Data Security using Multi Cloud Architecture

Prof. J. M. Patil
Assistant Professor Department of Computer Engineering
Shri Sant Gajanan Maharaj College of Engineering
Shegaon, India
jaypatil@yahoo.com

Ms. B. S. Sonune
ME II year Department of Computer Engineering
Shri Sant Gajanan Maharaj College of Engineering
Shegaon, India
bhagya.sonune@gmail.com

Abstract:- Cloud computing is a fastest growing technology. It allows business organizations to use or access different applications, store information without access their personal files. File access assure in real technique to the file protection due to untrusted cloud servers. Attacks from adversary user are difficult to stop in cloud storage. This paper helps for implementing the concept of multiple cloud storage along with enhanced security using encryption techniques where rather storing complete file on single cloud system. The system will encrypt the file and then splits the file in different chunks and store on different cloud.

Keywords- *encryption, security, spilting, multicloud.*

*****

I. INTRODUCTION

The boom in cloud computing over the past few years has led to a situation that is common to many innovations and new technologies: many have heard of it, but far fewer actually understand what it is and, more importantly, how it can benefit them. This whitepaper will attempt to clarify these issues by offering a comprehensive definition of cloud computing, and the business benefits it can bring. Security challenges are still amongst the biggest barrier when considering the adoption of cloud services. This focuses a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues the cloud paradigm comes with a new set of special features which open the path towards whole and sole security approaches, techniques and architectures [5]. It gives a survey on the achievable security merits by making use of multiple different clouds simultaneously. Various diverse architectures are introduced and discussed according to their security and privacy capabilities and prospects.

A. What is Cloud Computing?

Cloud computing is the practice of using remote servers on the internet to manage, store and process data instead of using a personal computer. Cloud computing is a general term that is better divided into three categories: Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service. IaaS (or utility computing) follows a traditional utilities model, providing servers and storage on demand with the consumer paying accordingly. PaaS allows for the construction of applications within a provider’s framework, like Google’s App Engine. SaaS enables customers to use an application on demand via a browser. A common example of cloud computing is Gmail, where you can access your stored data from any computer with internet access.

Cloud computing can allow a user to access applications and data from any computer at any time since they are stored on a remote server. It also reduces the need for companies to purchase top-of-the-line servers and hardware or hire people to run them since it is all maintained by a third party. Software licenses do not have to be purchased for every user as the cloud stores and runs the software remotely. Data can also be stored with cloud computing so companies do not have to house servers and databases themselves. By centralizing memory, bandwidth, storage & processing in an off-site environment for a fee, cloud computing can significantly reduce costs.

B. Types of Cloud Computing

- Public Cloud

Public cloud (also referred to as ‘external’ cloud) describes the conventional meaning of cloud computing: scalable, dynamically provisioned, often virtualized resources available over the Internet from an off-site third-party provider, which divides up resources and bills its customers on a ‘utility’ basis.

- Private Cloud

Private cloud (also referred to as ‘corporate’ or ‘internal’ cloud) is a term used to denote a proprietary computing architecture providing hosted services on private networks. This type of cloud computing is generally used by large companies, and allows their corporate network and data center administrators to effectively become in-house ‘service providers’ catering to ‘customers’ within the corporation. However, it negates many of the benefits of cloud computing, as organisations still need to purchase, set up and manage their own clouds.

- Hybrid Cloud

It has been suggested that a hybrid cloud environment combining resources from both internal and external providers will become the most popular choice for enterprises. For example, a company could choose to use a public cloud service for general computing, but store its business-critical data within its own data center. This may be because larger organisations are likely to have already invested heavily in the infrastructure required to provide resources in-house – or they may be concerned about the security of public clouds.

It will concentrate on public clouds, because these services demand for the highest security requirements. It also includes high potential for security prospects. It can provide a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various different architectures are introduced and discussed according to their security and privacy abilities and prospects.

II. LITERATURE REVIEW

Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The third party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software[1]. It will concentrate on public clouds, because these services demand for the highest security requirements. It also includes high potential for security prospects. [4] It can provide a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects.

Kan Yang and Xiaohua Jia propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi-authority CP-ABE scheme with efficient decryption, and also design an efficient attribute revocation method that can achieve both forward as well as backward security [2].

