Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique

Kajal Rani[1], Raj Kumar Sagar[2]
Dept. of CSE
Amity University
Noida Uttar Pradesh
Er.kajalchauhan6apr@gmail.com[1], rksagar@amity.edu[2]

***Abstract*-Now days cloud computing become one of the main topic of IT and main point is cloud data storage security. Cloud computing is the fastest growing technology. This technology provides access to many different applications. Cloud computing is used as data storage so data security and privacy issues such as confidentiality, availability and integrity are important factor associated with it. Cloud storage provides user to access remotely store their data so it becomes necessary to protect data from unauthorized access, hackers or any type of modification and malicious behavior. Security is an important concern. The meaning of data storage security is to secure data on storage media. Cloud storage does not require any hardware and software management.it provide high quality applications. As we proposed the concept of cloud data storage security strategy capable to overcome the shortcomings of traditional data protection algorithms and improving security using steganography, encryption decryption techniques, compression and splitting technique adoptable to better security for the cloud. We have developed a desktop application through which user can share data. This paper enhanced advance security goal for cloud data storage**.

Keywords-cloud computing, encryption, decryption, steganography, compression, sharing, AES

I. INTRODUCTION

Cloud computing is the prominent topic in present time. Cloud computing provides multiple services to the users over internet. Cloud storage data is maintained by storage service provider. Cloud can be considered as a large pool of virtualized and easily accessible resources. Companies like Amazon, Google run storage clouds on the public internet. Cloud storage may vary in terms of space, size and functionality. Users can remotely store their data, and can share resources with each other. Cloud computing allow storing and sharing large amount data in cloud. Cloud storage provides high speed data transfer services over internet. Cloud computing provide storage for all types of data. Cloud data Storage allows users to collect data or share data from anywhere via internet. Cloud computing data storage became more popular technique. As we can move our data on the cloud that means we uses the services delivered by the CSP(cloud service provider).so it is necessary to restrict unauthorized access, hackers , any kind of modification and denial of services. Cloud computing permits multiple users to access single server to perform several operations on their data without purchasing any license for multiple applications. Cloud computing provides high speed services at very low cost. Cloud computing creates new issues and challenging security threats. For security purpose there are different multiple existing method and techniques that are used in cloud computing environment. Cloud data storage refers as distributed system. In cloud data storage user regularly updates stored data, files. He may perform several operations including insertion, deletion, modification, reordering on stored data. Cloud data storage has several features like scalability, low cost services, reliability, maintenance, location independence. Cloud computing provide three type of services

(i) Product as a service
(ii) Platform as a service
(iii) Infrastructure as a service

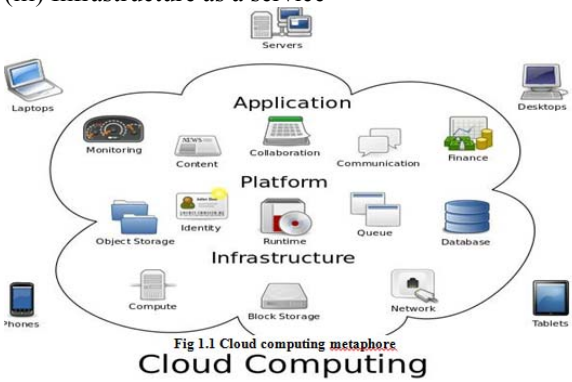

Fig 1.1 Cloud computing metaphore

Fig 1 represents cloud computing metaphore.

The rest of the paper is organized as follows: Section II presents literature study. Section III will describe about cloud storage security issues and challenges. Section IV shows the proposed methodology and implementation work. Section V discusses the result of implementation. Finally Section VI describes conclusion.

II. LITERATURE REVIEW

Gary Anthes [1] has discussed many security research works in cloud are described. Mohamed E.M et.al [2] proposed cloud storage data security model based on the cloud system

