Review On design and Implementation of Enhanced Security in Multicloud Storage System Using Distributed File System

Priyanka R. Raut[1], **Vaidehi Baporikar**[2]

[1]M.Tech Scholar Department of Computer Science and Engineering, Nagpur, India

[2]Assistant.Professor Department of Computer Science And Engineering, Nagpur, India

Abstract: In modern centuries plan of Cloud computing in different mode like cloud storage, cloud servers, cloud hosting are increased in industries and other organization as per requirements. While considering the power, the stability and security of cloud one can't ignore different threats to user's data on cloud storage. File retrieve is an actual technique to guarantee the file safety in the cloud. But on the other hand, due to file outsourcing and unauthorized cloud servers. The file entrance design an exciting issue in cloud storage systems. In effect it is right to suggest mechanism systems are no expanded related to cloud storage concepts, because they also design different converted copies of the similar files or involve a completely reliable cloud server. Intentionally harmful user at cloud storage is become most difficult destroy to stop. In proposed system, we are suggest the ideas of various cloud storage beside with enhanced safety using encryption methods otherwise storing complete file on single cloud system. File can divided into different sections at that time encode and store it on different cloud and the meta information necessary for decrypting and affecting *a file will be stored in metadata management server.*

Keywords: Multi-Cloud computing, Architecture of computing, RSA, Data spliting.

1. 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 not actually understand how it can benefit them and more importantly, what it is This whitepaper will attempt to clarify these issues by offering a comprehensive definition of cloud computing, and the business advantages it can bring. Security challenges are still amongst the largest obstacles when considering the adoption of cloud services. This triggered a lot of research action, resulting in a quantity of proposals targeting the various cloud security threats. These security issues the cloud paradigm comes with a new set of unique features which open the path towards novel security approaches, architectures and techniques. This paper provides a survey on the achievable security merits by making plan of multiple distinct clouds simultaneously. Different typesof architectures are introduced and discussed according to their safety and privacy capabilities and prospects.

Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The self-service, pay-per-use, on-demand, third-party 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.

Usually, make sure that monolithic system track across various PCs means splitting the file into distinct client and server modules. In such schemes, the client module controlled the user interface and the server provided back-end handling, such as record entrance, printing, and so on. As computers proliferated, cause to decrease in price, and became connected by ever-higher cable networks, splitting technique into multiple parts became more easy, with each part running on a different computer and performing a specialized function. This approach simplified progress, direction, administration, and often improved performance and vigorous, since failure in one computer did not necessarily disable the entire system.

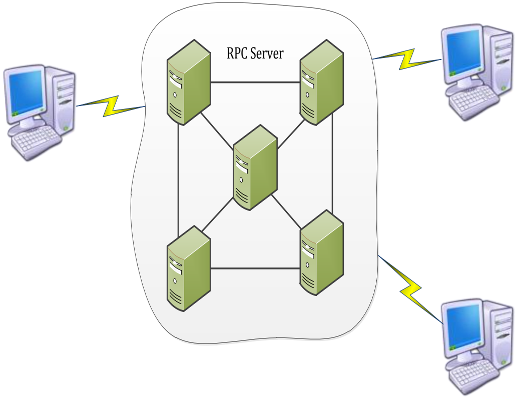

Figure 1 : Architecture of Computing

The ability of the cloud is supported because dividing processes are invoked on behalf of the client. For example, clients can detect a computer (a node) inside the cloud and call a given task; in proposed the task, that computer can invoke functionality on other computers inside the cloud without showing. The further phases or the computer on which they were accepted out, to the client.

With this model, the mechanism of a circulated, cloud-like system can be destroyed down into many distinct packet interactions, or exchanges between distinct nodes. Traditional client-server organisms have two nodes with secure characters and tasks. Modern-distributed organizations can have more than two nodes, and their characters are often dynamic. Once exchange a node can be a client, while in another exchange the node can be the server. In many cases, the final user of the visible

Licensed Under Creative Commons Attribution CC BY

functionality is a client with a user sitting at a console, observing the output. In other cases the distributed system functions unattended, performing related operations.

