A NEW APPROACH FOR CLOUD DATA SECURITY: FROM SINGLE TO CLOUD-OF-CLOUDS

[1]NIKHIL SHRIVASTVA, [2]POORVA ANDURKAR, [3]AJAY SURVASE, [4]SHUBHADA BHANDARE, [5]SUNIL KALE

[1,2,3,4,5]Savitribai Phule Pune University, India
E-mail: nikhil43874@hotmail.com, a992poorva@gmail.com, ajaysurvase768@gmail.com, shubdha24@gmail.com, kalesunild@gmail.com

Abstract- In the corporate world, a large number of people store their data on clouds. For doing this they need to give their confidential data in the hands of the third party, commonly known as service providers. These cloud service providers cannot be trusted since the complete data is stored in one single cloud. This increases security risks to the user's sensitive data. Due to this issue of data integrity risk and service availability failure, the concept of "Cloud-of-Clouds" comes into picture. Cloud-of-clouds are also known as "inter-clouds" or "multi-clouds". Use of cloud-of-clouds provides a higher level of security to the user's confidential data. The aim of this paper is to secure the user's data by using cloud-of clouds.

Keywords- Cloud Computing, Cloud-Of-Clouds, Inter-Clouds, Multi-Clouds, Security, Confidential Data, Data Integrity.

I. INTRODUCTION

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. Users often store sensitive information with cloud storage providers but these providers may be un-trusted. Working with "single cloud" providers is becoming less popular with customers due to risks of service availability failure and the possibility of data leakage. A movement towards "cloud-of-clouds", or in other words, "inter-clouds" or "multi-clouds" has emerged recently. This paper surveys recent research related cloud-of-clouds security and addresses possible solutions- one of the solutions being data distribution and replication for storage and retrieval on multiple clouds. The research into the use of cloud-of-clouds 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 cloud-of-clouds due to its ability to reduce security risks that affect the cloud computing user.

II. BACKGROUND

NIST describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

III. SECURITY RISKS IN CLOUD COMPUTING

Now a days many organizations are using the cloud services to store their precious data on the cloud. These organizations also include defense agencies and international research companies. So it all sums up to the security provided by the cloud environment. In the single cloud storage all the data is stored at one centralized storage system. If someone tries to illegally access the data, the hacker ends up getting the entire information stored at a single location. Hence, the use of single cloud storage is not that reliable. Another possibility of losing the data is a server crash. In this case as well the user is not able to access his data. Although cloud service providers can offer benefits to users, security risks are a major problem in the cloud computing environment. As the cloud storage is an online service, any problem with the internet security will also affect the cloud services.

IV. NEED FOR FILE REPLICATION ON CLOUD-OF-CLOUDS

This paper concentrates on providing security in the multi-cloud environment. The data is distributed in different clouds. Each cloud then generates a unique key that is further given to the user. When the user wants to access his data he can do so by using this key. However, if a particular cloud crashes or is hacked it is the loss of the user- as the user does not get the entire data. To overcome this issue, each of the distributed data unit is replicated and stored in another server and is recognized by the key generated for that unit by the original cloud. If any problem occurs in the clouds, this data can be retrieved from the server. Thus there is no loss of the user's data.

V. MATHEMATICAL MODEL

When the user uploads data, the system generates a secret key which is invisible to the user. This secret key is used to form polynomial from which the three

keys from different clouds are generated.
`

We are using (k, n) threshold where (k < n), k denotes number of clouds and n denotes number of bytes in the file.

Choose at random (k-1) coefficients a_1, a_2, a_3 … a_{k-1}, and secret key be a_0

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_{k-1}^{k-1}$$

The keys f(0), f(1), f(2) are being generated by cloud. The generalized key is then encrypted using Byte Substitution Encryption Algorithm. When the client sends the download/ retrieval request, the provider asks for the generalized encrypted key.

VI. MODULES

A. Registration & Authentication
It is a module where the login and registration of the users will be provided by the system. Their details will be stored in database or server.

B. File Distribution
In this module, all the files uploaded by the user are been distributed on 3 cloud servers and simultaneously key will be generated from each cloud.

C. Key sharing
It is a mode where unique and generalized key is generated from the system. The key will be encrypted and the key is stored by the server with their respective files allocated to it. This key will be used while retrieving the data again.