architecture and implement software that improve performance of cloud storage data security model. Reema gupta [3] proposed security model which is based on hybrid encryption system to fulfill security needs. Blowfish algorithm and modified version of RSA has been used for file encryption and decryption. According to Chintada et al [4] Cloud computing security issues can be divided into two types first is security concerns that are accepted by customers and second is security issues that are accepted by cloud service providers. Nisha D. Dable [5] implements multiple cloud storage along with enhanced security using encryption decryption techniques, splits the file into different parts and store it on different cloud. R. Velumadhava Raoa,[6]discussed about the data security challenges and their solutions to overcome related to cloud computing environment. Namita N. Pathak [7] proposed multi cloud model on data storage, splitting files into chunks and AES algorithm is used for encryption and MD5 is used for data verification of two cloud servers' data. S. Subbiah S. Selva Muthukumaran and T. Ramkumar [8] proposed a cloud data storage security strategy with the help of vertical partitioning algorithm. This algorithm protects data in very efficient manner. Zebin et al.,[9] implements PCA algorithm on SPARK and discusses risk of exploiting cloud architecture for distributed and parallel dimensionality reduction and he used data repositories for storing remotely sensed datasets. Bermer [10] combines cloud and peer to peer computing it contains backup, online gaming, content distribution and streaming.

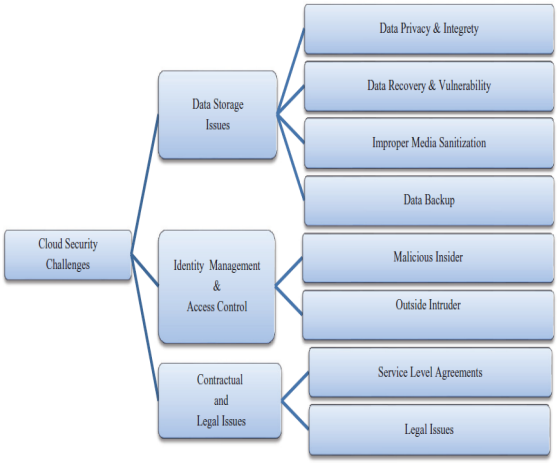

Fig.2 cloud computing security challenges [11]

III. CLOUD DATA STORAGE SECCURITY ISSUES AND CHALLENGES

In cloud based environment there are many security issues such as authentication, integrity, privacy, virtualization, confidentiality, large amount data processing, scalability, access control etc. Traditional security approaches are no longer suitable for data and application in cloud. Cloud computing have scalable and location independence features so application and data stored in cloud have no fixed limitations. In security breaches it is quite difficult to resolve a particular node in which threats occurred. Due to the openness of cloud environment data may be accessed by unauthorized users. In cloud the issue of verifying correctness of cloud data storage becomes more challenging. Cloud computing poses several security threats due to number of reasons.

Data Breaches is also major security concern in cloud storage. User stored large data sets in the cloud so there is a chance that malicious user may entered in the cloud storage system. There is high possibility of attack and threats. In cloud storage data integrity must be kept effectively to avoid data loss. In cloud storage data is stored over the remote server so it is necessary to preserve confidentiality. Security policies should be followed strictly. Data access provides user access to data storage. Data should be shared only between authorized users so it is required to provide privileged user access. Reliability is also an important issue in cloud storage because data is stored in virtual machines. Multi-tenancy is an important characteristic of cloud computing technique. Multitenancy permits multiple users to access and store data on cloud servers.so there is a risk of data intrusion. By injecting client code data can be intruded.

IV. PROPOSED OBJECTIVES AND IMPLEMETATION

We have proposed a system with following objectives.

- To understand the security issues related with cloud storage.
- To provide high quality services to the users.
- To provide high data security in cloud based environment using steganography, encryption and decryption.
- To minimizing the data uploading and downloading time on cloud storage.

A. Implementation

Development phase

Step1: Registration Module

In registration module user will register themselves by user name, password, contact number and email id. User generate random verification code by using Random.Next().user get the verification code on his email address after that user verify the code and redirect to home page. If verification code field remain blank or user entered wrong verification code then redirect to login page.

Step 2: Login Module

Login is the procedure by which individual get access to the data by identifying and authenticating through the credentials provided by the user. User has logout when access is no longer required.

Step 3: Steganography

In proposed system steganography is used for concealment of data, messages, text, and information within computer. In this step LSB technique is used for steganography. The primary goal of steganography is to hide data within some other data in such a way that hidden data cannot be detected even it is being sought. Only intended user can understand the meaning of the sent messages.

Step 4: File splitting

In Suggested system, we are splitting the data file, image file or video in different parts with some extension (.part in our case).After splitting we stored splatted file in our local system with extension .part.

Step 5: Encryption

In this proposed system, encrypt each and every splitted file which is of .part extension with public key so that it cannot be easily readable by any unauthorized access or hacker. Encryption technique like DES, AES, RSA is developed before storing it on cloud.