The distributed system may not have enthusiasticusers and servers for each specific packet exchange, but it is significant to remember there is a visitor. There is also the receiver of the call (often referred to as the server). It is unnecessary to have two-way packet exchanges in the request-reply format of a distributed system; often messages are sent only one way.

2. Related Work

A. What is Cloud Computing?

Cloud computing is the practice of using remote servers on the internet to control, process and store data instead of using a personal computer. This categories into three basic service model: Platform-as-a-service, Software-as-a-Service and Infrastructure-as-a-Service. IaaS (or utility computing) follows a standard utilities model ,providing servers and storage on demand with the consumer paying accordingly. PaaS allows for develop the applications within a provider's structure like Google's App Engine. Saa Sallow customers to use an application on demand via a browser. The example of cloud computing is Gmail, where you can retrieve your stored data from any computer with internet access.

Cloud computing can permit the user to access data and applications from any computer at any time since they are stored on a remote server. It also reduces the need for associations to buy 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 buy for every user as the cloud stores and runs the software remotely. File can also be stored with cloud computing so companies do not have to house servers and databases themselves. By bandwidth, storage, centralized memory & processing in an off-site condition for a fee, cloud computing can significantly reduce costs.

B. Types of Cloud Computing

a) 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.

b) Private Cloud

Private cloud (also referred to as 'corporate' or 'internal' cloud) is a term used to denote a proprietary computing structure providing hosted services on particular networks. This type of cloud computing is used by huge companies and permits 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 advantages of cloud computing, as organizations still need to manage, purchase and set up their own clouds.

c) 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 select to use a public cloud facility for general computing, but store its employment-analytical 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 focus on public clouds, because these facilityrequest for the highest security needs. It also add higher possibility for security prospects. It can provide a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Different types of structure are introduced and discussed according to their security and privacy capabilities and prospects.

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

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

The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as employment-analytical data and processes. When considering using a cloud facility, the user must be aware of the fact that all data given to the cloud provider leaves the own control and protection sphere. Even if locating data-processing applications to the cloud (via IaaS or PaaS), a cloud provider obtains full control on these processes. Hence, a strong belief relationship between the cloud provider and the cloud user is considered a general condition in cloud computing.

Depending on the political context this trust may touch legal rules. For instance, Italian prescription requires that government data of Italian citizens, if collected by official agencies, has to remain within Italy. Hence, applying cloud provider from outside of Italy for realizing an e-government service provided to Italian citizens would immediately violate this rules. Hence, the cloud users must beliefthe cloud provider hosting their data within the borders of the country and never copying them to an off-country location

Licensed Under Creative Commons Attribution CC BY

(not even for backup or in case of local failure) nor providing access to the data to entities from abroad.

An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This may be done unceasingly, multiple times or ones associate degree offender that additionally also has access to the process logic of the cloud can also modify the functions and their input and output data. Even though in the most of instance it may be legitimate to assume a cloud provider to be honest and managing the customers affairs during ahumble and responsible process, there still remains a dangerous of malicious employees of the cloud provider and successful attacks and compromisationby third parties, or of action ordered by a subpoena.

3. Proposed Methodology

Development Phases

Step 1: Registration Module

In registration get username, password, e-mail address, user generate random verification code.New random. Next () is plan to generate random code.The user can sign in and proceed to next step to verification code.Mail is to user email address by using SMTP protocol.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 planed by application to upload and download file from created table.Insert into table FTP details.

Step 3: Upload and Download module

Design a web interface to upload and download files in cloud storage. The variousfile 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, mp3,video etc.

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

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

Step 4: File encryption technique module

Setting up and configuring different cloud server in order to having storage cloud access. Each clouds its own server. Designing encryption techniques like DES, AES, RSA for file decryption before storing it on cloud. In proposed system, we suggest the Triple-DES Algorithm for encryption 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.

.

