A Novel Model for Security and Data Access for Jointly Accessing the Cloud Service

Bansi Khimani[1] and **Kuntal Patel**[2]

Submitted in July, 2014; Accepted in December, 2014

Abstract - Cloud computing is a set of resources and services offered by Internet. It provides all kinds of services for end user. One of the most important services provided by cloud computing is an Email (Data Storage and File Sharing). Employees or any Committee of Institution are very interested in sharing documents with group members. There is possibility of creating one group to share information with all. So, in everybody's registered email id, they will get notification for it. Here, everybody have their own mail id. In this research paper, a model is discussed which allow one email id and two users sharing same Email id. This mechanism is like Joint access of single bank account between two members.

Index Terms – Cloud Computing, Cloud services, User Access Control, Joint Access of Cloud data

1.0 INTRODUCTION

Nowadays different state governments and central government have taken initiative to successfully implement E-Governance in various areas of Service applying Information and communication Technology to provide better transparency, Accuracy and Security of its Services to the citizens [9]. The current commercial Systems are aimed mainly at governments and corporations with high security requirements [10].Internet continues to grow and bulk of information is transferred between individuals. Evolution of smart phone and tablets make more usage of cloud services. All these technological developments provide new business model which is known as cloud computing. Main idea behind a cloud is to provide on demand service with high reliability, scalability and availability in distributed environment. Cloud computing entrusts remote services with user's data, software and computation. Thus it is just like using some applications or facilities by not directly installing in devices as we normally do. This system is remote version of remote access [8].

National Institute of Standards and Technology (NIST) defines Cloud computing as:

"Cloud computing is 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.

This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS).There are four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: fast wide-area networks, powerful an inexpensive server computers and high-performance virtualization for commodity hardware."[1]

Cloud service is any resource that is provided over the Internet [2]. According to NIST, a cloud model is composed of three service models – IaaS, PaaS and SaaS.

1.1 Infrastructure as a Service (IaaS)

This is considered as a first layer of Cloud computing. Using this service model, you manage your operating systems, data, applications, middleware and runtime. IaaS allows you to easily scale based on your requirements and you only pay for the resources which you used. This means that extra data processing space is available to you whenever you need it, and when you don't need it then don't pay for it.

1.2 Platform as a Service (PaaS)

This layer provides developer the flexibility to make application on the provider's provided platform. It's fully virtualized platform that includes one or more operating systems, servers and also specific applications. Main features offered by PaaS are flexibility, scalability and database. E.g. Google app engine, Amazon web services s3 etc...

1.3 Software as a Service (SaaS)

This layer delivers single software to multiple clients on demand via web browser over Internet. So, Software as a Service consists of a software running on the provider's cloud infrastructure. E.g. Google docs, salesforce.com etc...

2.0 LITERATURE SURVEY

People use cloud because it provides on-demand services with high reliability, scalability and availability in distributed environment. Here, in this research paper, we start with survey of major cloud providers and Authentication Techniques adopted by various providers. After extensive literature survey related to cloud security, we finally proposed a model related to "Joint Access of Cloud Data" which is explained in this paper.

[1]*R. K. University, School of Computer Science, Bhavnagar Highway, Kasturbadham Road, Rajkot 360020, INDIA.*
[2]*Ahmedabad University, School of Computer Studies, Commerce Six Roads, Ahmedabad 380009, INDIA.*
E-mail: [1]*bansirkhimani@gmail.com and*
[2]*kuntal.patel@ahduni.edu.in*

2.1 Examples of Cloud Service Providers

There are many features of cloud computing. Cloud storage providers like Amazon S3, Microsoft SkyDrive, and DropBox permit consumers to access data online. Second feature is, it provides computation resources for users such as amazon EC2. Third, Google apps or versioning repositories for source code are examples of online collaboration tools.

Cloud service providers should ensure the security of their customer's data and should be responsible if any security risk affects their customers' service infrastructure. [5]Cloud providers must ensure that the information Security Systems they provide are responsive to customer requirements and the data, both primary and secondary, must be preserved as authentic and reliable [11].

- Several vendors with cloud offerings stand to benefit from this trend. Many of these vendors – Amazon, IBM, Microsoft etc. have established cloud products and have been active in this space for number of years.