Step 6: Compression Module

In this proposed system, splited files get compressed with GZIPSTREAM algorithm so that the size of splited files gets reduced, and it can easily be transferred to cloud server. zip is based on the DEFLATE algorithm.

Step 7: Upload and download module

We have developed a desktop application to upload files in cloud server. In other words splited files get saved to different cloud server. We created a method where user can share files to other users, for that we have designed a page in which user can simply enter the id of person whom to transfer the files and file gets uploaded to cloud server and name of the files get saved to SQL server table. The receiver will get a notification that somebody has shared a file with you. If user clicks on the download button all the splitted files get merged and saved to receiver local system. Now the receiver party gets the encrypted and compressed file it is the time that user has to decrypt and decompressed the received file.

Step 8: FTP Module

In this suggested system file is scattered at three locations. First one is at our application and next two where second and third files are stored. We developed setting page that will be used for uploading and downloading file from table. Insert FTP details into table.

B. Data Flow Diagram

A Data Flow Diagram illustrates the flow of information through information system. The DFD shows what kind of data will be input for the system and what kind of data will be received as output. The Data flow diagram can be explained as the separate levels indicating the individual complexity in the each level of the system and gives a detailed explanation in the further levels that are following them.

1) Level 0

Initially in the first level of the Data flow the level 0 explains the basic outline of the system. The end-user sends the packets to the system to determine the source and destination address. The diagram marked as the 0 represents the complete Packet watching system which simply represents the basic operation that is being performed by it in the initial level.

2) Level 1

The level 1 of the Data flow diagram given explains in detail about the Packet watching system which was marked as 0 in the previous level. In this level the end-user who passes the request for the system enters into the first process, the capturing process and then to the processing module. After processing the packets it was send for storing. The Level 1 shows how information moves from and to each of these processes. Level 1 explains more details of higher level processes.

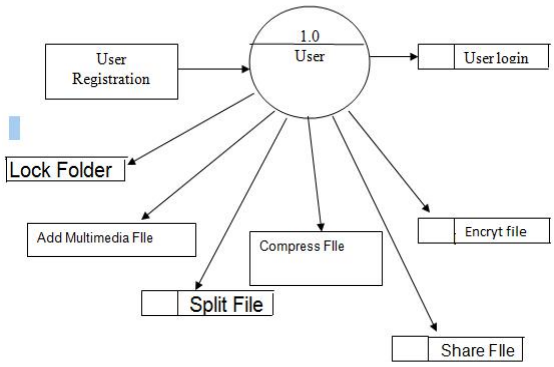

Fig.3 Data Level Diagram for Admin level-1

3) Level 2

The level 2 provides the clear explanation about the whole system. In this level first we have to select the packet and perform test over that selected packets. Then identify the end address of the packet and send that packet for processing. After processing the packet it was send to the identity content. Then send the processed packet for storing and display the source and destination addresses.

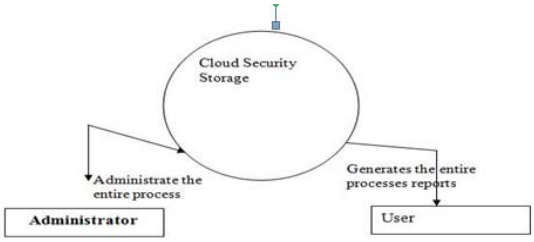

Fig.4 Data Flow Diagram (Context level)

Diagram for cloud storage where administrator looks up for the entire process and the user generates the process reports.

C. AES

AES (Advanced Encryption Standard) is a symmetric encryption algorithm.This algorithm is developed by two scientists Joan Daemen and Vincent Rijmen in 2001.Firstly AES algorithm is approved by U.S. government for securing sensitive information. Now AES is used worldwide. AES is fast symmetric algorithm. AES used same key for encryption and decryption process so this algorithm is known as Symmetric key algorithm. AES support 128 bits, 192 bits, 256 bits block cipher. AES is designed to replaces DES. AES is faster in implementation of both hardware and software. AES mainly repeats four functions to encrypt data.

Algorithm

1. Key Expansions—Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round
    1. Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
    1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. Add Round Key
4. Final Round (no Mix Columns)
    1. Sub Bytes-In this step each byte in the state matrix is replaced by a sub byte using an 8 bit substitution box the Rijndael S-box.
    2. Shift Rows-The shift rows step operates on the rows of the state it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively
    3. Add Round Key-In the Add Round Key step, the sub key is combined with the state. For each round, a sub key is derived from the main key using Rijndael's key schedule each sub key is the same size as the state. The sub key is added by combining each byte of the state with the corresponding byte of the sub key using bitwise XOR.

