International Journal of Advancement in Engineering Technology, Management & Applied Science

Volume 1, Issue 7 December 2014 ISSN No: 2349-3224

Multi-Cloud Storage Using Shamir's Secret Sharing Algorithm

Gaidhankar Sushil, Kanase Amit, Lonkar Tushar, Patil Chetan

Computer Dept. JSPM'S JSCOE, Hadapsar

Abstract:

Now a day's rapidly increased use of cloud computing in the many organization and IT industries and provides new software with low cost. So the cloud computing give we lot of benefits with low cost and of data accessibility through Internet. The security risks of the cloud computing is the main factor in the cloud computing environment, eg. sensitive information with cloud storage providers may be entrusted. But „single cloud" providers are a less popular with customers due to risks service availability failure and possibly of malicious insiders in the „single cloud". A towards movement of multi clouds "or multiple clouds" or "cloud-of-clouds" has emerged currently using Shamir's Secret Sharing Algorithm.

This project surveys to many running research related paper to single cloud and multi clouds security using Shamir's Secret Sharing algorithm and addresses possible solutions and methodology. The basis idea this paper use of multi clouds and data security and reduce security risks and affect the cloud computing user using Shamir's Secret sharing algorithm. It is a way of secret sharing, where a secret is divided into number of parts, which is giving each participant its own unique part, where may be some of the parts or all of them are required in order to reconstruct the secret. If we're going to Count all participants to combine together the secret might be impractical, and therefore the threshold scheme is used where any "k" of the parts are sufficient to reconstruct the original secret.

Keywords: **Private cloud; public cloud; access control; Privacy.**

Introduction:

At the present a day's, rapidly increased use of cloud computing in the many organizations and IT industries can provide new software with a minimum cost. The cloud computing give we lot of benefits with low cost and of data accessibility through Internet. The security risks of the cloud computing is the main factor in the cloud computing environment, eg. sensitive information with cloud storage providers may be entrusted. But a single cloud provider is a less popular with customers due to risks such as service availability failure and possibility of malicious insiders in the single cloud. A towards movement of multi clouds or cloud of-cloud has emerged currently using Shamir's Secret Sharing Algorithm.

Main focus of our proposed system is use of multi cloud and data security and reduces security risks and affects the cloud computing user using Shamir's Secret sharing algorithm. It is a way of secret sharing, where a secret is divided into multiple parts, which is giving each participant its own unique part, where some of the parts are required in order to reconstruct the secret. If we are going to Count all participants to combine together the secret might be impractical, and therefore the threshold scheme is used where any 'k' of the parts are sufficient to reconstruct the original secret.

International Journal of Advancement in Engineering Technology, Management & Applied Science
Volume 1, Issue 7 December 2014 ISSN No: 2349-3224

Literature survey:

Sr.No	Paper Name	Methodology	Disadvantages
1	A Practical Guide to cloud computing Security **By- Carl Almond August 2009**	*Giving risk and mitigation*	Points only the security of single cloud
2.	Security Challenges for public cloud **By- Kui Ren, Cong Wang Jan 2012**	Outlineing & motivat e Challenges further investigation	As maintaining security in public cloud, urgency of data not comes into picture
3.	Foundations and Properties of Shamir's Secret Sharing Scheme **By- Dan Bogdanov May 2007**	*Encryption & Decryption*	Properties related to Shamir's Secret Sharing

Architecture:

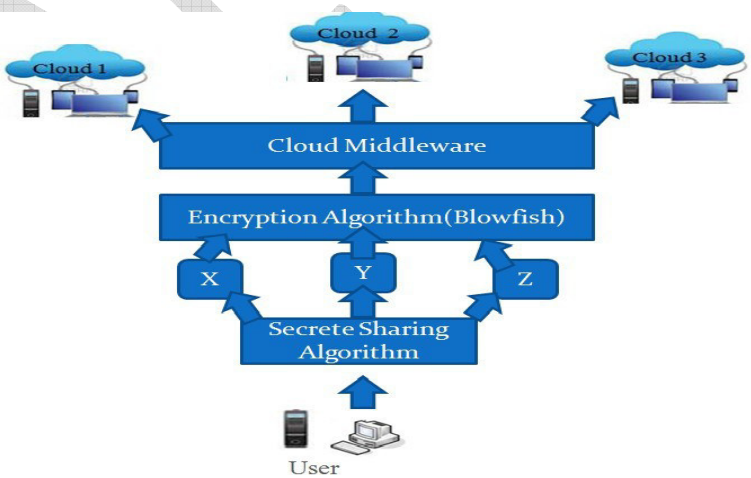

Fig.1 Architecture of Multi-Cloud Storage Using Shamir's Secret Sharing Algorithm

Future Work:

Our Project multi cloud storage using Shamir's secret sharing algorithm is extremely effective for storing the client data securely. It provides security by encryption and decryption and also provides authentication. Our project can be enhanced in following ways:

- To provide more security by using more strong encryption algorithm.
- To provide fast service to store data on server.
- Giving proof of integrity of the data to client.
- Reduce storage overhead of the customer by compressing the data.

Reduce computational overhead of the cloud storage server

Conclusion:

The purpose of this work is to study and design single cloud and multi-cloud using secret sharing algorithm and to address the security risks and solutions using Shamir's Secret Sharing algorithm. These algorithms generate their own secret sharing schemes and use secure channels to distribute shares among themselves. The Shamir's secret sharing scheme has a good abstract foundation which provides an excellent framework for proofs and applications.

Acknowledgment:

The authors would like to thanks to the publishers, researchers for making their resources available and teachers for guidance. We also thank to the college authority for supporting to us and providing required information. We would also like to thanks our friends and family members.

References:

[1] Axel Buecker, Koos Lodewijkx, Harold Moss, Kevin Skapinetz, Michael Waidner, "Cloud Security Guidance", a red paper, January 2011.
[2] Hassan Takabi, James B.D., Joshi, Gail-Joon, Ahn, "Security and Privacy Challenges in Cloud Computing Environments", University of Pittsberg, October 2010.
[3] Neil Robinson, Lorenzo Valeri, Jonathan Cave and Tony Starkey (RAND Europe), Hans Graux (time.lex), Sadie Creese and Paul Hopkins (University of Warwick), "The Cloud: Understanding the Security, Privacy and Trust Challenges", TR-933-EC, 30 November 2010, Prepared for Unit F.5, Directorate –General, Information Society and Media, European Commission.
[4] J. Archer, A. Boehm, "Security Guidance for Critical Areas of Focus in Cloud Computing", Cloud Security Alliance, December 2009.
[5] SNIA, Advancing Storage and Information Technology, "Cloud Storage for Cloud Computing", Storage Networking Industry Association,September 2009.