© 2016 IJSRSET | Volume 2 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Framework to Secure cloud Data Server Information Using Data Obfuscation

Juli Chaudhari[1], Bakul Panchal[2], Krunal Suthar[3]

[1]Computer Engineering, Merchant Engineering College, Basna, Gujarat, India
[2]Information Technology, L. D. Engineering College, Ahmedabad, Gujarat, India
[3]Computer Engineering, Sankalchand Patel College of Engineering, Vinegar, Gujarat, India

ABSTRACT

Cloud computing provide a high amount of virtual storage to the user. Cloud storage mainly help to small and medium scale industries to reduce their investment and maintenance of storage server. Users' data are sent to the cloud is to be stored in the public cloud environment. Data stored in the cloud storage might combined with other users' data. So, the issue about Security of cloud storage is ensured through confidentiality parameter. To ensure the confidentiality, the most common used technique is encryption. But encryption alone doesn't give maximum protection to the data in the cloud storage. To have efficient cloud storage confidentiality, this paper uses encryption and obfuscation as two different techniques to protect the data in the cloud storage. Applying encryption and obfuscation techniques on the cloud data will provide more protection against unauthorized usage. The proposed scheme, guarantees along with encryption, obfuscation technique is used to increase the confidentiality of data and also provide the verification & right management .where the users data is secure on the server. We hope this paper will help quality analyst in pulling data, is secure to store in the cloud storage with more accuracy with higher speed and verify content by preserving privacy.

Keywords: Cloud Storage, Data protection, Confidentiality, Encryption, Obfuscation.

I. INTRODUCTION

A. Cloud Computing

The term "Cloud" in Cloud computing is the communications network or a network which Combined with computing infrastructure. It is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. cloud storage is designed for virtualized environment. The cloud storage is implemented using cloud computing that means utilizing the software and hardware resources of the cloud computing service provider.

In today's IT industry, the more sophisticated data storage is Cloud storage. Cloud Storage provides a virtual space to store bulk data. But the data owners have no control over their data. The Cloud provider has full control on the user's data. This makes the user's mind to thing about the data security in the cloud. So, ensuring confidentiality of user's data in Cloud storage is the main research problem around the Cloud computing.

Data protection in the cloud storage is the core security problems. Data protection [2] is concerned with data confidentiality, integrity, authentication, availability and so on. **Data confidentiality** means that only authorized persons can use the data. **Data integrity** refers to information that has not been modified or remains untouched. **Authentication** refers to the process of verifying whether the incoming user is authorized or not. **Data availability** refers to the ability to guarantee to use data in time when needed and also refers to the availability of cloud service provider on-demand.

This paper proposes an efficient cloud storage confidentiality technique by using encryption and obfuscation technique [4]. Normally, confidentiality is

ensured by encryption technique, but for the cloud environment encryption alone is not enough for data protection. Encryption is integrated with obfuscation technique. Obfuscation technique alone is also not enough to adopt for complete confidentiality of data in cloud storage because the user can find values through reverse engineering or by using brute force technique, which may compromise cloud data security. This paper uses encryption and obfuscation techniques in an integrated manner to protect the data from the attackers (insiders and outsiders). In the proposed technique, users should encrypt data whatever they want to send to the cloud storage and the server can obfuscate the user_id & filename and after that store in on the cloud database. The Encryption done from user's side and Obfuscation of userid &filename done at server side. After sending the file on the cloud the cloud service provider can obfuscate user id and filename and then save to the storage database.

B. Data Security

Your Data confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or devices. Hence, we must make sure that users‟ data is not disclosed to service providers in any aspect of the cloud computing systems, including applications, platforms, CPU and physical memories.