Cloud computing offer a new and exciting way of computing with various service models that facilitates different services to the users. As all the data of an enterprise processed remotely and exchanges via different networks. Security is an essential parameter and the service provider must ensure that there is no unauthorized access to the sensitive data of an enterprise during the data transmission [6]. Prashant Kumar and Lokesh Kumar are analyzes various security threats to cloud computing. To offering good service, cloud computing service providers must avoid these threats.

III. WORKING METHOD

1.File encryption technique design: Setting up and configuring different cloud server in order to having storage cloud access.

2. Remote file split and storing module: Using Cloud Server API develop file accessing method in different cloud.

3.Remote file clubbing module: Developing encryption technique like RSA, AES for file decryption before storing it on cloud.

4.File Management & Web Access Module: Develop a file management classes in dot net.Develop a Web interface to upload and download files in cloud storage.

In proposed system the concept of multiple cloud storage along with enhanced security using encryption techniques is implemenred. The file is split in various parts then encrypt and store it on different cloud. Meta data required to decrypt and rearrange a file will be stored in metadata management server [12].

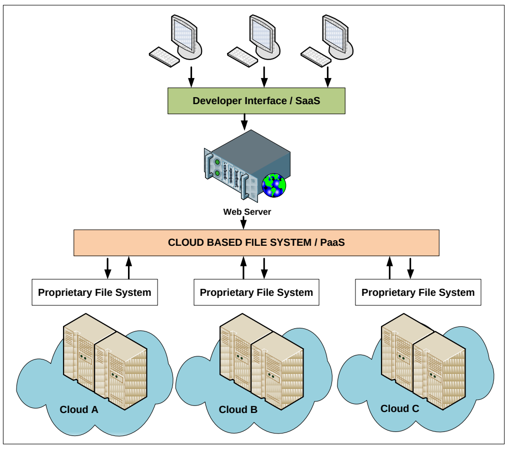

Fig. 1. System architecture

- Setting up and configuring different cloud server in order to having storage cloud access.Using cloud server API develop file accessing method in different cloud.
- Developing encryption techniques like AES, RSA for file decryption before storing it on cloud.
- Develop a file management classes in dot net.Develop a web interface to upload and download files in cloud storage.

A. Development Phases:

Step 1: Registration Module

In registration get username, email address, password, user generate random verification code. The user can sign in and proceed to next step to verification code. The user can verify the code if verification code is blank then redirect to login page else matched then update user status field with text active and redirect user to the home page.

Step 2: FTP Setting Module

The proposed system, file get distributed at three different location. First location that is our application and next two more FTP where 2nd and 3rd file is store. In proposed system, we design setting page where this will be further used by application to upload and download file from created table. Insert into table FTP details.

Step 3: Upload and Download module

Develop a web interface to upload and download files in cloud storage. The different file uploading links are open. The user can choose the link which we want to upload on cloud. User can upload the file on cloud such as doc file, video, mp3, etc.

Homepage will show list of file uploaded by user from user specific directory. In proposed system, we use data list to show file list .File class to get folder and file details like file name, file size.

- Upload file by using file uploader control we can let the user select file to be upload.
- Get the sever path by using Server.MapPath () function to get path of server directory.