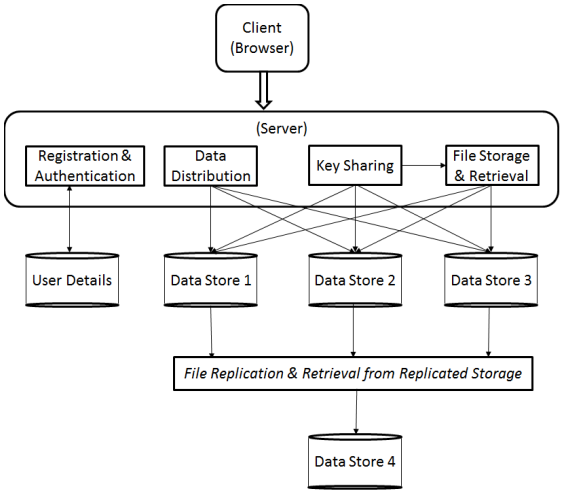
D. File Storage and Retrieval
This module is linked with key authenticating block too as these uploaded files are related to unique keys generated. The user enters the encrypted key and the encrypted key is then decrypted, once it's done they retrieve the required saved data from the different servers.

E. File Replication & Retrieval from Replicated Storage
The distributed files which are stored in 3 different clouds will be replicated/stored on another single server with three different files. The name of the files will be same as the three keys generated from the server.

Further is there is difficulty in retrieving the files from the clouds then the file is searched in the replicated storage cloud with the help of key.

VII. SYSTEM DESIGN

F. System Architecture



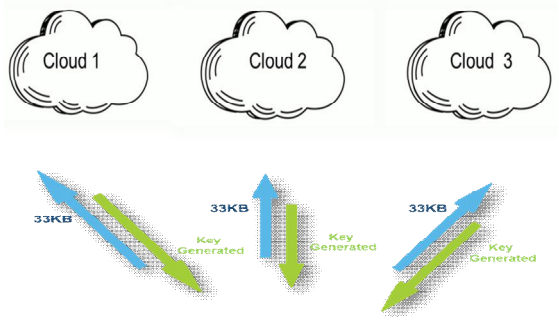
The client initially registers himself/herself by using his credentials into the application for further usage of application. Once after registration is completed then data is need to be uploaded on the servers (3 clouds storage). The data is divided using sequential binary distribution algorithm and the divided data is saved into the clouds byte by byte. Respective keys are being generated from respective clouds and a generalized key is encrypted using byte substitution encryption technique. This encrypted key is then provided to the user/client. For downloading the same data from the servers, the client uses the encrypted key which is decrypted and the three keys are again generated and are being given to clouds and the data is retrieved.

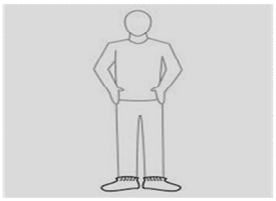
G. Equations

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_{k-1}^{k-1}$$

The above equations provides the key generation expression for different clouds where a_0 is the generalized secret key, a_1, a_2, a_3 … a_{k-1} are random coefficients and k is the number of cloud storages.

H. File Storage and Key Generation

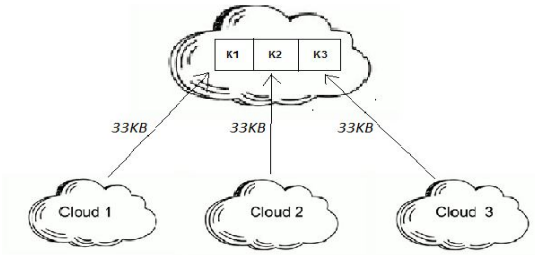




User wants to store 99KB data

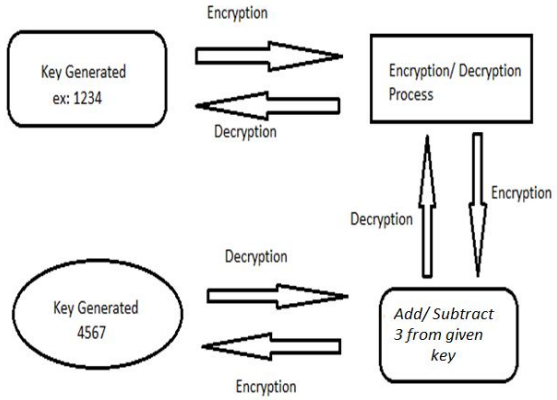
The above pictorial diagram shows the user who wants to upload 99Kb of data and the key provided by cloud after accepting the data. These keys are generalized into a single key which is further passed through encryption process.

I. File Replication



The file distributed on the three clouds is replicated/ copied on another cloud (Replicated Storage) with the same key generated by the cloud. Every time when the data is uploaded or updated, it will follow the same working. Thus enhancing the secure backup of the file.

