Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multi-cloud Data Security Using Shamir's Secrete Shearing

Desale Rutuja M., Jagtap Priya C., Labhade Swati P., Rokade Priyanka M., Prof. M. T. Jagtap
Dept of Computer, University of Pune,
Pune, Maharashtra, India

Abstract— In this competitive world, many organization uses the cloud computing. Due to this, the major issue is arises about security. There are many issues and possibilities of malicious insiders present in single cloud. But multi-cloud provides more security and efficiency for the users and researchers.

This paper surveys secret creation and the intrusion detection architectures. These are combined to provide a complete solution for security requirements. Data Integrity is provided for data. An integrated intrusion detection system is proposed to handle malicious attacks.

Keywords- cloud computing, Multi-cloud, secret, data intrusion, malicious insider.

I. INTRODUCTION

The cloud computing could be a cost-efficient, service convenience, versatile and on demand service delivery platform for providing business through the net. Cloud computing resources will be quickly extracted and effortlessly scaled with all the processes, services and applications provisioned on demand service despite the results of the user location or device. Hence, the chance for a company to reinforce their service rescue efficiencies is achieved through cloud computing. the problems in cloud security series from substantial security of the cloud fixing and hardware infrastructure, through the beaux arts security of operate and information deployments, to the particular security of the cloud framework within the presence of peripheral attacks and therefore the mechanisms accessible to retort to and recuperate from these attacks .

Cloud computing suppliers ought to address privacy and security as matter for higher and imperative priorities. The managing single cloud suppliers is changing into less standard service with customers owing to potential issues like service convenience failure for a few time and malicious insider's attacks within the single cloud. Thus currently move from single cloud to multi clouds, inter-cloud or cloud of clouds.

The data security facet of cloud computing, information and knowledge are shared with a 3rd party with none hacks. each cloud users need to avoid untrusted cloud supplier for private and vital documents like debit/credit cards details or study from hackers or malicious insiders is that the importance. It provides secure cloud information that may forestall security risks. Apply multi clouds conception victimization Shamir's Secret Sharing formula that\'s cut back risk {of information of knowledge of information} intrusion and loss of service convenience for making certain data.

II. MULTI-CLOUD ENVIRONMENT

These days, organizations tend to accept over one cloud for services. The clouds may well be public clouds, personal clouds still as hybrid clouds. Organizations have started operating during this multi cloud setting so they ne'er face lack of availableness of a service or a resource at any purpose of your time and will forestall from potential loss. Conjointly trusting one cloud is risky as there may well be some malicious user or code UN agency is spying on the info being changed. So, to upset these problems multi cloud environments have gained importance. The term multi cloud as outlined by Vukolic is "cloud of clouds" that says that the term cloud computing mustn't find yourself as one cloud". The foremost well-liked is that the public cloud. Here, the supplier of cloud services provides the user with applications, storage, resources etc. it's majorly the responsibility of the cloud supplier to produce the options of security, availableness, measurability etc. The infrastructure for provided such clouds are typically shared. Customers are either charged on a pay-per-use basis or it should even be free like 1st 500MB of Google App Engine are free. Alternative well-liked clouds are the personal cloud inside a corporation. it should be connected via net or computer network. it's created exclusively to be used by a corporation and its users. Hence, security issues are less here because it conjointly features a dedicated infrastructure for its cloud thence multi abidance issue is additionally avoided. However, managing the cloud, its data, users etc. all stay the responsibility of the organization providing the cloud. Users are typically not needed to procure such cloud. There may additionally be a condition wherever each these clouds and their services could also be needed. Such a state of affairs results in hybrid cloud. Rules and protocols are to be developed to use hybrid cloud as per the necessity and convenience.

III. WHY WE WANT CLOUD DATA SECURITY

Cloud computing ought to secure enough in maintaining cloud users trust. Secure shopper information and communication needs for evaluating cloud security. Distinctive security necessities for possible answer that eliminates potential threats, Confidentiality, integrity is provided to secure inter-working of data.