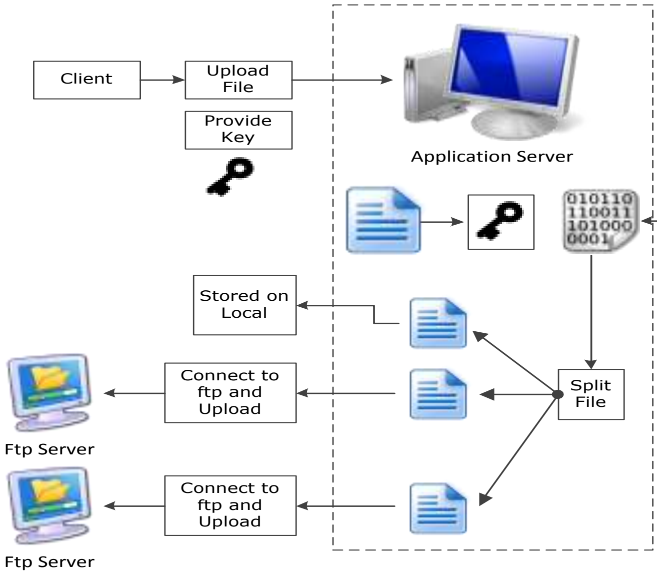

Fig:2.Uploading Process

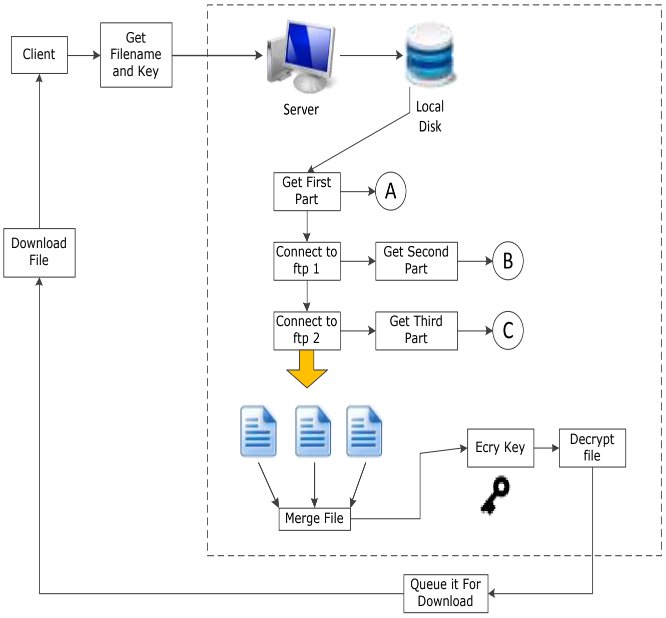

Fig:3.Downloading process

Step 4: File encryption technique module

Setting up and configuring different cloud server in order to having storage cloud access. Each cloud its own server. Developing encryption technique like RSA, AES, DES for file decryption before storing it on cloud. In proposed system, we use the Triple-DES Algorithm and we need to pass 24 byte encryption key.

Step 5: File splitting and clubbing module

In Proposed system, we are splits the file in different portions then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file.

.

B. Spliting and security scenarios based on multicloud architecture

The basic idea is to use several clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. This architecture modified targets the confidentiality of data and processing logic. It gives an answer to the following question: How can a cloud user avoid fully revealing the data or processing logic to the cloud provider? The data should not only be protected while in the persistent storage, but in particular when it is processed.

The idea of this architecture is that the application logic needs to be partitioned into fine-grained parts and these parts are distributed to distinct cloud. In encryption technique, the user encrypts the data with his public key and uploads the cipher texts to the Cloud. The cloud can independently compute on the encrypted data to obtain an encrypted result, which only the user can decrypt. The user (or a small trusted private cloud) manages the keys and performs the encryption and decryption operations, while the massive computation on encrypted data is done by an untrusted public cloud.

Triple-DES:

3DES is a way to reuse DES implementations, by chaining three instances of DES with different keys. 3DES is believed to still be secure because it requires 2^{112} operations which is not achievable with foreseeable technology. 3DES is very slow especially in software implementations because DES was designed for performance in hardware.

In 3DES, a mode of the DES encryption algorithm that encrypts data 3 time. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).

In cryptography, Triple DES (3DES) is commonly known as Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Initially, when the algorithm was designed the original DES cipher's key size of 56 bits was generally sufficient but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a complete new block cipher algorithm.

- Algorithm:

Triple DES uses a "key bundle" that comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits).

The encryption algorithm is:

$$\text{Cipher text} = E_{K3}\,(D_{K2}\,(E_{K1}\,(\text{plaintext})))$$

i.e., DES encrypt with K_1, DES decrypt with K_2, then DES encrypt with K_3.

Decryption is the reverse:

$$\text{Plaintext} = D_{K1}\,(E_{K2}\,(D_{K3}\,(\text{cipher text})))$$

i.e., decrypt with K_3, encrypt with K_2, and then decrypt with K_1.

Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

- Security:

In general, Triple DES with three independent keys (keying option 1) has a key length of 168 bits (three 56-bit DES keys), but due to the meet-in-the-middle attack, the effective security it provides is only 112 bits. Keying option 2 reduces the effective key size to 112 bits (because the third key is the same as the first) designated by NIST to have only 80 bits of security.

