Cloud Computing Security using Multiple Clouds

Nikhil Shrivastva[1], Ajay Survase[2], Poorva Andurkar[3], Shubhada Bhandare[4]
[1](Savitribai Phule Pune University, India)

Abstract :- Cloud Computing is a rapidly developing field. A large number of people store their data on clouds. However, for doing this they need to give their sensitive data in the hands of the third party, commonly known as service providers. These third parties cannot be trusted since the complete data is stored in one single cloud. This increases security risks to the user's sensitive data. To overcome these drawbacks based on security of the user's data, a concept of "multi-clouds" was introduced. Multi-clouds are also known as "inter-clouds" or "cloud-of-clouds". Use of multiple clouds or multi-clouds secures the user's sensitive data. The aim of this paper is to secure the user's data by using multiple clouds.

Keywords :- cloud computing, cloud of clouds, multiple clouds, security, sensitive data.

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 un-trusted.[1][8][9] 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.[2] A movement towards "multi-clouds", or in other words, "inter-clouds" or "cloud-of-clouds" has emerged recently.[1][6] 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 [7][10]. This work aims to promote the use of multi-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".[1][3][6]

III. SECURITY RISKS IN CLOUD COMPUTING

Now a days many companies are using the cloud services to store their precious data on the cloud. It includes defense agencies, international research companies. So it all comes to the security. In the single cloud storage all the data is stored at one centralized storage system. So if someone tries to hack the data it is possible that the hacker can get the whole information at a single place. So the single cloud storage is not that reliable. Another chance of losing the data is that if a server gets clash then the user is not able to access his data.[3]

Although cloud service providers can offer benefits to users, security risks are the major problem in the cloud computing environment. User can store the important personal details like credit card and medical record. As the cloud storage is on the internet any problem with the internet security will also affect cloud services.

IV. 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

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

The keys f(0), f(1), f(2) are being generated by cloud.[5] 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.

V. MODULES

Login and Registration :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.

Data Replication : In this module, all the data uploaded by the user are been replicated on 1 or more servers and simultaneously key will be generated from each cloud.

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.

