International Journal of Research in Engineering, Science and Management
Volume-3, Issue-1, January-2020
www.ijresm.com | ISSN (Online): 2581-5792

Approach to Multi-Cloud Based Distributed File Storage Security Enhancement

Mithilesh R. Zade[1], Rashmi Jain[2], Ashwini Yerlekar[3]
[1]*M.Tech. Student, Department of Computer Science and Engineering, Rajeev Gandhi College of Engineering & Research, Nagpur, India*
[2,3]*Assistant Professor, Department of Computer Science and Engineering, Rajeev Gandhi College of Engineering & Research, Nagpur, India*

***Abstract*: In modern centuries use of cloud computing in different mode like cloud storage, cloud hosting, cloud servers are increased in industries and other organization as per requirements. While considering the power, stability and the security of cloud one can't ignore different threats to user's data on cloud storage. File access mechanism is an actual technique to guarantee the file safety in the cloud. On the other hand, due to file farm out and untrusted cloud servers. The file entrance mechanism develops an exciting issue in cloud storage systems. In effect right to use mechanism systems are no extended related to cloud storage schemes, because they also produce various converted copies of the similar files or involve a completely reliable cloud server. Malicious user at cloud storage is become most difficult attacks to stop. This paper state the different methodology available to overcome the problem of cloud security.**

***Keywords*: Multi-Cloud, Distributed file storage security.**

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 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 obstacles when considering the adoption of 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 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.

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.

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, 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. 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 execution 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.

2. Background

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

1) 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.

2) 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 organizations still need to purchase, set up and manage their own clouds.

3) 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 centre. 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 distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects.

3. Literature survey

Proposed by Mambo and Okamoto [1], a proxy cryptosystem is a system where a user can delegate his/her decryption right to a designated decrypter. Subsequently, Blaze, Bleumer and Strauss extended this notion by introducing the concept of proxy re-encryption (PRE). In this new cryptographic primitive, a proxy server can transfer a ciphetext designated for one user to another cipher text designated for another user without the need to have the knowledge on the plaintext. Since then, some useful PRE schemes have been proposed accordingly. Weng, et al. proposed a new PRE scheme called conditional PRE (C-PRE). In this scheme, only the cipher texts, which satisfy the condition given by the original decryptor can be transferred to the cipher texts for a designated decryptor, instead of all cipher texts. Subsequently, Fang, et al. extended the notion of C-PRE to be hierarchical C-PRE (HC-PRE). In this scheme, a proxy server can delegate his re-encryption right to other proxy servers under a specified condition. Furthermore, they pointed out some application scenarios, such as ZigBee security for visitors in home automation, privacy-preserving location sharing protocol etc.

Ateniese, et al. [2] improved the concept of PRE and employed it to data storage. In their scheme, the owner encrypts his/her files and outsources them to a proxy server. The proxy server can transfer a cipher text for the owner to a cipher text for the requester if and only if he has obtained a re-encryption key from the owner.

Introduced by Shamir [3], identity-based encryption (IBE) is an efficient cryptographic system where the public key can be any arbitrary string and the secret key is extracted from a trusted party called private key generator (PKG).

Boneh and Franklin [4] proposed the first practical IBE scheme based on the bilinear group. Since its seminal introduction, IBE schemes have been discussed extensively as in this new cryptographic notion, the need for public key infrastructure (PKI) has been eliminated efficiently.

Ivan and Dodis [5] proposed two identity-based proxy encryption schemes where the master secret key held by the PKG is split into two parts. One is for the user and the other is for the proxy server. Then, the user can cooperate with the proxy server to decrypt a ciphertext. Unfortunately, these schemes are not secure against the collusion attacks as the user and the proxy server can collaborate to compute the master secret key.

Green and Ateniese [6] introduced the concept of identity-based proxy re-encryption (IBPRE). In an IBPRE scheme, a proxy server can transfer a ciphertext encrypted under one identity to a ciphertext encrypted under another identity without learning the contents of the plaintext.

Subsequently, Matsuo [7] proposed two IBPRE schemes. In the first scheme, a ciphertext encrypted under traditional PKI can be transferred to a cipher-text encrypted under an identity in IBE schemes. Meanwhile, the second scheme is proposed to transfer a ciphetext encrypted under the identity of the original decrypted to a ciphertext encrypted under the identity of the designated decrypter.

Wang, et al. [8] proposed two new IBPRE schemes. The relationships between the IBPRE secure against chosen plaintext attacks and the PRE properties: unidirectional, non-transferable and collusion safe. It was proposed31 that the proxy server can transfer a ciphertext for the original decrypted to a ciphertext for the designated decrypter, and decrypt the ciphertext for the original decrypter. Additionally, the original

decrypter can revoke the decryption and re-encryption rights of the proxy server. In the schemes, the re-encryption key must be computed with the help of the PKG.

4. System architecture

To address the security issues mentioned above the method of "Enhancing data security using redundant array of independent cloud storage" is proposed. This scheme captures following properties:

1. The file owner can decide the access permission of the file.
2. For one query the receiver can access single file instead of all files of the owner
3. The scheme is secured against collusion attacks.
4. The file is divided in smaller chunks and stored on multiple clouds to reduce the risk downtime due to a localized hardware, software, or infrastructure failure in a cloud-computing environment.
5. The file is merged and decrypted when requested by the authenticate user.

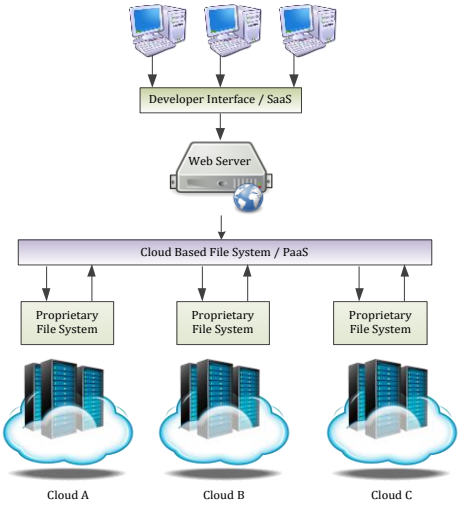

Fig. 1. System architecture

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.

5. 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. However, the public literature that discusses the research issues in cloud computing are still inadequate. In a study of the research literature surrounding cloud computing. By implementing the cloud-based storage it solves 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, 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] 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," in Proceeding of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE 2012.
[11] J. D. Ramkumar, 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, Volume 2, No. 1, December 2013.