ISSN:2320-0790

An International Journal of Advanced Computer Technology

Enhancing the Cloud Security by Using Identity Based Multicloud Architecture

Rutuja G. Warhade[1], Basha Vankudothu [2]

[1]PG Scholar, [2]Professor
Dept. of Computer Engineering,GSMCOE, Pune

Abstract: In today's IT world Cloud computing is emerging as a most powerful technology. Cloud provides the user with the resources on a pay-as-you go basis, which fulfils the demand of most of the industries. Security challenges are the biggest obstacles in adopting cloud services. This triggered 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 unique features, which open the path towards novel security approaches, techniques and architectures. This paper provides a scheme to enhance the security of stored data in the cloud by using multiple clouds and identity verification of the user.

Keywords: cloud; cloud security; data security; splitting; identity

I. INTRODUCTION

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. Clouds can be categorized taking the physical location from the viewpoint of the user into account [1]. Cloud service providers offer a Public Cloud, this are the resources outside the cloud users premises. If the cloud system is installed within the user's premise this setup is called Private Cloud. A hybrid approach that is the combination of public and private is denoted as Hybrid Cloud. Public clouds demand for the highest security requirements hence the paper will mainly focus on public clouds.

Traditionally, having a monolithic system run across multiple computers means splitting the system into separate client and server components. In such systems, the client component handled the user interface and the server provided back-end processing, such as database access, printing, and so on [2]. As computers proliferated, dropped in cost, and became connected by ever-higher bandwidth networks, splitting software systems into multiple components became more convenient, with each component running on a different computer and performing a specialized function. This approach simplified development, management, administration, and often improved performance and robustness, since failure in one computer did not necessarily disable the entire system.

In many cases the system appears to the client as an opaque cloud that performs the necessary operations, even though the distributed system is composed of individual nodes, as illustrated in the following figure.

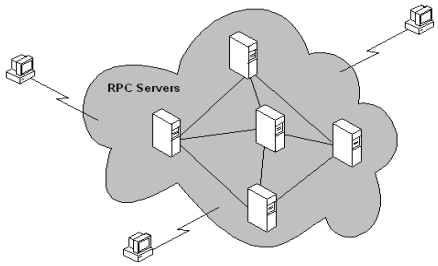

Figure 1: Architecture of Computing

The capacity of the cloud is maintained 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. The additional steps or the computer on which they were carried out, to the client.

With this paradigm, 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 [3]. 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.

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. 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 [8]. 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. PROPOSED WORK

In proposed system we are implementing the concept of multiple cloud storage along with enhanced security using encryption techniques and user identity verification. We are going to splits the file then encrypt and store it on different cloud service providers. The details of the CSP remain with the file user itself. The device of the user can be registered with the system as the users identity, and this will serve as an enhanced security feature while data access on the cloud storage. The figure below shows the system architecture.

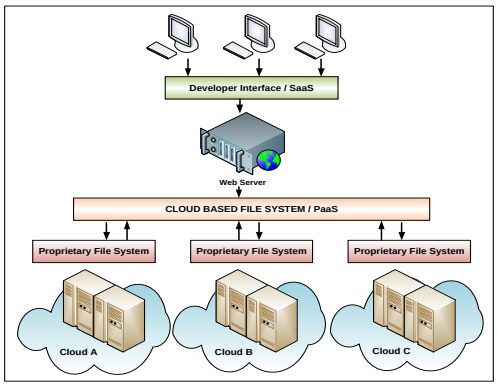

Figure 2: System Architecture

A. *Plan of Execution*

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 system consists of following phases:

- User web access and device registration.
- File encryption technique design.
- Remote file splitting and storing.
- Maintaining users FTP details.
- Remote file clubbing.
- File decryption technique and download.

These are the phases of system to store and maintain the security of the file in the cloud. We will briefly describe each of these phases.

1) User web access and device registration: In this phase user will be registered with the system and the users device from which he logs into the system will be considered as the users identity. The user has to use the same device each time to login into the system. The users credentials will be mailed to him on the verified email id.

2) File encryption technique design: The file uploaded by the user will be encrypted by using the AES encryption algorithm. The user has to provide the encryption key while uploading the file to the system.

3) Remote file splitting and storing: The encrypted file is splitted into small chunks. The splitted file will be stored on different clouds through different FTP. Each cloud provider holds only a single chunk (part) of the file. Hence the security is enhanced, as a single clod service provider doesn't posses the entire user data.

4) Maintaining users FTP details: The user has to provide the FTP details where the files will be stored. The details include FTP IP address, username and password etc. These

details will be used by the system to connect to each FTP and upload a single part of the file over there.

5) Remote file clubbing: The file that is splitted and stored on multiple clouds needs to be clubbed when the user downloads it. In this phase the chunks of the file are collected from each FTP and the chunks are clubbed together to form the original file, which was uploaded by the user.

6) File decryption technique and download: When the file is clubbed it is still in the encrypted form. The user has to provide the encryption key while downloading the file. In this phase the file is decrypted using the user provided key and is downloaded on the users machine.

B. System Model

The system will be more clearly understood by depicting it through the use case diagram and sequence diagram. The following figure shows the system models.

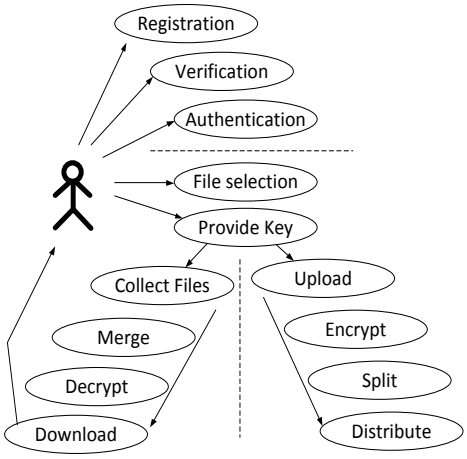

Figure 3: Use Case Diagram

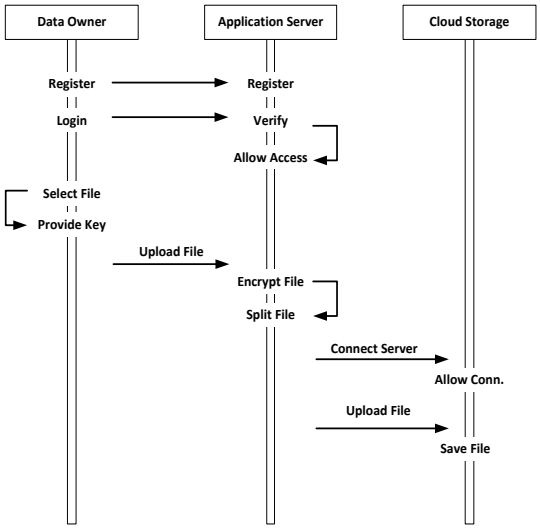

Figure 4: Sequence Diagram

IV. CONCLUSION

Cloud computing is an emerging computing paradigm that is increasingly popular. Leaders in the industry, such as Microsoft, Google, and IBM, have provided their initiatives in promoting cloud computing. One of the other aspects of the cloud is the social aspect of it. The Cloud is going to happen but which services should be offered on the cloud and for whom. What happens if smaller IT companies start to offer their services on the cloud and no one uses them? It is believed that everything eventually can move to the Cloud. The question is if users are ready for that and if it's the right move then this need must be addressed.

By implementing 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

REFRENCES

[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.

[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] 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