IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 11-15

Enhanced Data Storage Security In Cloud Environment Using Encryption, Compression And Splitting Technique.

Mr. Mohit Patil[1], Mr. Pratik Chavan[2], Mr. Pratish Chavan[3],
Ms. Nileema Pathak[4]
[1, 2, 3] *(Student, Department of Information Technology, Atharva College of Engineering, Mumbai, India)*
[4] *(Asst. Professor, Department of Information Technology, Atharva College of Engineering, Mumbai, India)*

Abstract: *Now days cloud computing has become one of the main topics 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 provides 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*

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

II. Statement Of Problem

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.

III. Objectives:

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.

IV. Preliminary Literature Review

A previous literature review shows that past studies are primarily focused on understanding and modeling system of cloud security. 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

V. Methodology

Development phase

Step1: Registration Module

In registration module user will register themselves by user name, password, and email id.

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: File Upload and Processing

After login user can select and upload file in the cloud and and store in userspace

Step 4: 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.

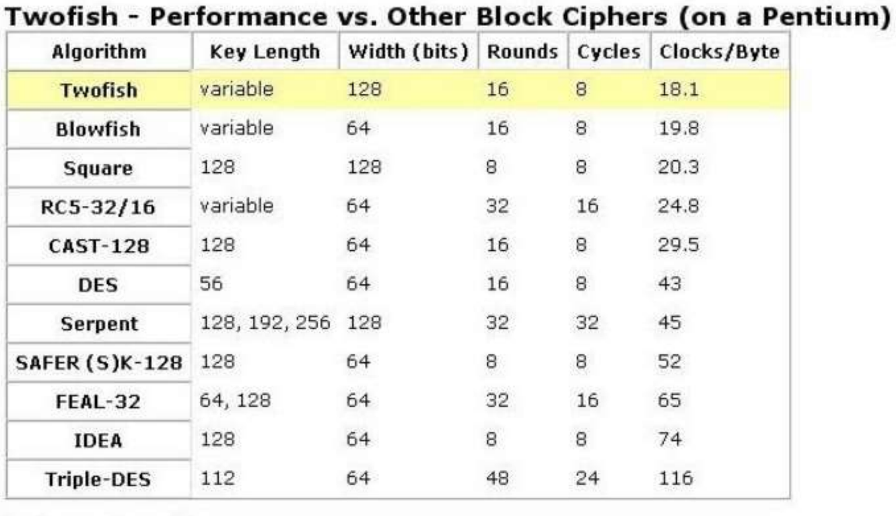
Step 5: File splitting

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 splitted file in our local system with extension .part.

Step 6: 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, and RSA is developed before storing it on cloud

Two Fish Performanceanalyses

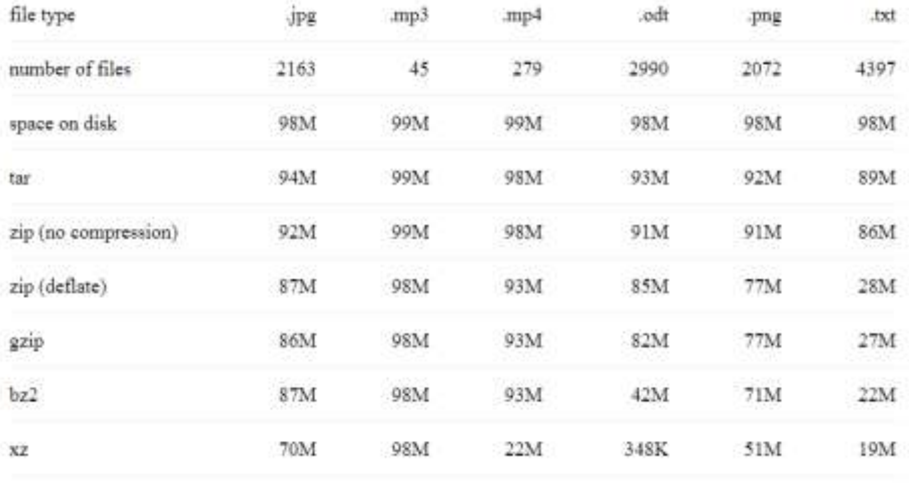


Twofish - Performance vs. Other Block Ciphers (on a Pentium)

Algorithm	Key Length	Width (bits)	Rounds	Cycles	Clocks/Byte
Twofish	variable	128	16	8	18.1
Blowfish	variable	64	16	8	19.8
Square	128	128	8	8	20.3
RC5-32/16	variable	64	32	16	24.8
CAST-128	128	64	16	8	29.5
DES	56	64	16	8	43
Serpent	128, 192, 256	128	32	32	45
SAFER (S)K-128	128	64	8	8	52
FEAL-32	64, 128	64	32	16	65
IDEA	128	64	8	8	74
Triple-DES	112	64	48	24	116

Step 7: 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.