1. Why data Obfuscation required in Cloud computing Environment?

i. Data Confidentiality Protection

Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or Devices. Users' confidential data is disclosed to a service provider if all of the following three conditions are satisfied simultaneously.[1]The service provider knows where the users' confidential data is located in the cloud computing systems.[2]The service provider has privilege to access and collect the users' confidential data in cloud.[3]The service provider can understand the meaning of the users' data.

ii. Problems With Current Cloud Computing

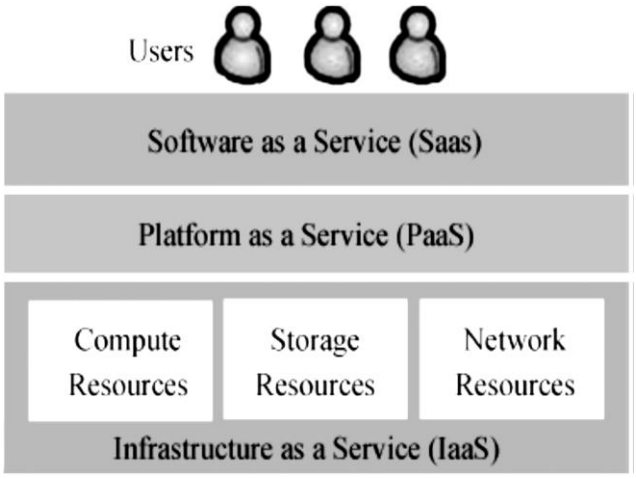


Figure 1. Cloud Computing System Architecture

The following are the major problems of current cloud computing system:

A. Each service provider has its own software layer, platform layer and infrastructure layer. When a user uses a cloud application from a service provider, the user is forced to use the platform and infrastructure provided by the same service provider, and hence the service provider knows where the users' data is located and has full access privileges to the data.

B. The user is forced to use the interfaces only provided by the service provider, and users' data has to be in a fixed format specified by the service provider, and hence the service provider knows all the information required understanding users' data.

iii. Approach to Protect Confidentiality

In our approach, we have the following five entities : Cloud ,Infrastructure Cloud, Encryption, Data Obfuscation and Data De-Obfuscation.

1) **Cloud:** A Software Cloud provides software as a service upon users' requests.
2) **Infrastructure Cloud:** An Infrastructure Cloud provides virtualized system resources, such as CPU, memory, and network resources. An authenticated user can request a virtual machine on which the user can deploy any platform or os to execute service instance.
3) **Encryption:** This technique offers the option of leaving the data in place and visible to those with the appropriate key while remaining effectively useless to

anybody without the key. This would seem to be a very good option – yet, for anonymous test databases, it is one of the least useful techniques.

4) **Data Obfuscation :**A Data Obfuscator is provided by a Server that can be deployed on a virtual machine in an infrastructure Cloud. The Data Obfuscator provides an operating system environment for software service instance to be run in an Infrastructure Cloud.
5) **A Data De-obfuscator:** It de-obfuscates obfuscated data so that a user can see the plain data. A Data Deobfuscator.

Obfuscation[4]

Obfuscation is look for, only to resist attacking during small time. It is largely an "art" rather than science. Obfuscation is a form of data masking where data is purposely scrambled to prevent unauthorized access to sensitive materials. There is various form of technical protection of intellectual property which are available to software developer. The basic idea of our proposed method is to secure the user information, who upload file on the cloud, as well as the file name also. Using this method, each user can protect his/her own data more effectively. Detailed implementation will be discussed in the next section

2. Objective

This research has following specific goal:

- ✓ To Enhance the security of existing solutions.
- ✓ To provide faster solution using proper Obfuscation method.
- ✓ To establish a trust(authentication) between sender and receiver.
- ✓ To achieve solution in short time with higher security.
- ✓ To provide hashing based verification.
- ✓ The Prevention methods like encryption, authentication , integrity are enough at client side while obfuscation is important at server side.
- ✓ The goal of obfuscation is to make attacking complicated enough to repel attacker, rather than formally proving the strength of algorithm.

3. Literature Review

Obfuscation is approach of information or data hiding method has recently become very important in a number of importance areas. Document increasingly make available with distinguishing but ordinary marks, which may contain a hiding copyright notice or serial number or even help to avoid or prevent unauthorized copying directly. The Scenario of the Obfuscation is shown in below figure[13].

As shown in the figure the general Scenario of Obfuscation used for hiding the data or information(like user id, file name,), that is transmitted on Cloud server for storage.