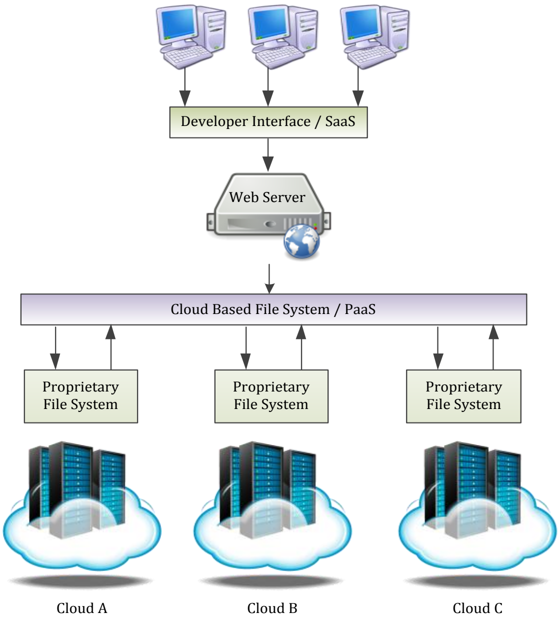

Figure 2 : System Architecture

4. Spliting And Security Scenarios Based on Multicloud Architecture

The basic idea is to planseveral 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 allows an answer to the subsequent question: How can a cloud user avoid fully revealing the data or processing logic to the cloud provider? The data should not only be secured while in the resolute 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 separately 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 extensive computation on encrypted data is done by an untrusted public cloud.

- **Triple-DES**

We use the*3DES algorithm because this algorithm easy to use. 3DES* **is** a way to reuse DES implementation, by chaining three cases of DES with various keys. 3DES is believed to still be secure but it requires 2^{112} operations which is not achievable with foreseeable technology. 3DES is very slow work in software performance because DES was designed for performance in hardware.

Licensed Under Creative Commons Attribution CC BY

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 ciphertext is once more encrypted with a third key).

In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which relates the Data Encryption Standard (DES) cipher algorithm three times to each data block. The actual DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing method of computingpower made brute-force attacks sensible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the requirementto design a completely 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:
Cipher text = E_{K3} (D_{K2} (E_{K1} (plaintext)))
i.e., DES encrypt with K_1, DES *decrypt* with K_2, and next DES encrypt with K_3.
Decryption is the opposite:
Plaintext = D_{K1} (E_{K2} (D_{K3} (cipher text)))
i.e., decrypt with K_3, *encrypt* with K_2, and next decrypt with K_1.
Each triple encryption encrypts one block of 64 bits of data. In all instance the middle operation is the reverse of the first and last. This enhance the strength of the algorithm when using keying option 2, and provides similarity 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), only because of the meet-in-the-middle attack, the powerful security it provides is only 112 bits. Keying choice 2 reduces the effective key size to 112 bits (because the third key is the same as the first). Although, this option is susceptible to certain chosen-plaintext or known plaintext attacks, and thus, it is delegates by NIST to have only 80 bits of security.

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

- **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.

5. Conclusion

By proposed the cloud based storage it 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. A web portal which let the user to manage his data and the managed data should be splitter over the multiple cloud drive as a chunk of file along with encryption. Proposed system will be tested and demonstrate over a local network or on live storage cloud server.

References

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, “Security and Privacy Enhancing Multi-Cloud Architectures”, IEEE Transaction on Dependable and Secure Computing, Jan 2013.

[2] Zhifeng Xiao and Yang Xiao, “Security and Privacy in Cloud Computing”, IEEE Communication Survey & Tutorials, Accepted for Publication, March 2012.

[3] Ayesha Malik, Muhammad MohsinNazir, “Security Framework for Cloud Computing Environment”, Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 3, March 2012.

[4] MukeshSinghal and Santosh Chandrasekhar, “Collaboration in Multicloud Computing Environments: Framework and Security Issues”, Published by the IEEE Computer Society, 2013.

[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom’ “Cloud Computing Security: From Single to Multi-Clouds”, International Conference on System Sciences, 2012.

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

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

[8] 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

[9] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and =8L.L.L. Iacono, “Security Prospects through Cloud Computing by Adopting Multiple Clouds,” Proc. IEEE Fourth Int’l Conf. Cloud Computing (CLOUD), 2011.

Licensed Under Creative Commons Attribution CC BY

[10] 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), 2009.3

[11] 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 ,2012

[12] 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

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

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

[15] 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

[16] Prashant Kumar, Lokesh Kumar,” Security Threats to Cloud Computing”, International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), Volume 2, No. 1, December 2013

Licensed Under Creative Commons Attribution CC BY