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

VI. SYSTEM DESIGN

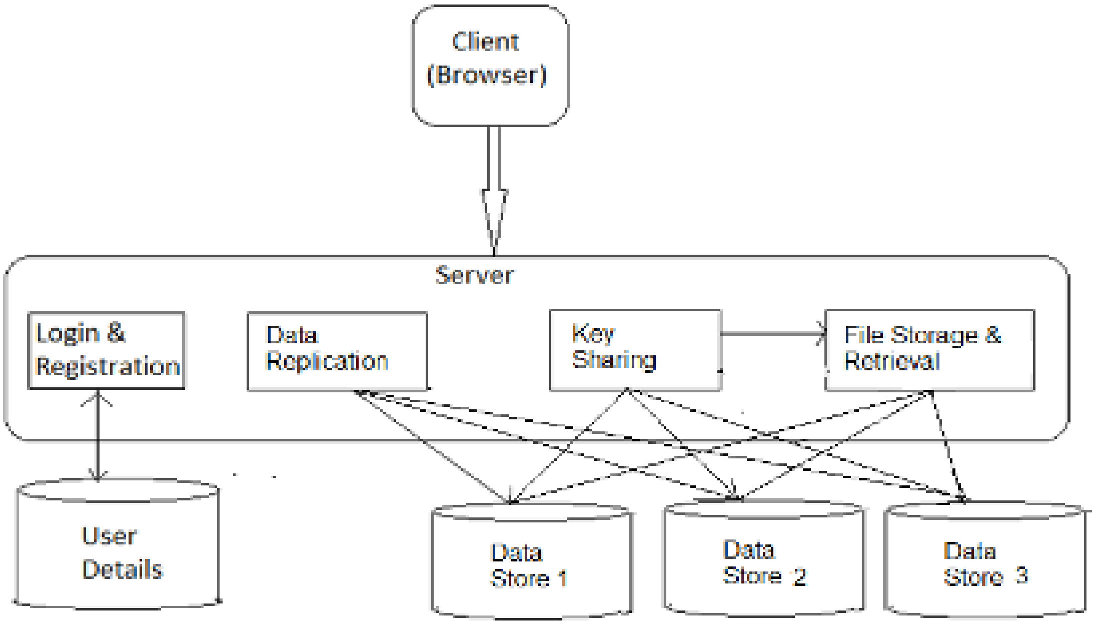


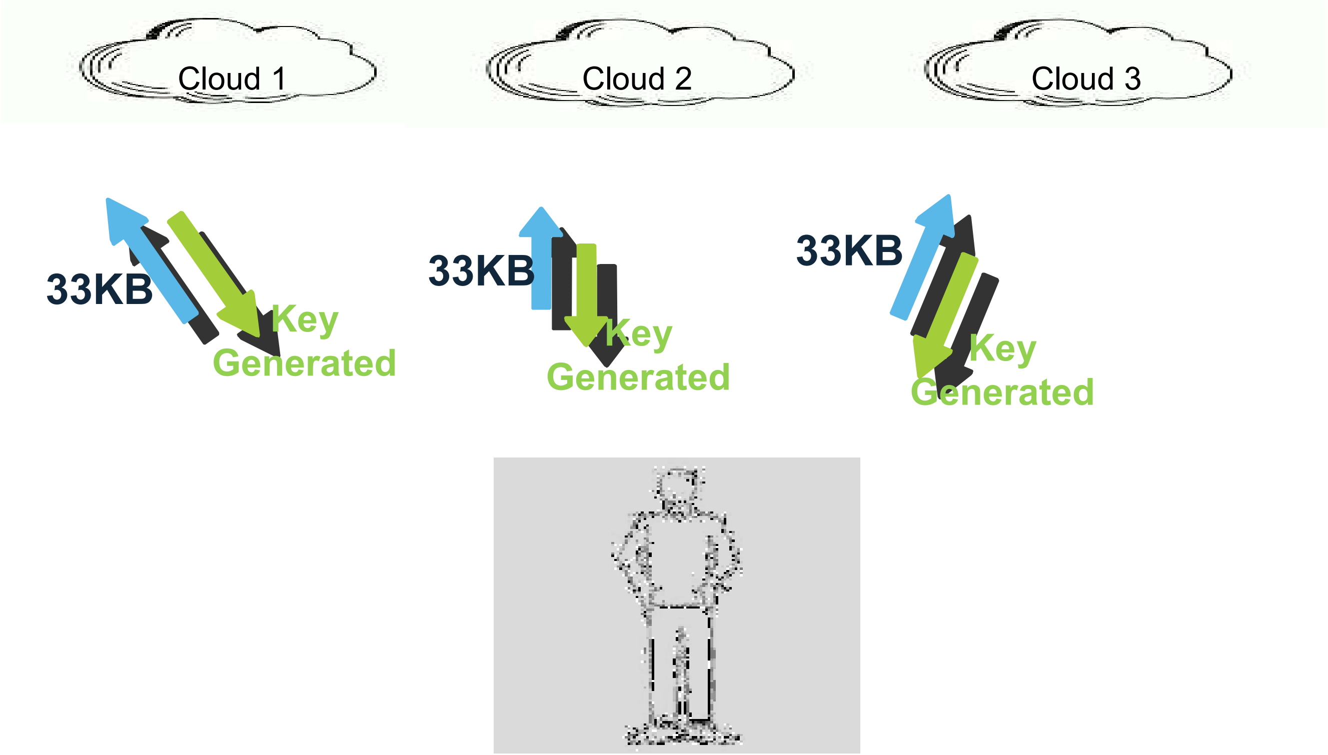
Fig. 1. System Architecture

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.

Equations

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{k-1}{}^{k-1} \qquad (2)$$

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.



User wants to store 99KB data

Fig.2.Data Storage and Key Generation

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.

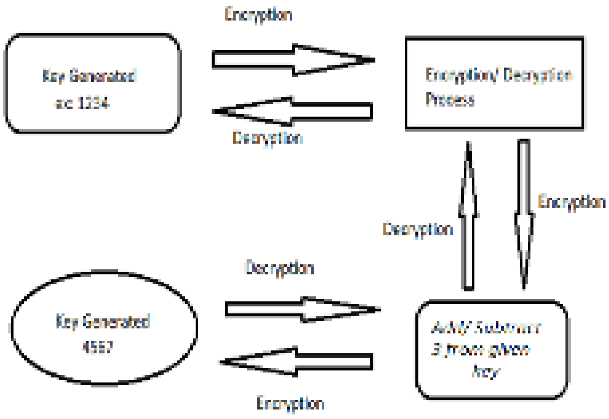


Fig.3: Encryption and Decryption

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.