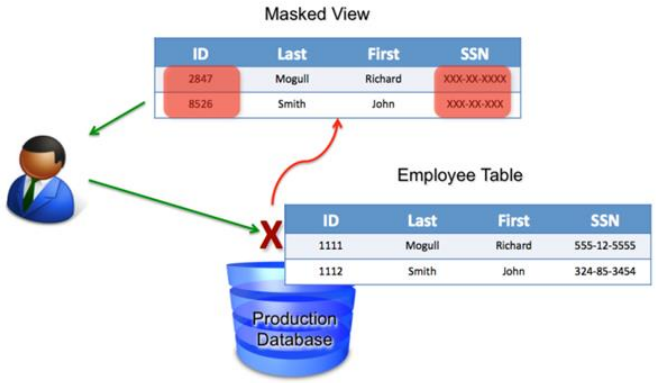


Figure 2. https:// securosis.com/blog/understanding-and-selecting-data-masking-how-it-works [14]

Here, in this fig we define that actually the user information is like employee table .But after apply obfuscation technique the SSN (social security number) is masked. So when hacker try to fetch it its look scramble. In final summary Obfuscation is:

Christian Collberg,Clark Thomborson,Douglas Low in[5] define different type of obfuscation. **[1]Code Obfuscation:** which convert Programme into more difficult to understand and reverse engineer. Once original format is gone it can not be recover. **[2]Control Obfuscation:** control flow of programme is changed (while same computation functionality is continued.) **[3] Data Obfuscation:** is also known as data scrambling and privacy , preservation that is changing the data structure appearing in the source code. Data obfuscation (DO) is a form of data masking where data is purposely scrambled to prevent unauthorized access to sensitive materials. This form of encryption results in unintelligible or confusing data. This can be classsified into techniques

that affect Storage and Encoding, Aggregation and Ordering.

Strength of Obfuscation Technique[5]:-

Domain	Techniques	Potency	Resilience	Cost
Transform	Code	Medium	One-way	Free
Transform	Data	High	Two-way	Cheap
Transform	Control	Medium	Partial One-way	Costly

Table 1 : Comparison Between Various Obfuscation Technique[5]

Muhammad Hataba and Ahmed EI-Mahdy in [6] give the Knowledge of Data Obfuscation.

• **Storage:** Used to choose unnatural storage class for dynamic & static data. • **Encoding :** Encoding used to choose unnatural encoding for common data type. • **Aggregation :** The main work of reverse engineering is to restore the program data structure.so, important for obfuscator is try to hide this data structure. • **Ordering :** Randomizing the order in which computation are perform is useful obfuscation.

A Net 2000 Ltd. White Paper in [10] Data Obfuscation Techniques. **1. Character Scrambling-** The characters contained within a given statement are re-ordered in such a way that its original value is obfuscated. **2. Repeating Character Masking-** Only a few of the last numbers appear in plain text with the remainder of the number being replaced with a series of "x" or "*" characters. **3. Numeric Variance-** The numeric values that are stored within a development database can be changed, within a defined range, so as not to reflect their actual values. **4. Encoding-** A series of characters is used to represent another value. Masking data, besides being the generic term for the process of data anonymization, means replacing certain field with a mask character.

Dr. L. Arockiam and S. Monikandan in [7] Author proposed a new Confidentiality technique to address the data security problem. In the proposed method, represent the cloud storage confidentiality protection system using encryption and obfuscation technique. Encrypted data are stored on storage server while secret key(s) are retained by data Owner, access to the user is granted by issuing the corresponding data decryption keys. Along with encryption, obfuscation technique is used to increase the confidentiality of data. The Proposed technique is secure to store the cloud user's data in the cloud storage.

Atiq ur Rehman,M.Hussain SZABIST in [8] author presented a model to preserve confidentiality of data stored in cloud database like DaaS. Model has two main features. The first one cover that how to store data into the DaaS. Second feature cover that how to query data from DaaS so that confidentiality of data could not compromised specially by the database administrator. The proposed model focuses on to query ovser encrypted plus obfuscated data. All query transformed on client side to execute over encrypted and obfuscated, stored into database of CSP.