D. GZIPSTREAM Algorithm

GZIP is a compression tool which is used for file compression and decompression. Gzip is a software program developed by Jean Loup Gailly and Mark Adler. It is an open source software program that is available publically. It is similar to DEFLATE algorithm, which is a combination of Huffman coding algorithm & LZ77 algorithm. DEFLATE is used as a replacement for LZW data compression algorithm.

- Gzip can be used for all type of text files such as .html, .php, .css, .aspx.
- Gzip algorithm helps to save bandwidth so it increases the loading speed of the pages.
- For Compression and Unzipping this algorithm takes only fraction of a second

V. EXPERIMENT RESULTS

In this proposed work we have developed desktop application. For implemented we developed a web page to register the user and login on the cloud. We created a method where user can share files to other users. We have designed a page in which user can simply enter the id of person whom to transfer the files and file gets uploaded to cloud server and name of the files get saved to SQL server table. The receiver will get a notification that somebody has shared a file with you. AES algorithm is used for Encryption. GZIPSTREAM is used for compression. Steganography is used for hiding data files. We also implement Split algorithm for security Enhancement. By implementing spilt algorithm we can split long file and after that we process encryption and decryption.

VI. CONCLUSION

Due to the openness of cloud storage privacy and security problems are major concern that need to be solved we must use new method for cloud storage security enhancement. By implementing Cloud storage many business related security issues and problems and threats will be resolved. By implementation of this proposed work we can increased cloud storage security using encryption, decryption, compression, sharing technique. In this paper we discussed about cloud storage security issues and challenges. In future we will try to deploy this in other cloud based environment and the best can be chosen. In Future we can add training module to our system this module will be helpful for the users of the system about the system usage. In future standard can be developed for cloud storage security. We will try to find out problems related to existing security algorithms and implement better version of existing security algorithms.

REFERENCES

[1] G. Anthes, “Security in the cloud”, in communication of the ACM, vol. 53, no.11, pp. 16-18, 2010.

[2] E. M. Mohamed, H. S. Abdelkader and S. El-Etriby “Enhanced Data Security Model for Cloud Computing”, the 8th International Conference on Inforrmatics and Systems (INFOS2012 Cloud and Mobile Computing Track, pp. cc-12, 2012.

[3] R. Gupta, Tanisha, Priyanka “Enhanced Security for Cloud Storage using Hybrid Encryption” International Journal of Advanced Research in Computer and Communication Engineering vol. 2, no.7, July 2013.

[4] Chintada. S. Rao , C. C. Sekhar ”Dynamic Massive Data Storage Security Challenges in Cloud Computing Environments ”International journal of innovative research in computer and communication Engineering vol.2, no.3,March 2014.

[5] N. D. Dable, N. Mishra, “Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment” International Journal on Advanced Computer Theory and Engineering (IJACTE) ISSN: 2319-2526, vol.3, no.4, 2014.

[6] R. V. Raoa, K. Selvamanib “Data security challenges and its Solutions in cloud computing” International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014), vol. 48, pp.204-209, Jan 2015.

[7] N. N. Pathak , M. Nagori “Enhanced security for multi cloud storage using AES algorithm”, International Journal of Computer Science and Information Technologies, vol. 6 , pp. 5313-5315, 2015.

[8] S. S. Muthukumaran and T. Ramkumar “An Approach for Enhancing Secure Cloud Storage Using Vertical Partitioning Algorithm”, Middle-East Journal of Scientific Research, vol.23,no. 2, pp. 223-230, 2015.

[9] Z. Wu, Y Li, A. Plaza, J. Li, F. Xiao, and Z. Wei, “Parallel and Distributed Dimensionality Reduction of Hyper spectral Data on Cloud Computing Architectures”, IEEE, vol.9, no.6, pp. 2270-2278, 2016.

[10] Bremer and K. Graffi, “Symbiotic Coupling of P2P and Cloud Systems: The Wikipedia Case”, In the Proceedings of IEEE International conference on communication, pp. 3444-3449, 2013.

[11] N. Vurukonda1, B. T. Rao "A Study on Data Storage Security Issues in Cloud computing" in 2nd International Conference on Intelligent Computing, Communication & Convergence in ELESVIER (ICCC-2016), vol.92, pp.128-135, 2016.

[12] ″Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001.