Single to Multi Cloud Security Issues

[1]Vakkalagadda.J.R.V.Sai Mounika, [2]K.Varada Raj Kumar
[1,2]Sir C.R.Reddy College of Engineering, Eluru, Andhra Pradesh, India

Abstract
Cloud Computing has established its roots in the IT industry as an alternative technology for traditional computing. The user applications can be deployed easily on the cloud under shared server and storage resources. Keeping the untrusting nature of the Cloud service providers, the security of the data stored in shared resources like cloud environment is at risk. The researches of the cloud environment focus on the single to multi cloud security. In this paper it is studied and understands that security in multi clouds can be further increased by using the Secret Sharing Algorithm. It suggests that it is better to shift from single to multi clouds for better security.

Keywords
Cloud Security, Single to Multi Clouds, Secret Sharing Algorithm

I. Introduction

The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers. One of the solutions that they propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al. State that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al. Claim that using the Byzantine fault tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place. Another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password. Another major concern in cloud services is service availability. Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.

II. DepSKy System Model

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Bessani et al. explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

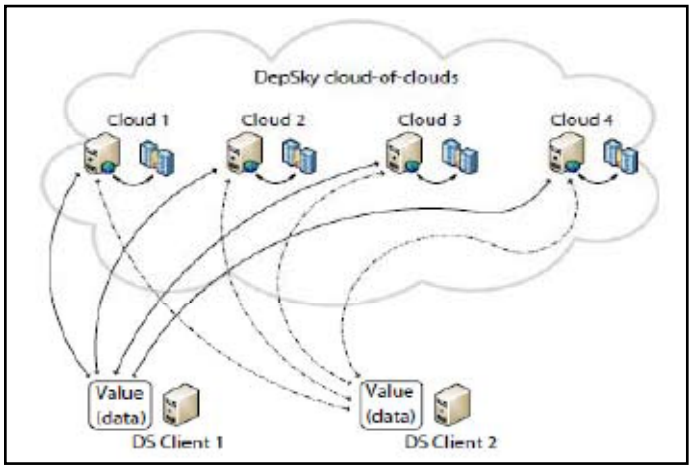

Fig: Architecture – Depsky Model.

III. Existing System

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds".

Disadvantages of Existing System:

1. Cloud providers should address privacy and security issues as a matter of high and urgent priority.
2. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

IV. Proposed System

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with

a third party, cloud computing users want to avoid an un-trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed.

Advantages of Proposed System:

1. Data Integrity
2. Service Availability.
3. The user runs custom applications using the service provider's resources
4. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure.

V. Conclusion

Security is the reason due to which most of the businesses hesitating for moving their workload to cloud computing. Cloud clients fear to lose their private information if malicious insiders in the cloud. Also service availability is area to be concerned in single cloud, if that cloud fails. In multi-cloud data is replicated so available even if on cloud fails. Integrity of data is also maintained in our proposed work by making use of MD5.We are making use of strongest cryptographic algorithm named Shamir's secrete sharing algorithm, which has number of advantages including security, client-side aggregation.

References

[1] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom,"Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences, 2012.
[2] (NIST), [Online] Available: http://www.nist.gov/itl/cloud/.
[3] Hassan Takabi, James B.D., Joshi, Gail-Joon, Ahn, "Security and Privacy Challenges in Cloud Computing Environments", University of Pittsberg, October 2010.
[4] A. Shamir,"How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.
[5] A. Bessani, M. Correia, B. Quaresma, F. André, P.Sousa, "DepSky: Dependable and secure storage in a cloud-of-clouds", EuroSys'11: Proc. 6thConf. On Computer systems, 2011, pp. 31-46.
[6] Md Kausar Alam, Sharmila Banu K,"An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds", International Journal of Scientific and Research Publications, Vol. 3, Issue 4, April 2013
[7] A. Juels, B.S. Kaliski Jr,"PORs: Proofs of retrievability for large files", CCS '07: Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 584-597.
[8] C. Cachin, I. Keidar, A. Shraer,"Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.