International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 1, January 2014)

Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique

Priya jaiswal[1], Randeep kaur[2], Ashok Verma[3]
[1]PG Student, MTECH (CSE), [2]Asst Prof. Computer Science Engineering, [3]Head of Department of Computer Science & Engineering, Gyan Ganga Institute Of Technology & Sciences, Jabalpur, Madhya Pradesh, India

***Abstract*-- In present scenario cloud network is a boon in network technology. It is providing number of services which are very difficult to summarize because each and everything on cloud is completely dependent on virtualization. Microsoft 2012, Window Azure, IBM...etc are few companies which are providing these services in a nominal rate. This is the reason it is widely used by a number of users to utilize its services to the fullest. It is widely used for data storage of private, important file or secrete document. The paper present a secure cloud data storage technology which encrypt the data using hybrid security algorithm with cryptography using symmetric key. The proposed security technique provides a highly secure cloud network.**

***Keywords*-- Cloud storage, secure, substitution, transposition**

I. INTRODUCTION

Cloud computing is large technology in simple word we say it is a large network which provide all type of facility which are required by the user related to operating system facility, Application software, resources, cloud data storage and some hardware like RAM or memory. We all know Window XP, or number of flavor of window are single user, with the help of cloud computing we can found the number of user of any flavor of window operating system Microsoft designed Microsoft 2012 operating system as the best example of cloud computing which are completely hardware dependent. If we are increasing the size of memory or other hardware device then we create unlimited number of user under the single operating system. At this technique we can create one simple private cloud with the help of hypervisor(virtualization)or simple networking concept. Since The ever-increasing amount of valuable digital data both at home and in business needs to be protected, since its irrevocable loss is unacceptable. Cloud storage services promise to be a solution for this problem. Recent years cloud computing popularity has increased dramatically.

It provide the ways to store and automatically back up arbitrary data, as well as data sharing between users and synchronization of multiple devices. Cloud computing services are completely depending on virtualization. Virtualization is a technology say a platforms which run multiple operating system in a single machine ,and it provide the facility that we can run multiple application software in guest operating system. Cloud computing is a recent trending in IT that where computing and data storage is done in data centers rather than personal computer. It refers to applications delivered as services over the internet as well as to the cloud infrastructure. The sharing of resources reduces the cost to individuals' .According to cloud computing services; all users data are stored on the cloud data storage. So cloud. So, all the data must be encrypted before it is transmitted to the cloud storage.

Although cloud computing service providers describe the security and reliability of their services, but actual there are a number of security issue are created in cloud computing services. The service is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. In March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to execute malicious code. Microsoft's Azure cloud computing platform also took place a serious outage accident for about 22 hours. Serious security incidents even lead to collapse of cloud computing vendors. As administrators' misuse leading to loss of 45% user data.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 1, January 2014)

II. Related Work

Pradnyesh Bhisikar, & Prof. Amit Sahu explain the Security in Data Storage and Transmission in Cloud Computing. They have explain In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Security threats faced by cloud data storage can come from two different sources[7]. Survey on Various Techniques for Data Storage Security in Cloud Computing Jahnvi S. Kapadia[8].They explain the need of cloud security and also explain the various type of frame work which are used to provide the security algorithm in cloud data storage. Data Security and Privacy Protection Issues in Cloud Computing. 2012 .they explain the various of security threat which are lost various data server [2].And there are also present two white paper which are based on the survey of data privacy and security on cloud data storage [3] and [5].So [1] Dr. L. Arockiam1, S. Monikandan2 describe the method of data privacy and security in cloud data storage using hybrid Security algorithm.

This paper describes data security and privacy protection issues in cloud. This paper is organized as follows: Section II gives a brief description of what exactly cloud computing data storages. Section III discusses data security and privacy protection issues associated with cloud computing. Section IV shows current solutions for data security in cloud. Section V summarizes and conclusion of the contents of this paper. Section V describes result and conclusion of the contents. Section VI describe the future work will perform on this paper.

III. Brief Description Cloud Computing Data Storage Issue

According to Cloud computing data storage is places which are virtualized located in a large network. There are a large capacity in cloud data storage &there a number of user which are store our personal data in cloud storage .there are a need of large security algorithms for no one can access those data from the cloud data storage because of any reason if any unauthorized user access those data he can misuse that data, which are create a large security threat. There are Three different network entities can be identified as follows:

• *User:* users, who have data to be stored in the cloud and there are a client or company which can store the data in cloud for safety in data storage.

• *Cloud Service Provider (CSP):* a CSP, who has managing distributed cloud data storage servers,

• *Third Party Auditor (TPA):* an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert and append. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable

IV. Discusses Data Security And Privacy Protection Issues Associated With Cloud Computing

Generally we study from the basic form of data which are stored in the user or client system in form of message is called the plaintext. Here we use cryptography schemes which are converting our plaintext to cipher text. Cipher text is (no readable form) conversion of plaintext. These are general basic scheme for providing the security of text data. Here we discuss some data security and privacy protection issue which makes our data is more secure in network:-

Personal identity-The personal identification is a user is user id and passwords which are provided to user at a time when data (some personal) information is stored I the cloud. Meaning of that personal information that it is a unique and no one can open that personal data without permitted to authentic user.