J. Encryption and Decryption

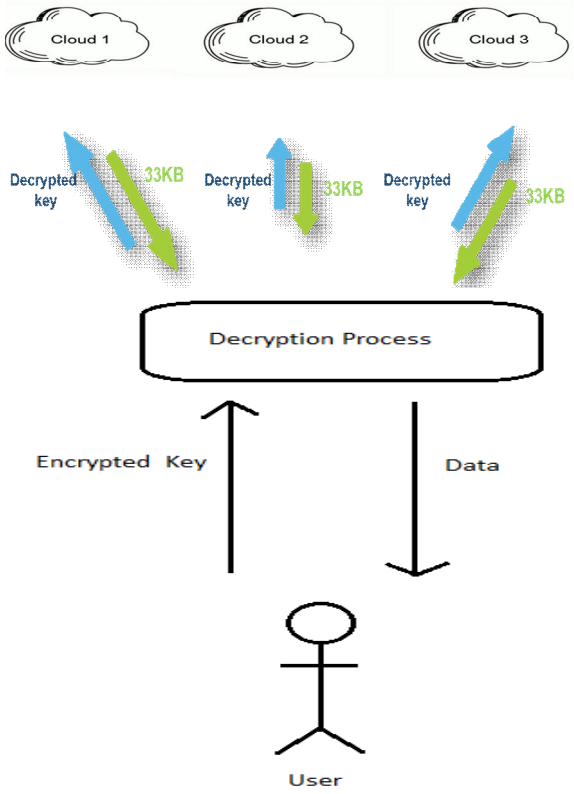


The key is encrypted to enhance further security to data. In this paper we have done the encryption by adding 3 to the current value of each digit of the key. And the decryption process is done vice-versa.

The purpose of adding encryption to the generalized key is just to enhance more security to access the cloud data. The above diagram shows the simple encryption technique whereas in real time implementation we can use higher version of encryption technique used in cryptography.

K. Data Retrieval

i. Ideal Data Retrieval

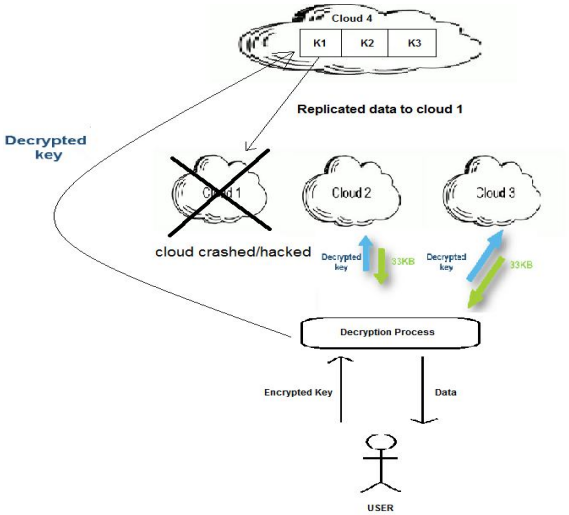


The encrypted key is provided by the user which further decrypts and this decrypted key is provided to the cloud and the data is being retrieved.

ii. Data Retrieval on Cloud Crashed/Hacked

If any cloud crashes or hacked then data is retrieved from the replicated storage cloud, file naming the corresponding key is copied in the respective cloud again. Thus, the user gets to access the file again.

The fig. below demonstrates the working and retrieval of data when the cloud crashes or hacked.



CONCLUSION

It is clear that although the use of cloud computing is rapidly increasing, cloud computing security is still a major issue. Due to this, people or customers prefer storing theor data in multiple clouds or cloud-of-clouds. Thus this paper implements a solution to enhance security in the cloud computing environment with the help of multiple clouds. It also supports the migration to multi-cloud environment due to its ability to decrease security risks that affect the cloud computing user. The method proposed in this system will overcome the securities issues in single clouds well as multi-clouds.

REFERENCES

[1] Mohammed A. AlZain, Eric Pardede , Ben Soh, James A. Thom, “Cloud Computing Security: From Single to Multi-Clouds”, 2012 45th Hawaii International Conference on System Sciences, pp. 5490-5499

[2] Nikhil Shrivastva, Ajay Survase, Poorva Andurkar, Shubhada Bhandare, “Cloud Computing Security using Multiple Cloud”, International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS), Volume 2, Issue 1

[3] Francisco Rocha, Miguel Correia,” Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud”, IEEE 2011, pp. 129-134.

[4] Mukesh Kant, Tripathi Jaypee, “Enhanced Cloud Computing Security with the help of Inter-Clouds”, IEEE transaction on Service Computing, 2012, pp. 122-127

[5] B.Arun, S.K.Prashanth,” Cloud Computing Security Using Secret Sharing Algorithm”, paripex - indian journal of research, March 2013, pp. 93-94.

[6] B.Srinivasulu, S.V.Sridhar, U.Narasimhulu, K.Ramakrishna, “Cloud Computing Security potential for migration from a single cloud to a Multi-Cloud Environment”, International of Advanced Research in Computer Science and Software Engineering Research, Volume 3, Issue 5, May 2013, pp. 919-925 .

[7] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[8] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240

[9] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80

[10] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010

[11] G. Brunette and R. Mogull (eds), "Security guidance for critical areas of focus in cloud computing", Cloud Security Alliance, 2009

[12] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

★★★