Security necessities are:

1. Authentication
2. Authorization
3. Confidentiality

Cloud computing, in currently days it's been enjoying a vital role in terms of knowledge storing and reducing the general value to entrepreneurs. However most of them distressed concerning security; largely they accustomed keep the information in single cloud. During this case if {the information the info the information} is lost or hacked within the sense entire data are loose. To avoid these forms of vulnerabilities and to realize higher security system proposing of multi cloud wherever the information are keep in numerous databases means that clouds. it's discovered that the employment of multi cloud suppliers to keep up security has received less attention from the analysis community than has the employment of single clouds. The system aims to push the employment of multi-clouds owing to its ability to scale back security risks. In cloud information is been ever-changing dynamically from user facet during this case hacker might have an opportunity to hack the information through the network or assaultive on the information.

A. System Architecture

The use of cloud computing has increased rapidly in many organizations. Cloud computing is beneficial in terms of low cost and accessibility of data. The major factor in the cloud computing environment is ensuring the security of cloud computing, as users often store confidential 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, "inter-clouds" or "cloud-of-clouds" has emerged recently. This system recent research related to single and multi-cloud security and addresses possible solutions. It is observed 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.

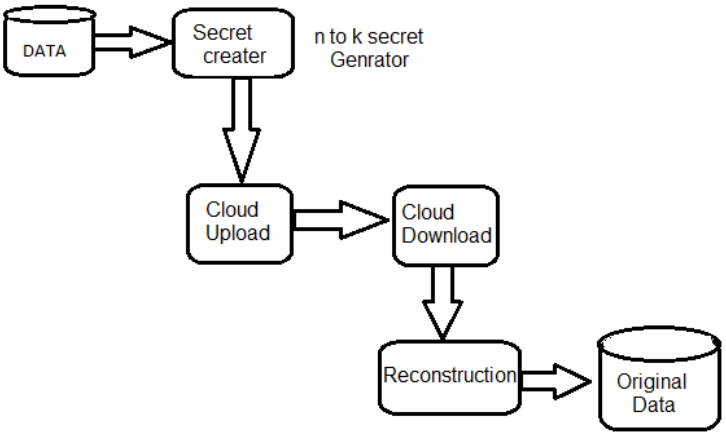

Figure 2: System Architecture

IV. RELEVANT THEORY

A. Google Drive

Google Drive could be file storage and synchronization service provided by Google, free on 24th April 2012, that allows user cloud storage, file sharing and cooperative written material. Rumors regarding Google Drive began current as early as March 2006. Google Drive is that the home of Google Docs, associate degree workplace suite of productivity applications that supply cooperative written material on documents, spreadsheets, shows, and more. Initially 15 GB (originally 5 GB) of on-line storage space is offered by Google drive usable across 3 of its most-used services: Google Drive, Gmail, and Google+ Photos (aka Picasa net Albums). 100 GB to 16 TB additional storage space is shared between Picasa and Google drive through a paid monthly subscription plan(USS 4.99 per month for 100 GB) A user with any paid storage doesn't get any free storage together with the paid storage. For Google Drive to synchronize files between the user\'s laptop and Google Drive storage, the Google Drive shopper code should be running on the user\'s laptop. The shopper communicates with Google Drive to cause updates on one facet to be propagated to the opposite in order that they each ordinarily contain identical knowledge.

B. Dropbox

Dropbox could be a free cloud storage service for sharing and storing files together with photos, documents and videos. To use Dropbox you would like to make Associate in Nursing account on dropbox.com and permit the service to make folders on all of your connected devices alternative mobile devices} and synchronize any files you store on Dropbox with the connected devices. Files may be shared with others by providing them with a link to your Dropbox folder. Dropbox came in July 2012 once the corporate proclaimed that some users received spam on email accounts that were connected entirely to Dropbox accounts. As rumored on Datamation, Associate in Nursing investigation discovered that passwords

purloined from alternative websites were wont to gain access to atiny low variety of Dropbox accounts, however the breach inspired Dropbox to institute new procedures to enhance the cloud storage platform\'s security. Dropbox offers free storage accounts BGB storage space) and paid accounts for choices between 50GB and 100GB of storage. Dropbox shopper supports synchronization and sharing in conjunction with personal storage. It supports revision history, thus files deleted from the Dropbox folder is also recovered from any of the synced computers. Dropbox additionally pro- vides a technology referred to as computer network adjust, that permits computers on an {area a neighborhood} area network to firmly transfer files domestically from one another rather than continually touch the central servers. LANSync was developed by Dropbox Engineer Paul Bohm.

