IJCSN International Journal of Computer Science and Network, Volume 3, Issue 1, February 2014
ISSN (Online) : 2277-5420
www.IJCSN.org

File Management System in Multi Cloud Storage System

[1] Dolly Talware, [2] Ms. Purnima Soni, [3] R. C. Dharmik

[1,2] Department of Computer Science and Engineering, Nagpur University,
G.H. Raisoni Institute of Engineering and Technology for Women, Nagpur-440034, India

[3] Department of Information Technology, Nagpur University,
Yeshwantrao Chavan College of Engineering, Nagpur, India

Abstract - Cloud computing service providers take advantage of virtualization technologies, combined with self-service capabilities, to offer cost-effective access to computing resources via the internet. But major issue in cloud Computing is security. Several concerns which identify security requirements in cloud computing.. In this Paper, We have proposed to implements, the concept of multiple cloud storage along with enhanced security using encryption techniques. Rather than storing complete file on single cloud system. It will split the file in different chunks then encrypt and store them it on different clouds. The Meta data required for decrypting and rearranging a file and it will be stored in metadata management server.

Keywords - *Cloud, Security algorithm, Tiers*

1. Introduction

Cloud computing signifies important prospect for service sources and initiatives. On the cloud computing, initiatives can reach cost savings, flexibility, and choice for computing resources. They are looking to expand their own promise infrastructure, by adding capacity on demand. Cloud computing, most, simply, extends an enterprise's ability to meet the computing demands of its everyday operation. Offering flexibility and choice, mobility and scalability, all coupled with potential cost savings, there is significant benefit to leveraging cloud computing. However, the area is causing organizations to hesitate most when it comes to moving business workloads into public cloud is security.It looks at the security effects and tasks that IaaSdenotes and offers best performs to service providers and enterprises.

In cloud systems, the client component held the user interface and the server providing back-end processing, such as database access, printing, and so on. For example, if the computers increase cost will be release and became connected by higher bandwidth networks, splitting software systems into multiple modules became more suitable, with each component organization on a different computer and performance a specialized function. This approach basic development, managing, administration, and often improved performance and robustness, since failure in one computer did not necessarily disable the entire system. In many cases, the method appears to the client as a cloudy cloud that accomplishes the necessary operations, even though the distributed system is composed of individual nodes, as illustrated in the following figure.

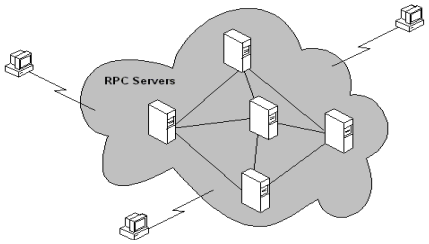

Figure 1: Architecture of Computing

The ability of the cloud is retained because computing operations are invoked on behalf of the client. As such, clients can locate a computer (a node) within the cloud and request a given operation; in performing the operation, that computer can invoke functionality on other computers within the cloud without exposing.

With this model, the mechanics of a distributed, cloud-like system can be broken down into many individual packet exchanges, or conversations between individual nodes.Traditional client-server systems have two nodes with fixed roles and responsibilities. Modern-distributed systems can have more than two nodes, and their roles are often dynamic. In one conversation a node can be a client, while in another conversation the node can be the server. In many cases, the ultimate consumer of the exposed functionality is a client with a user sitting at a keyboard, watching the output. In other cases the distributed system functions unattended, performing background operations. The distributed system may not have dedicated clients and

servers for each particular packet exchange, but it is important to remember there is a caller, (or initiator, either of which is often referred to as the client). There is also the recipient of the call (often referred to as the server). It is not necessary to have two-way packet exchanges in the request-reply format of a distributed system; often messages are sent only one way.

2. Literature Review

In recent year, 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. It will concentrate on public clouds, because these services demand for the highest security requirements. It also includes high potential for security prospects. [1] 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 security and 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 [3]. 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.

3. Proposed Research Methodology

Development Phases:

Step 1: File Management Module

Develop a file management classes in dot net.In this module, the login page of the cloud is open.In this login page the user can sign in and proceed to next step this is file uploading step.

Step 2: User Web access 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.

Step 3: Remote file split and storing module

Using Cloud Server API develop file accessing method in different cloud. In this model, we are splitting the files in different clouds and store the data into multiple cloud.

Step 4: File encryption technique design

Setting up and configuring different cloud server in order to having storage cloud access. Each cloud its own server and server can encrypt the file with is public key.

Step 5: Remote file clubbing module

Developing encryption technique like RSA, AES for file decryption before storing it on cloud. File can club with another file.

In proposed system we are implementing the concept of multiple cloud storage along with enhanced security using encryption techniques [4] [5]. We are splits the file in different chunks then encrypt and store it on different cloud. Meta data required for decrypting and rearranging a file will be stored in metadata management server [6].

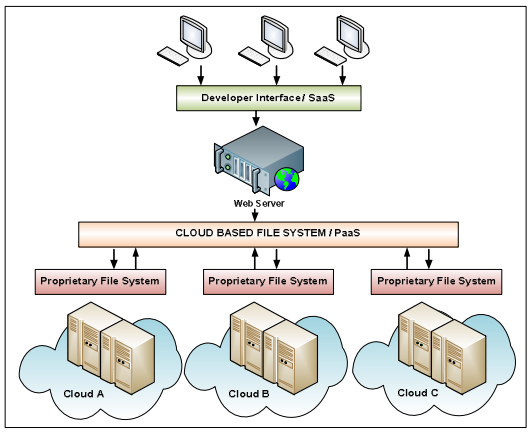

Figure 2: System architecture

RSA is widely used Public-Key algorithm. RSA stands forRon Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we

are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data.

RSA is a block cipher, in which every message is mappedto an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø (n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e <Ø (n) and greatest common divisor of e, Ø (n) is 1. Now e is released as Public-Key exponent.
5. Now determine d as follows: d = e-1(mod Ø (n)) i.e., d is multiplication inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e., (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e., (d, n).

Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).
Steps:

1. Cloud service provider should give or transmit the Public-Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is C = me (mod n).
4. This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption:

Decryption is the process of converting the cipher text(data) to the original plain text(data).
Steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e., C.
3. The Cloud user then decrypts the data by computing,
m = Cd (mod n).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

4. Conclusion

A web portal which let the user 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] 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, Xiaohua Jia, Bo Zhang, and Ruitao Xie, "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] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.

[6] 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.

[7] Kan Yang, Xiaohua Jia, " 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.

[8] 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.

[9] C. Selvakumar G. Jeeva Rathanam M. R. Sumalatha ," PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique," IEEE,2012.

[10] Akash Kumar Mandal, Mrs Archana Tiwari , " Performance Evaluation of Cryptographic Algorithms: DES and AES," inProceeding of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science,IEEE 2012.

[11] 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.

[12] 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