Arvind Narayanan and Vitaly Shamatikov in [9] In this research paper researcher introduced in detail the different concept of privacy. Consider a data owner who wants to distribute a database to potential user. Instead of hiding individual data entries, he wants to obfuscate the database so that only certain queries can be evaluated on it. The goal is to ensure that the database, after it has been given out to users, can be accessed only in the ways permitted by the privacy policy.This paper proposed a new concept of database privacy, which is based on permitted queries rather than secrecy of individual records, and realized it using provably secure obfuscation technique.

Martin M,Agnew G.,Bole.J,Page M,Rhodes W.in [10] This paper proposes a new Procedure IRM. Author are recommended to implement IRM in order to prevent data leakage. It is much more secure than shared password and IRM rights can still be modified after information has already been broadcasted. Education, arousing people's awareness of the danger linked to the publication of unprotected documents, is the key to improve global security.

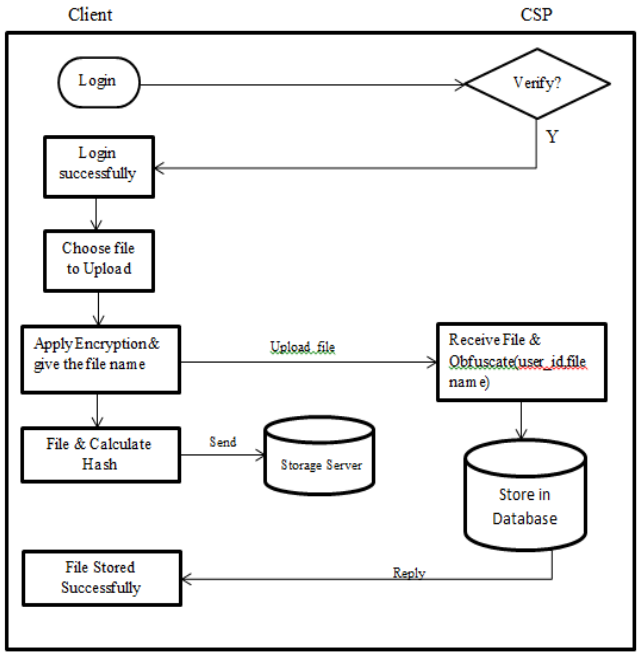
II. METHODS AND MATERIAL

Cloud computing provides an efficient storage setting to store and retrieve the cloud users critical data. Ensuring data security is a vital role to cloud users as well as cloud providers. This paper uses the confidentiality parameter to address the data security problems. Fig.2 represents the cloud storage confidentiality protection system using encryption and obfuscation technique. All the data must be encrypted before it is sent to the cloud database and Obfuscate before store on cloud database. Encryption of cloud data is done in the user side. The key used for encryption algorithm is generated in the
user environment.

Generally, Confidentiality is ensured by encryption algorithm. For cloud data storage, Symmetric encryption is best choice, because symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data [7].

Our approach can be depicted in Fig. In our approach, the obfuscation technique is improve the data confidentiality in cloud storage.