V. DESIGN AND IMPLIMENTATION

Shamir's secret sharing mechanism is based on polynomial evaluations. The computation operations on input secrets and distributes the resulting shares to other parties which are performed by the central party dealer. When the secret has to be regenerated, the parties give their shares to the dealer, which can then combine the shares and obtain the secret. An intruder needs to retrieve at least three values to find out the original value that wants to keep away from the intruder. This depends on Shamir's secret sharing algorithm with a polynomial function technique which claims that even with full knowledge of (k 1) clouds, the service provider will not have any knowledge of s1 (s1 is the secret value) in other words, hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud. Therefore, if the hacker hacked one cloud providers password or even two cloud providers passwords, they still need to obtain the third cloud provider (in the case where k = 3) to know the secret which is the worst case situation. Hence, replicating data into multi-clouds by using a secrete shearing technique may reduce the risk of data intrusion and increase data integrity.

Example of Shamir Secrete Sharing Algorithm:

The following example illustrates the basic idea. Note, however, that calculations in the example are done using integer arithmetic rather than using finite field arithmetic. Therefore the example below does not provide perfect secrecy, and is not a true example of Shamir's scheme.

Secret creation:

1. Suppose that secret is 1234(s=1234).
2. We wish to divide the secret into 6 parts (n=6),
   Where any subset of 3 parts (k=3) is sufficient to reconstruct secret.
3. We select 2 random numbers: 166, 94. (a1=166, a2=94).
   Our polynomial to produce secret shares (points) is therefore:
   F(x) = 1234+166x+94x2.
4. We construct 6 points from the polynomial:
   (A,1494),(B,1942),(C,2578),(D,3402),(E,4414),(F,5614).

We give each participant a different single point.

- Reconstruction:

In order to reconstruct the secret any 3 points will be enough.

Let us consider.

(x0, y0)=(B,1942), (x1,y1)=(D,3402), (x2,y2)=(E,4414)

We will compute Lagrange basis polynomials:

$$\text{Lo}= \frac{x-x1}{x0-x1} * \frac{x-x2}{x0-x2} = \frac{x-4}{2-4} * \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\text{L1}= \frac{x-x0}{x1-x0} * \frac{x-x2}{x1-x2} = \frac{x-2}{4-2} * \frac{x-5}{4-5} = \frac{-1}{2}x^2 + \frac{7}{2}x - 5$$

$$\text{L2}= \frac{x-x0}{x2-x0} * \frac{x-x1}{x2-x1} = \frac{x-2}{5-2} * \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$f(x) = \sum_{j=0}^{2} yj.lj(x)$$

$$= 1942\left(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}\right) + 3402\left(\frac{-1}{2}x^2 + \frac{7}{2}x - 5\right) + 4414\left(\frac{1}{3}x^2 - 2x + \frac{8}{3}\right)$$

$$= 94x^2 + 166x + 1234$$

VI. FUTURE SCOPE

For future work, system aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community.

VII. CONCLUSION

This system concludes here that the data of enter pruners is very volatile to the enterprises. At the same time providing a security to that data is a big deal to cloud owners as well as firm maintainers. It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. The research has been done to ensure the security of the single cloud and cloud storage whereas multi- clouds have received less attention in the area of security. This system supports the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

ACKNOWLEDGMENT

We express our profound gratitude to the *Dr. N. S.Walimbe (Principal)* forallowing us to proceed with the seminar and also for giving us full freedom to access the lab facilities. Our heartfelt thanks to our guide and HOD *Prof. M. T. Jagtap* for taking time and helping us through our seminar. He has been a constant source of encouragement without which the seminar might not have been completed on time. Weare very grateful for his guidance. We express our immense pleasure and thankfulness to all the teachers and staff of the Dept. of Computer
Engineering for their cooperation and support.

REFERENCES

[1] Satyakshma Rawat, “One Time Password for Multi-Cloud Environment”,International Journal of Advanced Research in Computer Science and Software Engineering, March 2013
[2] M. Vukolic, "The Byzantine empire in the inter cloud", ACM SIGACT News, 41, 2010, pp.105-111.
[3] M.A.Alzain, E.Pardede, B.Soh, J.A.Thom: “Cloud Computing Security: From Single To Multi Clouds”, 45th Hawaii International Conference on System Sciences, 2012.
[4] (NIST), http://www.nist.gov/itl/cloud/.
[5] James A. Thom,” Cloud Computing Security: From Single to Multi-Clouds”, IEEE, 2012