file type	.jpg	.mp3	.mp4	.odt	.png	.txt
number of files	2163	45	279	2990	2072	4397
space on disk	98M	99M	99M	98M	98M	98M
tar	94M	99M	98M	93M	92M	89M
zip (no compression)	92M	99M	98M	91M	91M	86M
zip (deflate)	87M	98M	93M	85M	77M	28M
gzip	86M	98M	93M	82M	77M	27M
bz2	87M	98M	93M	42M	71M	22M
xz	70M	98M	22M	348K	51M	19M

Step 8: Upload and download module

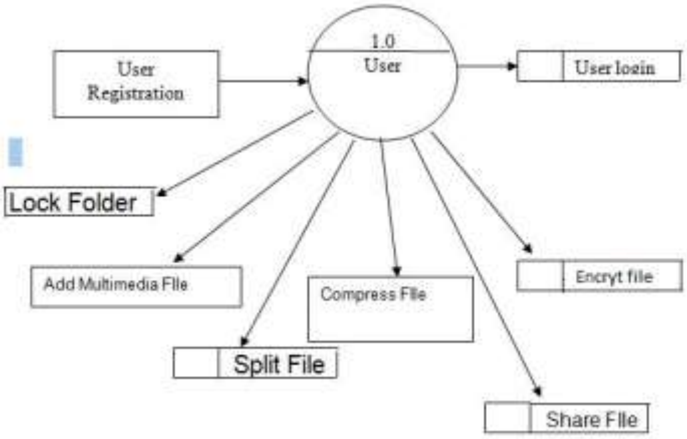
We have developed a desktop application to upload files in cloud server. In other words, splited files get saved to different cloud server. We created a method where user can share files to other users, for that we have designed a page in which user can simply enter the id of person whom to transfer 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.

4. Data Flow

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 each level of the system and gives a detailed explanation in the further levels that are following them.

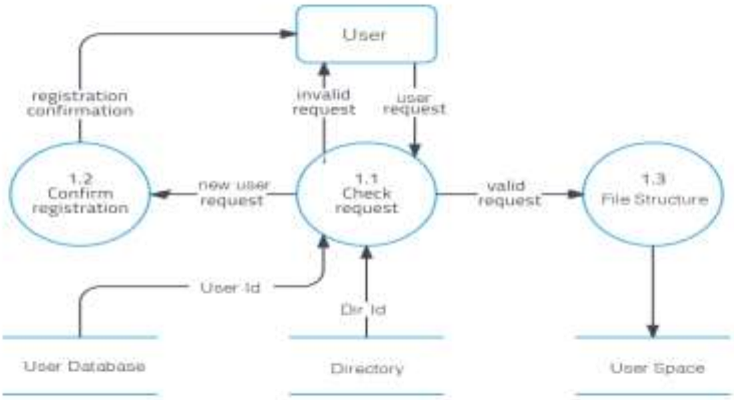
1) Level 0

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 sending 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.



B.Two-fish Algorithm

Two-fish is a symmetric block cipher; a single key is used for encryption and decryption. Two-fish has a block size of 128 bits, and accepts a key of any length up to 256 bits. (NIST required the algorithm to accept 128-, 192-, and 256-bit keys.) Two-fish is fast on both 32-bit and 8-bit CPUs (smart cards, embedded chips, and the like), and in hardware. And it's flexible; it can be used in network applications where keys are changed frequently and in applications where there is little or no RAM and ROM available.

Two-fish is a Feistel network. This means that in each round, half of the text block is sent through an F function, and then XORed with the other half of the text block. DES is a Feistel network. Blowfish (another Schneier algorithm) is a Feistel network. Five of the AES submissions are Feistel networks. Feistel networks have long been studied in cryptography, and we know how they work.The basic process of Two fish is given as follows:

I) the plaintext is broken up into four 32-bit words and each

IsXORd with a 32-bit expanded key (The first word is XORd
WithKK0, the second word with KK1 and so on).

ii) The first word is broken up into 4 bytes, each of which is
Applied to a substitution box (or S-box, like the lookup table
Mentioned in AES). The second word is first rotated left by 8
Bits and then is also applied to the same set of S-boxes.

iii) From here both the first and second words are applied to
An MDS matrix (Maximum Distance Separable) which serves to diffuse the newly substituted data of the 32-bit word
Amongst its 4bytes.

iv) After the MDS matrix multiplication the first word is
applied to a pseudo-Hadamard Transform:
aa′ = aa+ bbmmmmmm232
where a is the first word, b is the second word and a’ is the
new first word. Using the ‘new’ first word as input, the second word is applied to the same transform, which can equivalentlyberepresented as: bb′ = aa+ 2bbmmmmmm232

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.

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 algorithm

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. Abd-el-Kader 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. Dabble, 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]. BruceSchneier “Twofish: A 128-Bit Block Cipher” https://www.schneier.com/academic/paperfiles/paper-twofish-paper.pdf

[7]. Twofish-Encryption-Algorithm-by-Horatiu-Paul-Stancu” https://users.cs.jmu.edu/abzugcx/Public/Student-Produced-Term-Projects/Cryptology-2002-SPRING/Twofish-Encryption-Algorithm-by-Horatiu-Paul-Stancu.ppt