {
    scanf(«%c»,&message[i]);
    }
    printf(«Enter Cloud provider key : «);
    scanf(«%d»,&cpkey);
    if(cpkey==247)
    cpkey=247-26;
    for(i=0;i<10;i++)
    {
    fcipher[i]=message[i]+(cpkey*29%247);
    }
    printf(«\n»);
    printf(«Cipher text enrypted using cloud provider key is : «);
    for(i=0;i<10;i++)
    {
    printf(«%c»,fcipher[i]);
    }
    printf(«\n\n»);
    printf(«******* Now Next Step is to encrypt message by cloud user key ********»);
    printf(«\n\nEnter Cloud User key : «);
    scanf(«%d»,&cukey);
    for(i=0;i<10;i++)
    {
```

```
scipher[i]=fcipher[i]+(cukey*29%247);
}
printf(«\n»);
printf(«Cipher text enrypted by cloud user key is : «);
for(i=0;i<10;i++)
{
printf(«%c»,scipher[i]);
}
printf(«\n||||||||||||||||||||||||||||||||||||||||||||||||||»);
printf(«\nAbove message is to be sent to the cloud provider»);
printf(«\n\nAT CLOUD PROVIDER SITE»);
printf(«\nRequest Cloud user to enter key : «);
scanf(«%d»,&cukey);
for(i=0;i<10;i++)
{
fcipher[i]=scipher[i]-(cukey*29%247);
}
printf(«\nCipher text decrypted by cloud user key is : «);

for(i=0;i<10;i++)
{
printf(«%c»,fcipher[i]);
}
printf(«\nEnter Cloud provider's key : «);
scanf(«%d»,&cpkey);
if(cpkey==247)
cpkey=247-26;
for(i=0;i<10;i++)
{
message[i]=fcipher[i]-(cpkey*29%247);
}
printf(«\nOriginal Message decrypted by cloud provider key is : «);
for(i=0;i<10;i++)
{
printf(«%c»,message[i]);
}
getch();
}
```

6.2 Screenshots and Results

6.2.1 Case 1: When Right Message is Evaluated

In first case, we will discuss the scenario assuming that the true (accurate) message is retrieved and decrypted at cloud provider's site. First of all, the cloud user will be prompted to enter the message (data) which he wants to send onto the cloud provider's site as shown in Figure 2.

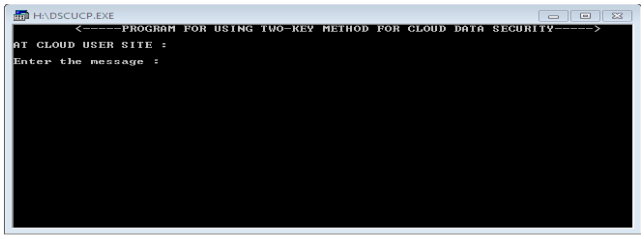

Figure 2. Output screen when executing the above code first time.

As cloud user enters the right message, the message must be encrypted with the cloud provider's encryption key first. It is shown in Figure 3 that cloud user is entering the cloud provider's encryption key, i.e. 456. After execution of encryption algorithm, the message 'SECRET MSG' will be converted to the cipher text. Finally again the cipher text obtained will be encrypted using cloud user's own key i.e. 65. So, final message which must be sent to the cloud user is encrypted as "tfdsfuAnth" as shown in Figure 3.

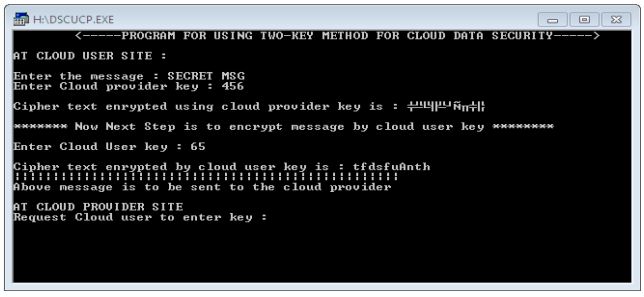

Figure 3. Output screen for entering message, cpkey and cukey

Next step is to decrypt the original message ("SECRET MSG") at the cloud provider site. So the cloud provider asks cloud user to send his decryption key i.e. 65 and then apply on it, then after finally applying his own decryption key i.e. 456 to the data and retrieves the original message as shown in Figure 4.

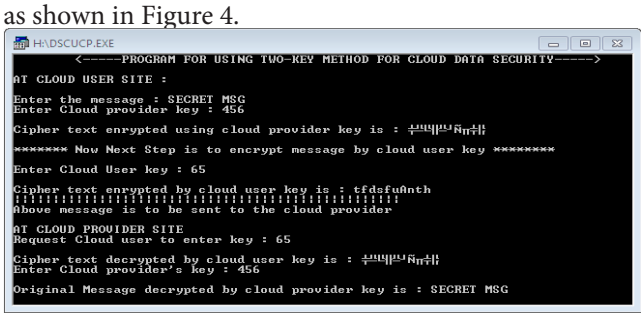

Figure 4. Output screen when right message is decrypted using right cloud user key.