Security:-There are a number of Security concerns relate to risk areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security. Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry on the vulnerability of remote data to hackers.

Performance and Availability:-There is one other issue of cloud data storage that after storing our data in cloud data storage we have very comfortable for access our data in any place or in any location without carrying data to everywhere.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 1, January 2014)

Trust: - Trust is defined as the term of privacy in security in cloud data storage that if any user require that he can store our personal file or important or secrete data in a place where no one can see that document, and no one can perform write operation on the data.

Data Backup:-Data backup required in any reason or in cause if your personal data or important file are corrupted or simple word we say data is lost due to system formatted. In this situation we need a backup file which store a secondary copy of our data or file.

Performance and Availability:-There is one other issue of cloud data storage that after storing our data in cloud data storage we have very comfortable for access our data in any place or in any location without carrying data to everywhere.

Privacy:-In cloud computing data storage system all users know that Different from the traditional computing model, utilizes the virtual computing technology. Its mean User's personal data may be distributed in various virtual data center rather than stay in the same physical location. At this time, data privacy protection will face the controversy of different legal systems.

V. Security Algorithm For Data Security In Cloud

In general we study cryptography is a technique applied for encryption and decryption. Cryptography technique are classified in two categories Conventional and public key Cryptography. In conventional cryptography is a technique generally referred to as a symmetric encryption.thats means one single key is used for encryption and decryption. And public key cryptography is a technique simply referred to as a asymmetric encryption technique, there are two different key are used for encryption and decryption, if one key is used for encryption then another key is used for decryption.

This paper presents a symmetric encryption technique. Because of this technique is very suitable to encrypt a large amount of data, which are stored in cloud data storage.

Symmetric Encryption:-In this paper involves the technique use of a single secret key for both the encryption and decryption of data. Symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data. For example, a source produces a message in plaintext, X = [X1, X2, X3….XM].. With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2,….YN]. This may be written as Y = EK(X). Cipher text Y is produced by using encryption algorithm, where E indicates the encryption algorithm used and K indicates the key used for encryption. The receiver of this message should apply decryption algorithm with same key used for encryption to get the actual message X = DK[Y]. Here D indicates decryption algorithm.

Classical Encryption: - There are various encryption algorithms are available that are used in information security. These algorithms can be classified as classical encryptions technique. These encryption algorithms are based on two general principal substitution cipher, and Transposition cipher. And with the help of key we can change the actual format of data or actual value of that data.

Proposed Algorithm:-This algorithm describes the classical encryption technique which is mixture of substitution and transposition. This paper present a technique which are increase the complexity of data, which are stored in cloud data storage.there are one other issue which are create that this algorithm also increase the space complexity of this data . Proposed algorithm is described below. A Encryption Algorithm Followings are the steps in proposed encryption algorithm.

Step1: Fetch any single file from the database.

Step2:-count the number of character in single line.

Step3:-convert the number of according to its ASCII value.

Step4:-create a square matrix according to the counting character.

Like if count character=12

Then size of matrix is =4x4

Step5:-put the number of character in a square matrix. Remainder block are filled by the left alphabet.

Step6:-Divide the square matrix in three part 1.upper traingle2.diagonal 3.lower triangle

Step7:-add some key value in three divisions. Each matrix use three different key K=K1, K2, K3for encryption. Do the encryption.

Step8:-Apply the encrypted value into the matrix in the same order of upper, diagonal and lower.

Step9:-Swap the element from upper triangular to lower triangular. .

step10:-Read the message by column by column. Here the order in the columns read from the matrix is the key K4.

step11:-Convert the ASCII code into character value.

The same but reverse method is applied for the decryption. We apply the same procedure but apply the step from 10 to 1 to decrypt the cipher text.

In both the procedure encryption and decryption, key is more important. Algorithm could be known to everyone but key should be known only to user.

VI. Conclusion

Data Security and Privacy of cloud data stored in Cloud Computing has full of challenges and of. Many research problems are yet to be come which are increase the security problem the cloud data storage's this paper present hybrid security algorithms using the symmetric key. The only difficult task is here that the key is secure. That are only accessible by the authorize user. And the purpose of using that key the is save the more time to store the large amount of data in cloud date storage. And the purpose of these algorithm is generally in cloud data storage(server storage system) not in travelling the data between the user by secure channel.

VII. Future Work

The future work of this paper is that there are one drawback of this algorithm, this increase the space complexity because of in every line he count the number of character and convert them in a square matrix form, which are very space consuming.

So here we apply compression algorithm which are removed the number of space between the words. There are we apply some other technique which are help us to create the data more complex.

REFERENCES

[1] Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm Dr. L. Arockiam1, S. Monikandan2 International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[2] Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and electronics engineering.

[3] Data storage protection risk and return. Document: WPSDPRR-Oct02

[4] Dr. A.Padmapriya ,P.Subhasri," Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4, pp 1067-1071, 2013.

[5] the White paper publish on Cloud Storage – The Issues and Benefits ts.

[6] International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 842 ISSN 2229-5518 IJSER © 2013 Survey on Various Techniques for Data Storage Security in Cloud Computing Jahnvi S. Kapadia.

[7] Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in computer Science and Software Engineering Security in Data Storage and Transmission in Cloud Computing Pradnyesh Bhisikar #1, Prof. Amit Sahu *2