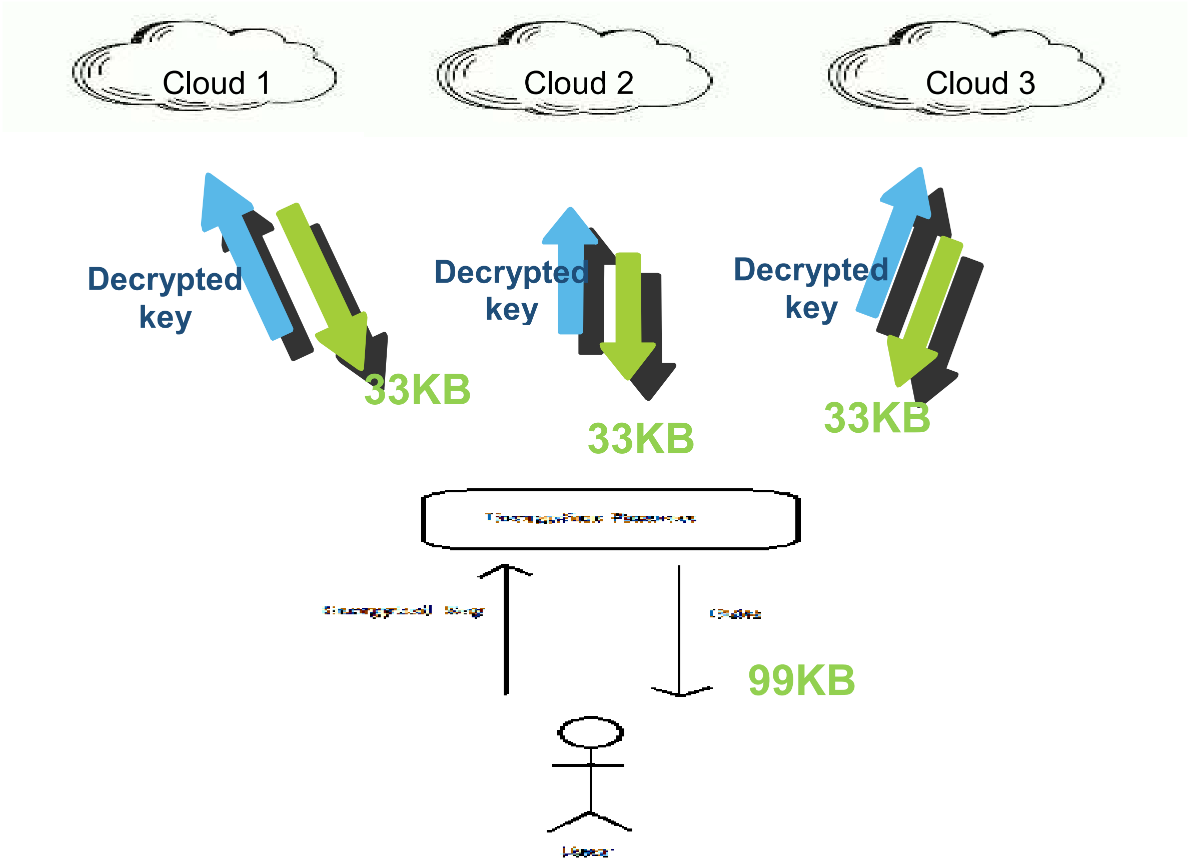


Fig.4. Data Retrieval

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.

VII. CONCLUSION

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. People or Customers do not want to lose their private information or data 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.

The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multiple clouds have received less attention in the area of security. We support the migration to multi-clouds 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 cloud.

VIII. ACKNOWLEDGEMENT

We have been benefited greatly due to sincere efforts from our project guide Mr. S.D. Kale who gave us an opportunity to work on this topic and provided us a guideline and standards for selecting this project and helping us to choose our project topic appropriately.

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

[3] Mukesh Kant,TripathiJaypee, "*Enhanced Cloud Computing Security with the help of Inter-Clouds*", IEEE transaction on Service Computing, 2012, pp. 122-127

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

[5] 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 .

[6] 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.

[7] 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

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

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

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

[11] 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