1. Upload Data on Cloud



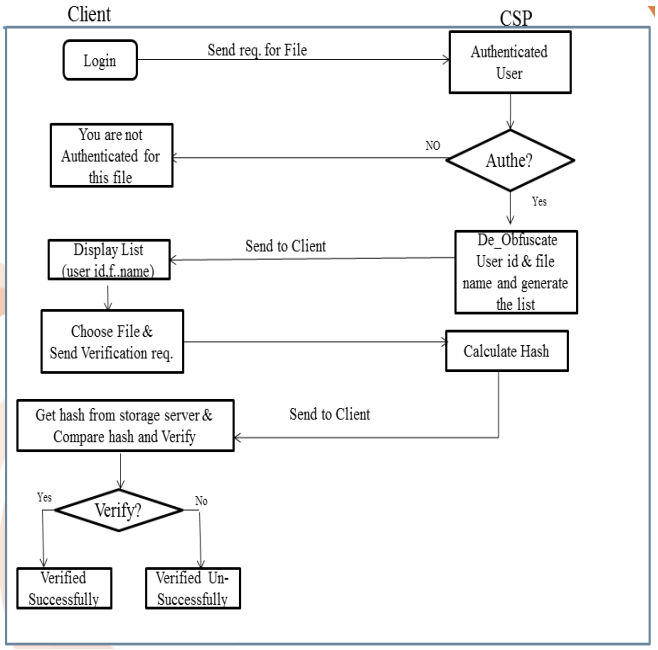
Algorithm #1

1. Input Login Detail
2. Then(Login Detail is Verify?)If Yes then Go to Step 3,
   Otherwise Go To Step 1.
3. Client Choose File and apply encryption on that file
   and give the name of that that file. After that upload file on cloud storage.
4. Then after CSP Receive the File and Obfuscate the User Id & file name and Store in the Database.
5. Then Client also calculate Hash of that file and store that (hash + file) on the storage server.
6. CSP Store Data in the Server & Modify Database. then give reply to the Client.

2. For Integrity

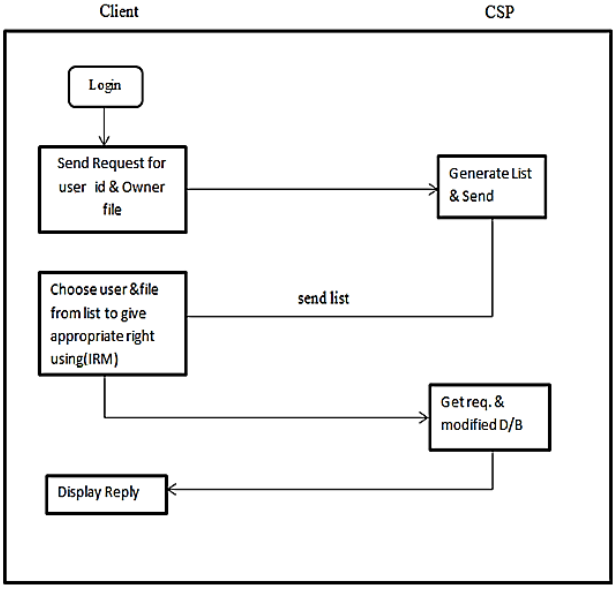
Algorithm #2

1. Client Send Request For Files to CSP.
2. CSP Check the User is Authenticated or not. If No then Display Reply and Go to Step1.If Yes then Go to Step3.
3. If Yes then CSP can De_Obfuscate List of Files and Send to the Client.
4. Client Choose File and Send Verification Req. to Server.
5. CSP Calculate Hash and Send to the Client.
6. Client Compare Hash Code and Verify the file, If Yes then Verification is Done and Process goes to the End. If No then message display.



3. For Right management

File Size	With Obfuscation	Without Obfuscation
512 KB	75	71.14
1 MB	89	83.22
2 MB	221	189.251
10MB	430	401.89
20MB	675	632.47



Algorithm #3

1. Client Send request for User List and Owner File to CSP.
2. CSP Generate User List and Owner File and Send to the Client.
3. Client Choose User and File and apply IRM policy then Send to the CSP.
4. CSP Modify Database and Send Reply to the Client.

III. RESULTS AND DISCUSSION

We run our model on system with following configuration.

1. Intel Core I3 processor with 4GB RAM with 500 GB of storage.
2. System running 64-bit windows-8 Operating System.
3. FRONT END : Cloudsim Simulation.
4. Back-End : MySQL.

A. System analysis

In system analysis phase we analyzed whole system in term of different parameter which used in Proposed method and based on that we prepare graphical representation of that. First we check the encryption, obfuscation and uploading time of file. The table and graph shown below.

