Data Security in Cloud

Jijo.S. Nair, BholaNath Roy
Dept. of Computer Science &InfoTech
MANIT-Bhopal

Abstract
Cloud computing is a model for delivering information technology services over the Internet as per the Customers demand. Big conquerors'of IT commercial enterprise is drifting ahead for big business profits to Cloud Computing podium. Even after the backbreaking work by the organization very few customers are exercising cloud although numberless clients are ready to get services on from Cloud. The hurdle most of the customers are facing is with the availability and security of data in Cloud.

Keyword: Cloud, Data storage, Security of Cloud, Steganography, Peer to peer data access

I. Introduction
User of a cloud access cloud services through internet by the help of a web browser they do not need to buy any software to avail the benefits of software. Cloud provider will avail the software and resources required by the user on a minimal rental basis these software and data are stored on servers at a remote location of the service provider which activates only on the demand of user.A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. You don't need software or a server to use them. All a consumer would need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. The consumer gets to use the software alone and enjoy the benefits. The analogy is,*if you need milk, would you buy a cow? All the users or consumers need is to get the benefits of using the software or hardware of the computer like sending emails etc. Just to get this benefit (milk) why should a consumer buy a (cow) software /hardware? [1]*
One of the mentality thebeguile users of cloud are discouraged themselves to opt to cloud is the proclivity in Confidentiality, privacy, availability of data in cloud. Encryption is a method by which we can secure our data from unauthorized access, similarly there are many methods but every methodhas its own advantages and disadvantages in itself. Steganography is a popular method used for data hiding. Steganography (pronounced STEHG-uh-NAH-gruhf-ee, from Greek *steganos*, or "covered," and *graphie*, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data. [2] Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen. [3] By using this method we can increase the confidentiality, privacy of data stored in the Cloud to a limit.
Another risk present in the cloud is availability of data in the cloud which can be managed by adopting peer-to-peer storage systems. It introduces redundancy to data and distributes it among peers in the network which allows availability of data at any point of time as required by the user. Although data redundancy is exploited in cloud, ithas another disadvantage as more space is required to store same data at different peers but our main motive is the availability of data.

2. How data is stored in cloud
Storing a data on the "Cloud" means remote storage of data i.e. every thing is virtualisation in Cloud.Cloud storage is a model of internet based services provided to the user on demand. Client uses the client computer to connect to the database(storage) with the help of a web serviceapplication programming interface (API), or through a Web-based user interface. With the help of this the client can upload/download his data to or from the storage space allotted to the user by the Cloud provider.

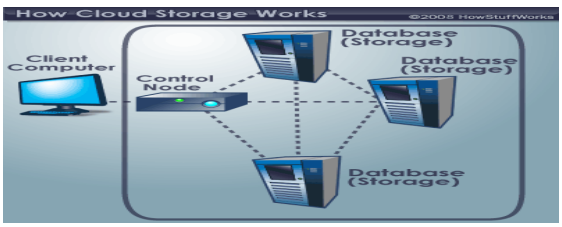

Fig.1 [4]

A typical cloud storage system architecture includes a master control server and several storage servers.
Each time user want to access his data he have to verify his account details with the node controller, if details are found correct it allows user to manipulate his data storage area and services allotted to him. User feels as if he is accessing all the data from his

computer but it is the power of virtualisation which makes him realise so, actually each time data is brought to the client computer from the storage server of the cloud provider. Many cloud service provider at the server end store all data of the user using AES 256 encryption by which a great security for data is complexly implemented at server end. Between the Client computer and the Node control cloud providers use Secure Sockets Layer (SSL) as an encryption technology that protects clients private information while it transit via the Internet.

3. Proposed work

Core study in Cloud summarises us that if data security is raised to an arc the number of users in cloud will increase exponentially asusersare required to spend verylittle money from his pockets. We are planning to increase the Confidentiality, Privacy and availability of data present in Cloud. The data on which we will be working is the text data, we prefer this kind of data, as most of the data stored in Cloud by the user is of this type. Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually unencrypt the data. A solution to this problem is steganography. []We are using combination of Steganography and Storage System (Markov Chain Model) for this purpose.The idea of using Steganography is for the process of hiding messages inside a computerized image file so that if at all unauthorised recipient is able to get data any how then also he will not be able to access the secret data stored within the image. A secret key is generated by the user which will be known to him and for the authorized client. This approach will boost the client side data security to an extent. Then the file generated after processing steganography is uploaded to the Cloud in a peculiar way. Processed data is stored at different storage location i.e redundancy (R) and uses peer to peer data access technology. Fig.2. will give a nut shell idea and clear picture of the proposed work by us.

User makes the text data and an image (grey-scale image) and hides the text behind the grey-scale image using Steganography. The file generated is cut into *data-blocks* that are in turn divided into initial*fragments* (or pieces) of equal size.These piecesare uploaded into the cloud

Fig.2.

4. Conclusion

The proposed approach is more efficient and effective that provides a more secure way of data transmission at higher speed.Distributed and peer-to-peer storage systems are foreseen as an alternative to the traditional data centres and in-house backup solutions.Our contribution is a guideline to the users of cloud to choose a better way of securing data in the cloud. Steganography transmits secrets through apparently innocuous coversin an effort to conceal the existence of a secret. Digital imagesteganography and its derivatives are growing in use and application.In areas where cryptography and strong encryption are beingoutlawed, citizens are looking at steganography to circumvent suchpolicies and pass messages covertly. As with the other greatinnovations of the digital age: the battle between cryptographers andcryptanalysis, security experts and hackers, record companies andpirates, steganography and Steganalysis will continually develop newtechniques to counter each other.In the near future, the most important use of steganography techniques will probably be lying in the field of digital watermarking.Content providers are eager to protect their copyrighted works againstillegal distribution and digital watermarks provide a way of trackingthe owners of these materials. Steganography might also becomelimited under laws, since governments already claimed that criminalsuse these techniques to communicate.

References

[1] http://www.wikinvest.com/concept/Cloud_Computing
[2] http://searchsecurity.techtarget.com/definition/steganography
[3] http://www.webopedia.com/TERM/S/steganography.html
[4] Fig.1.http://computer.howstuffworks.com/cloud-computing/cloud-storage.htm
[5] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition.MIT Press and McGraw-Hill, 2001. Section 11.5: Perfect hashing.
[6] A New Perfect Hashing based Approach for Secure Stegnograph by Imran SarwarBajwa, RubataRiasat ©2011 IEEE.
[7] Peer-to-Peer Storage Systems:a Practical Guideline to be Lazy by Fr´ed´ericGiroire and Julian Monteiro and St´ephaneP´erennes in the IEEE Globecom 2010 proceedings.
[8] A New Perfect Hashing based Approach for Secure Stegnograph by Imran SarwarBajwa, RubataRiasat ©2011 IEEE.
[9] Steganography- A Data Hiding Technique by Arvind Kumar and Km. Pooja on International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010