The best attack known on keying option 1 requires around 2^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions, and 2^{88} memory (the paper presents other tradeoffs between time and memory). This is not currently practical and NIST considers keying option 1 to be appropriate through 2030. If the attacker seeks to discover any one of many cryptographic keys, there is a memory-efficient attack which will discover one of 2^{28} keys, given a handful of chosen plaintexts per key and around 2^{84} encryption operations.

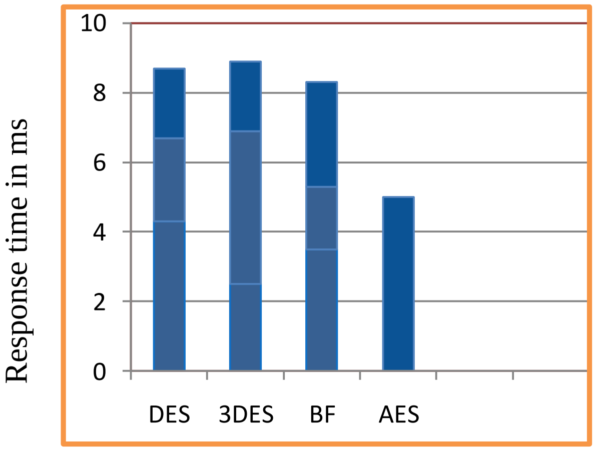

Fig:4.Comparison with different techniques

- Download:

Get the file name selected by user read 1st part of file (means file a) from user specific directory and get A and also FTP detail from user get from user name and FTP password user in textbox connect B FTP download 2nd part from FTP. Download file function, we get part B and repeat above process we will get C or part C. we combine 2nd (B) and 3rd (C) part we will get X, then combine i.e. 1st part with X. Finally we have club file in Byte buffer and save this buffer to memory Stream.

- Decrypt :

Get the public key i.e. encryption key from textbox and decrypt the memory stream. We save this memory stream to sever disk in temporary function and redirect web client i.e. browser to this Temp file and browser start download file.

IV. CONCLUSION

By implementing the cloud based storage it may solve many business secure and safe storage issues. But on the other side many expert state that it is more risky to put the data over single cloud as it increase the malicious user attack possibilities hence by designing the proposed system we are extending the storage cloud security by distributing and encrypting the data.

REFERENCES

[1] J.M. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, “Security and Privacy-Enhancing Multi-cloud Architectures,” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[2] Kan Yang, Ren, XiaohuaJia, Bo Zhang, and RuitaoXie, “DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems,” IEEE 2013

[3] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Tech. Rep., Sept 2011.

[4] Jing-Jang Hwang and Hung-Kai Chuang, ” A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service,” National Science Council of Taiwan Government, IEEE ,2012

[5] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “On Technical Security Issues in Cloud Computing,” in Proceeding of IEEE Int’l Conf. Cloud Computing (CLOUD-II), 2009.

[6] Kan Yang, XiaohuaJia, ” Attributed-based Access Control for Multi-Authority Systems in Cloud Storage,” in Proceeding of 2012 32nd IEEE International Conference on Distributed Computing Systems , IEEE ,2011

[7] M. A. AlZain, B. Soh and E. Pardede,” MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing,” in Proceeding of 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing,IEEE,2011

[8] C. Selvakumar G. JeevaRathanam M. R. Sumalatha ,” PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique,” IEEE,2012

[9] Akash Kumar Mandal, Mrs. ArchanaTiwari , ” Performance Evaluation of Cryptographic Algorithms: DES and AES,” inProceeding of 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science,IEEE 2012

[10] J. D Assistant Professor, Ramkumar P Systems Engineer, Kadhirvelu D,” Preserving Privacy through Data Control in a Cloud Computing Architecture using Discretion Algorithm,” in Proceeding of Third International Conference on Emerging Trends in Engineering and Technology,IEEE,2010

[11] PrashantKumar,Lokesh Kumar,” Security Threats to Cloud Computing”, International Journal of IT, Engineering and Applied Sciences Research (IJIEASR),Volume2,No.1December,2013