Enhanced SecurityIn Multicloud Using Visual Cryptography And Secret Sharing

Navya Atmakuri[1], Mihir Mulay[2], Roshan Surana[3], Yash Tibdewal[4]

Department of Information Technology, AISSMS IOTS, Pune

Abstract- *The cloud computing is a modern technology of storing the large chunk of information on the internet and accessing it from anywhere. Dealing with "individual cloud" service providers is anticipated to become infamous with customers due to scare of service availability failure and the possibility of malicious intruders in the individual cloud. A apporach towards "poly-clouds", "interclouds" or "cloud-of-clouds" has come up lately. The proposed work surveys recent research related to single and poly-cloud security and addresses possible solutions. This work aims to promote the use of plyo-clouds due to its capability to nullify security threats that harm the user. In the proposed system we are using architecture to implement the poly-cloud system helps to provide "Confidentiality" as well as "Integrity" along with protection to phishing attacks. Also there is a security mechanism which uses an image based authentication using Visual Cryptography. Once the unique image captcha is displayed to the user it can be used as the password. Using this, website verifies its uniqeness and proves that it is a not fished website put in front of the users.*

Keywords- Interclouds, poly-iclouds, Visual Cryptography, Image based authentication.

I. INTRODUCTION

Proposed approach illustrates cloud computing as "a example for ensuring easy, whenever needed network access to a shared plethora of managable computing assets that can be quickly made available and documented with minimal management struggle or service provider interaction". In area of security, to protect from phishing attacks attribute based schemes are used. But false positive rate of these methods is higher, so we propose new VCS based anti-phishing framework.

II. OVERVIEW OF SYSTEM

The use of cloud computing has taken its toll in many applications. Cloud computing is prolific in terms of low cost and availibility of data. Confirming the secureness of cloud computing is a major factor in the cloud computing, as users often store key information with cloud storage providers, but these providers may be untrusted. Dealing with "individual cloud" service providers is anticipated to become infamous with customers due to scare of service availability failure and the possibility of malicious intruders in the individual cloud. A action towards "poly-clouds", or perhaps, "interclouds" or "cloud-of-clouds" has come up lately. This paper focuses on research related to single and poly-cloud and addresses possible solutions. It is found that the use of poly-cloud providers to sustain security has received less attention from the research community than has the use of single clouds. This work aims to urges the use of poly-clouds due to its ability to reduce security risks that affect the cloud computing user. While assuming a cloud secure, the following aims are to be met:

1) Getting acquainted with the cloud computing lay work at your diposal by the service provider.

2) The cloud computing solution should meet the basic security and privacy requirements of any firm deploying it.

3) Maintain an record of the cloud and data and applications that are present in cloud computing habitat.

4) Data Integrity.

5) Service Availability.

In this system we are uploading the file onto the different public cloud which maintains the integrity confidentiality and security of uploaded files on cloud. We use MD5 algorithm for computing the hash value (digital signature) of files before upload. After that we apply our main algorithm which divides files into different shares and each share contains unreadable text format and that will be uploaded to each cloud. At download time we can choose any of the 3 clouds and that file will be reconstructed. We are implementing this using .net Platform with MS sql server as database.

III. SPECIFICATION OF EXISTING SYSTEM

User able to register and login using our visual cryptography scheme. After login user is able to see his uploaded and downloaded files .User can upload/download files from/on cloud securely. While uploading file, file is divided into number of shares using secret sharing algorithm and each share is uploaded to each cloud. Before dividing the file we generate hash value of file so after downloading of file from we compare these hash value to new computed hash value. if this value is similar then we conclude that file is not corrupted. In download phase, when user click on file to download from cloud. Then he is able to click on checkbox of

cloud option from where he can download the file. Minimum 3 check box must be in checked state to download the original file. So in this way user can reconstruct the file and stored into local desktop system.