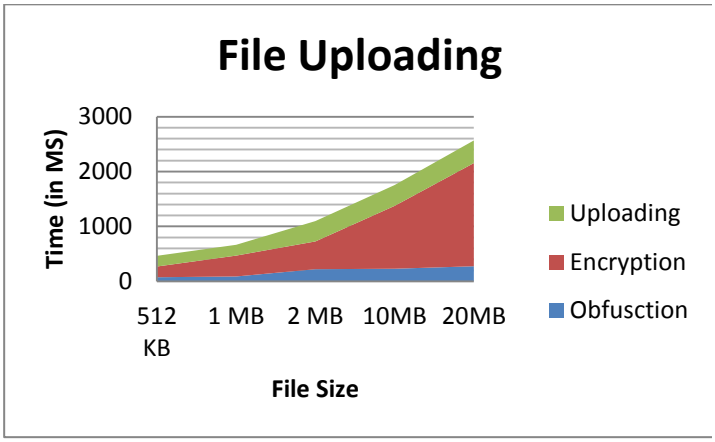


Figure 1. Combination of all Parameter

Result

Table 2. Result to check proposed system and Regular system

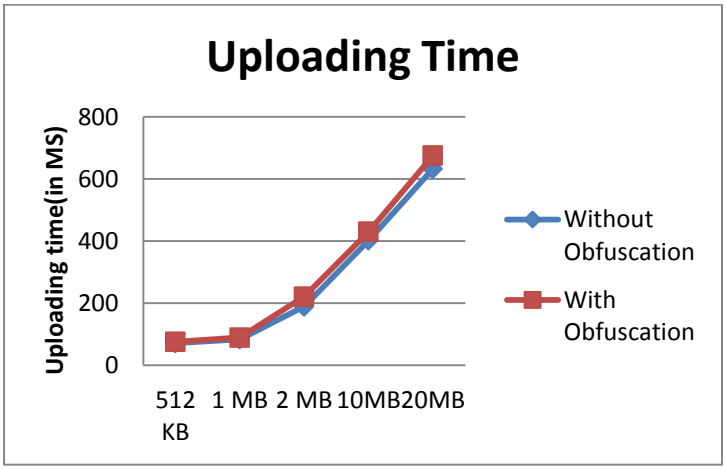


Figure 2. Result to check proposed system and Regular system

B. Data Obfuscation

To simple understanding of the proposed technique, consider a sample table as shown below:

User_Id	File name	Upload date	Hdd_name
Abc@gmail.com	C:\User\enc.txt	8-8-2016	C drive
Ram09@gmail.com	C:\User\ppr1.txt	8-8-2016	C drive
Krishn923@gmail.com	D:\File\ppr2.txt	9-8-2016	D drive

Table 3. Information Table with Plaintext

Based on the proposed technique encryption and obfuscation can be applied on the table 3.

User_Id	File name	Upload date	Hdd_name
anVsaUBnbWFpbC5jb20=	RTpcQWNhZGVtaWMgRlxkYXRhXNoX0Rlc3NlcnRhdGlvblxKdWxpXENvZGluZ1xjbG91ZHV4YW1wbGVcZmlsZXNccnJyLnR4dA==	MDIvNC8xNg==	ZGg=
YWJjQGdtYWlsLmNvbQ=	QzpcVXNlcnNcU09OWS1QQ1xEZXNrdG9wXGNsb3Vkc2ltX0p1bGlcY2xvdWRzaW1fSnVsaVxzcmNc	MDMvNy8xNg==	ZGg=
bWFydXRAZ21haWwuY2	QzpcVXNlcnNcU09OWS1QQ1xEZXNrdG9wXGNsb3Vkc2ltdWRzaW1fSnz	MjgvNi8xNg==	Feh=

Table 4. Information Table with CipherText

User's information like information table Table 3 is submitted to the cloud storage in the form of encrypted and obfuscated shown in table 4. This will increase the data security in the cloud storage.

IV.CONCLUSION

Here we present a model to protecting users' confidential data in cloud computing. The proposed scheme comes up with following benefits. The proposed method introduces a new way of security using data Obfuscation. Hiding information about the owner of data. Increase trust of user on service providers. We use hashing scheme which is used to check integrity of data this helps user to ensure that no modification is done in data. Owner can share the data with only important user. The user can ask for sharing of files to the owner anytime and from anywhere. System provides higher speed with more accuracy. Reduce the overhead of client because obfuscation done at server side. The proposed methodology works better compare to existing scheme in cloud environment.