6.2.2 Case 2: When Wrong Message is Evaluated

In this case, the malicious insider (at cloud provider's site) cannot access the cloud data without knowing the decryption key of cloud user. It is shown in Figure 5 that wrong message is evaluated when the malicious insider doesn't know the right cloud user key and enters wrong cloud user key i.e. 78 instead of 65 as well as wrong cloud provider's key 65 instead of 456.

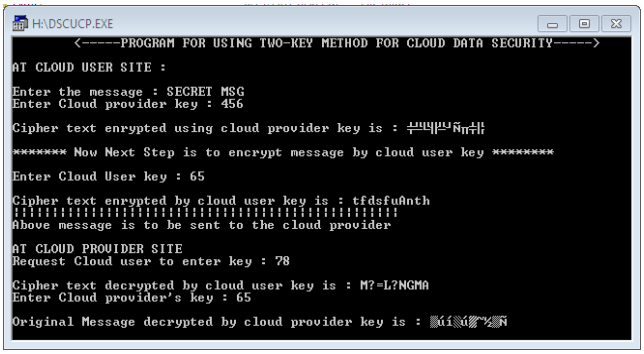

Figure 5. Output screen when wrong message is decrypted using wrong cloud user key.

7. Conclusions

In this research paper, we have discussed various techniques applied for data security and found that no one has given a solution for fraudulent activity that can take place even at the cloud user end. We have given a model for data security which will protect cloud data from malicious insider attacks as well as fraud cloud user simultaneously. So a single combined approach is enough to tackle the fraud at both ends i.e. at cloud user end and at cloud provider end. Implementation for above model is also done under compiler "Turbo C" and results are also shown in the form of screenshot for each case. It is also concluded that the cloud provider will have always a proof that he is not responsible for the corruption of cloud user's data unless he has cloud user's decryption key.

8. References

1. Mell P, Grance T. The NIST definition of cloud computing. National Institute of Standards and Technology, Gaithersburg, MD 20899-28930, 2011 September, 1.
2. Amazon Web Services LLC. Amazon EC2 Cloud Service SLA. http://aws.amazon.com/ec2-sla, Date accessed: 13 February, 2016.
3. Cloud computing technology. http://www.gartner.com/technology/topics/cloud-computing.jsp. Gartner Researchers, Inc. and its Affiliates, Gartner Research and Analysis Section, Date accessed: 17 /03/2016.
4. Malik A, MohsinNazir M. Security Framework for Cloud Computing Environment: A Review. Published in Journal of Emerging Trends in Computing and Information Sciences. 2012 March; 3:1-10.
5. Gens F, Mahowald RP, Villars RL. Cloud computing: benefits, risks and recommendations for information security. International Data Corporation (IDC) Cloud Research. 2009 November; 1-125.
6. Randles M, Lamb D, Bendiab AT. A Comparative Study into Distributed Load Balancing Algorithms for Cloud Computing. IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, 2010 June, 551-56.
7. Cloud computing: benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA). 2009 November; 1-125.
8. Grobauer B, Antony A, Walloschek T, Stocker E. Understanding cloud-computing vulnerabilities, In: IEEE Security and Privacy. June 2010, 99.
9. Morsy MA, Grundy J, Müller I. An analysis of cloud computing security problem. In: Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 2010 November.
10. Kofi K. Fletcher Cloud security requirements analysis and security policies development using a high-order object-oriented modelling technique. Presented to the Faculty of the Graduate School of the Missouri at University of Science and Technology, Missouri, 2010 April.
11. Kandukuri RB, Atanu Rakshit RP. Cloud security issues. Proceedings of the IEEE International Conference on Services Computing, 2009 September, 517-520.
12. Popovic K, Hocenski Z. Cloud computing security issues and challenges. In: The Third International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services, July 2010, 344-349.
13. Tirthani N, Ganesan R. Data security in cloud architecture based on Diffee Hellman and elliptical curve cryptography, International Association for Cryptological Research, Eprint Version. http://eprint.iacr.org/2014/049.pdf.
14. Sato H, Kanai A, Tanimoto S. A Cloud trust model in a security aware cloud, 10th Annual International IEEE/PSJ, Symposium on Applications and the Internet, 2010 August.
15. Makhija B, Rajput VKJI. Enhanced data security in cloud computing with third party editor, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). 2013 February; 3(2):341-345.
16. Tromer RT, Shacham EH. Savage Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, Proceedings of the 10th Association of

Computer Machinery (ACM) Conference on Computer and Communications Security (CCS), 2009 November.
17. Bhatt TP, Mehta A. Security in cloud computing using file encryption. International Journal of Engineering Research and Technology (IJERT). 2012 November; 1(9).
18. Ashalatha R. A Survey on Security as a Challenge in Cloud Computing, International Journal of Advanced Technology and Engineering Research (IJATER), at National Conference on Emerging Trends in Technology (NCET-Tech), 2012 July, 2(2).
19. Ren WQ K. Lou Ensuring data storage security in cloud computing. IEEE Conference Publication at IWQoS, 17th International Workshop on Quality of Service, 2009 July.
20. Bakshi K. Cisco Cloud Computing-Data Center Strategy, Architecture and Solutions, Point of View White Paper for U.S. Public Sector, 1st Edition, April 2009.
21. Khan KM, Malluhi Q. Establishing Trust in Cloud Computing. IEEE IT Professional Publication. 2010 August; 12(5):20-27.