IV. SYSTEM ARCHITECTURE

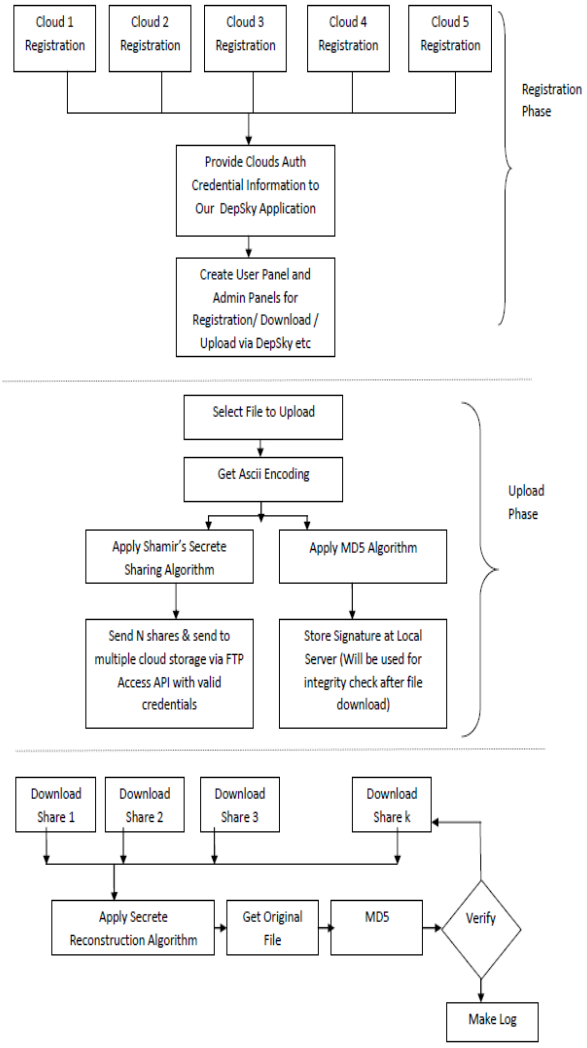

Fig 1: Multicloud Architecture for Data Security

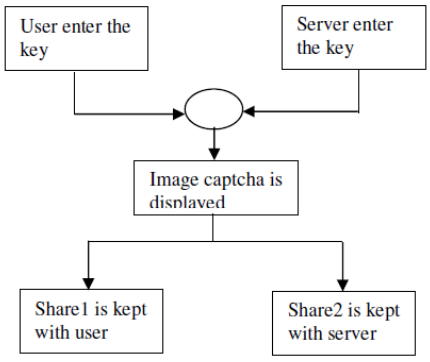

Fig 2: User Registration Process

V. WORKING OF PROPOSED SYSTEM

Step 1:

By using user and server respected key we generate one captcha and divide the share of it which is available with user as well as server.

Step 2:

After that for login process, user need to browse that share and send to server, users share is stacked with the server share and new captcha is generated.

This will detect the phishing site.

Step 3:

Register your cloud with particular space and specification to store your document.

Step 4:

Prepare database with the provided cloud credentials.

Step 5:

Design the GUI where user can is able browse the files which he wants to upload/download from/to cloud.

Registration phase:

In the initial phase, a key sequence (password) is required from the user for the first time for the secure website. The key sequence is allowed to be a match of alphanumeric characters to provide more secure habitat. This sequence is combined with randomly generated sequence in the server and an image is produced. The image is divided into two parts such that one of the part is kept with the user and the other part is kept in the server. The user's part and the original image is sent to the user for later verification during login phase. The image is also stored in the desired backend of any trusted website as secured data. After the process, the user can change the key sequence whenever needed. Registration pahse is depicted in Figure 1.

Login phase:

In this phase initially user is asked for the username. Then the user is prompted to enter his image which is kept on his machine. This image is sent to the websites database where the user's image and image which is stored in the database of the website, for each user, is combined to produce the original image. The image is displayed to the user .Here the user can verify whether the displayed image matches with the image created at the time of registration. The user is suppose to enter the text shown in the image and this can cater the need of password and with this, the end user can successfully log in into the desired website. Using the user id and image generated by combining two shares one can assure whether the website is genuine website or a fake website and can also check whether the user is a human user or not. In this system file is uploaded onto the different public cloud which preserves the integrity, confidentiality and security of

uploaded data on cloud. MD5 algorithm for calculating the digital signature of files before uploading. Later main algorithm which subdivides files into different shares and each share contains unrecognizable text format and that will be uploaded to each cloud. At download time we can select any of the 3 clouds and that file will be reconstructed.

Cloud Controller:

Cloud controller is the application that serves to web application using HTTP Requests and HTTP Responses. Cloud controller divides the data to be saved or updated on cloud into different data blocks using shamir's secret sharing scheme, and provides data to different task managers to store it on different disks. It would increase the availability of data. If user requests any data then, user will generate request to cloud controller through web interface. Cloud controller will request for data to different n task managers, after collecting data from different task managers cloud controller will reconstruct the data from k task managers.

VI. CONCLUSION

It is not a hidden fact that although the use of cloud computing has taken its toll, cloud computing security is still considered the major issue in the cloud computing habitat. Customers cannot afford to lose their personal credential information as a result of malignant intruders in the cloud. Moreover, the loss of service availability has resulted many issues for a large chunk of customers recently. Furthermore, data intrusion leads to many inconvenience for the users of cloud computing. The purpose of this paper is to survey the outcomes on single cloud and poly-clouds to address the security threats and solutions. It has been found that much research has been conducted to make sure that the security of the single cloud and cloud storage whereas poly-clouds have been neglected in the area of security. We are in favor of the migration to multi-clouds due to its capacity to reduce the security threats that hamper the cloud computing user.

REFRENCES

[1] 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.

[2] Kevin D. Bowers,Ari Juels, Alina Oprea,"HAIL: A High-Availability and Integrity Layer for Cloud Storage",2009.

[3] Marko Vukoli_c,"The Byzantine Empire in the Intercloud", IBM Research – Zurich CH-8803 R□uschlikon, Switzerland ,2009.

[4] Seny Kamara , Kristin Lauter ,"Cryptographic Cloud Storage",2012.

[5] Thiyagarajan, P. Venkatesan, V.P. Aghila, G, "Anti-Phishing Technique using Automated Challenge Response Method", 2010.

[6] [Divya James, Mintu Philip," A Novel Anti Phishing framework based on Visual Cryptography", 2014.

[7] Akash Mehra, Emon vuess,"Enhanced Security in Cloud Computing",2014.

[8] Muralidhara B L, Chitty Babu G, "Centralized Admission: A Novel Student-Centric E-Governance Process", International Journal of Computer Applications (0975 – 8887) Volume 66– No.23, March 2013