V. REFERENCES

[1]. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy , "Cloud Computing: Security Issues and Research Challenges". (IJCSITS) Vol. 1, No. 2, December 2011.

[2]. Xiaojun Yu, Qiaoyan Wen, "A View about Cloud Data Security fromData Life Cycle", International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, Dec 2010, pp 1-4.

[3]. Shilpashree Srinivasamurthy and David Q. Liu "Survey on Cloud Computing Security" Department of Computer Science,Indiana University – Purdue University Fort Wayne,Fort Wayne, IN 46805,2010.

[4]. Anca Apostu, Florina Puican, Geanina Ularu, George Suciu, Gyorgy Todoran, "Study On Advantages And Disadvantages Of Cloud Computing" ISBN 2013.

[5]. Christian Collberg,Clark Thomborson,Douglas Low," A Taxonomy of Obfuscating Transformation ," Department of computer science ,The University of Auckland, Private Bag 92019 Auckland,New Zealand. {collberg,cthombor,dlow001}@ cs.auckland.ac.nz"2012

[6]. Muhammad Hataba and Ahmed EI-Mahdy, "Cloud Protection by Obfuscation : Techniques and Metrics,"2012 IEEE Seventh International conference on P2P,Parallel,Grid,Cloud and Internet Computing,

[7]. Dr.L.Arockiam and S.Monikandan ,"Efficient Cloud Storage Confidentiality to Ensure Data Security"2014 International conference on Computer communication and Information(2014 IEEE) ,jan.03-05,2014,coimbatore,India.

[8]. Atiq ur Rehman,M.Hussain SZABIST Islamabad Pakistan,"Efficient Cloud Data Confidentiality for DaaS," International Journal of Advanced Science and Technology Vol.35,october,2011.

[9]. Arvind Narayanan and Vitaly Shamatikov , "Obfuscated Database and Group Privacy", The University of Texas at Austin{arvind,shmat}@cs.utexas.edu,2013.

[10]. Martin M,Agnew G.,Bole.J,Page M,Rhodes W.,"Information Right Management & Digital Right Management "Published on the IEEE Emerging Technology Portal,2006-2012.(http://www.ieee.org/go/emergingtech)

[11]. A Net 2000 Ltd. White Paper ,"Data Masking: What You Need to Know" (http://www.Net.2000Ltd.com & Info@Net2000Ltd.com)
[12]. Priyank Rajvanshi, Varun Singh Nagar, Priyanka Chawla , "Data Protection in Cloud Computing" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-3, August 2013.
[13]. Sergey Vinogradov and Alexande Pastsyak,"Evaluation of Data Anonymization (Obfuscation) Tools" The Fourth International conference on Advances in Database,Knoweldge, and Data Application ,DBKDA 2012.
[14]. Christian S. Collberg and Clark Thombor-son. Watermarking, tamper-proofing, and obfuscation - tools for software protection.In IEEE Transactions on Software Engineering, svolume 28, pages 735–746, August 2002.
[15]. United States Patent" System and Method for Management of secure Data in Cloud Network" Patent No.:US 8,108,912 B2(Jan.31,2012)
[16]. Google app engine. http://code.google.com/appengine/.
[17]. Juli Chaudhari, Jayesh mevada,"A Framework to Secure Cloud Data Server Information Using Data Obfuscation" Technix International Journal for Engineering Research, Volume 2 Issue 08,March-2016.

Book

[1]. Rajkumar Buyaa , Joshy Josef , Craig Fellentein ,Michael Miller" **Advance Computing Technology**" PEARSON.
[2]. Rajkumar Buyya et. el., **Cloud Computing**: Principles and Paradigms, Wiley India Edition
[3]. Martin Lambert OCtober2009 "**Information Rights Management** "– Managing information everywhere it is stored and used **.** Copyright © 2009, Oracle.