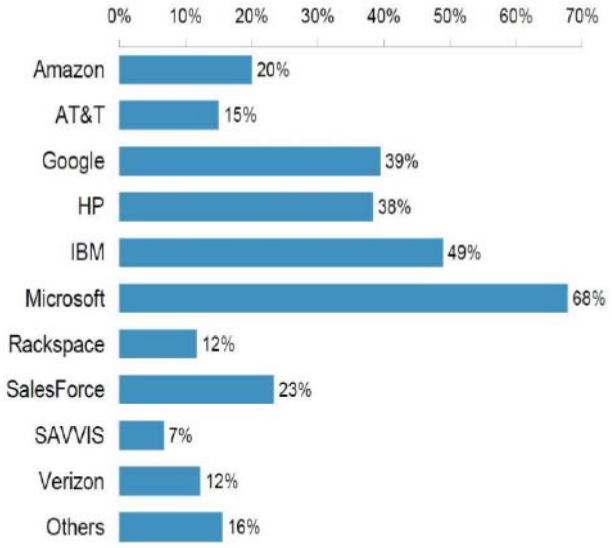

Figure 1: Major Cloud Vendor Used in 2012[6]

From above Figure 1, we can observe that Microsoft is likely to gain most from a broader adoption of the cloud. Of all respondents, 68% of all respondents who expect to move workloads or provision new ones to the cloud environment mention Microsoft as their preferred vendor of choice [6].

Report Published in 2014 says that in Microsoft's Storage – OneDrive, If Privacy is major Concern then it should be noted that Microsoft reserve the right to scan your files to look for what it would deem Objectionable Content. This could be copyrighted Material or things of an explicit nature. Apple has similar policy, making the two potentially more intrusive than their competitors [12].

3.0 TECHNIQUES FOR USER ACCESS CONTROL

3.1 Username and Password

Unique username is provided to user for accessing services. For security purpose, password is a powerful mechanism if you choose your password unhackable. Unhackable password is combination of Alpha-numeric characters, special symbols and difficult to imagine by intruder too. It is also known as one factor authentication.

3.2 Two Factor Authentication

Username and passwords are not enough to secure your online data. Two factor authentications must have feature for any successful and popular service to protect it against password phishing, hacking and account hijacking. [3] There are several solutions i.e. One Time Password (OTP), Authenticator app, SMS and email codes, Security questions, Device recognition etc. which are not costly and secure enough too.

3.3 Biometrics Verification

Biometric Verification enables identification based on "who you are". Every person has distinguishing and measurable physical traits. Personal recognition based on unique physical attributes forms a powerful tool for identity management. Other ways of verifying authorization include "what you have" (a key, a swipe card) and "what you know" (a password, your mother's maiden name).Biometrics is the only mode of authentication that uses "who you are" for verification. [4]

4.0 PROPOSED TECHNIQUE AS "JOINT ACCESS OF CLOUD DATA"

"Ad hoc networking" is popular, which allows device to establish communication, anytime, anywhere without the aid of a central infrastructure [7]. Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and MP3 players, for use in their professional and private lives. For the most part, these devices are used separately i.e. their applications do not interact.

Now imagine, however if they could interact directly. Participants at a meeting could share documents or presentations; all communication could automatically be routed through the wireless corporate campus network [7].So, like sharing documents and all these things if happen via single mail id with separate password mechanism then how much it will be helpful to circulate information between groups of students and participants or user. So, Proposed model follow somewhat same concept i.e With Single Shared Mail ID user can access shared data by their personal password mechanism.

Generally single user has single id and single password to access cloud service. But in proposed model, user id will be single and passwords will be infinite.

Following Simple Steps shows how our proposed model will work to access jointly accessing cloud based data:

Step 1: Input User ID and Password.

Step2: System will compare (by password) about which user want to access cloud data.

Step 3: System will forward Barcode image File to registered email id of Particular user.

Step 4: User will provide correct barcode image file

Step5: System will check that verification of correct barcode

file upload or not?

Step 6: If step 5 is correct then User can access cloud based data otherwise he will perform again from step 1.

Above 5 steps are explained in Figure 2 which shows flow to retrieve data from cloud. Here, multifactor authentication is applied on cloud.

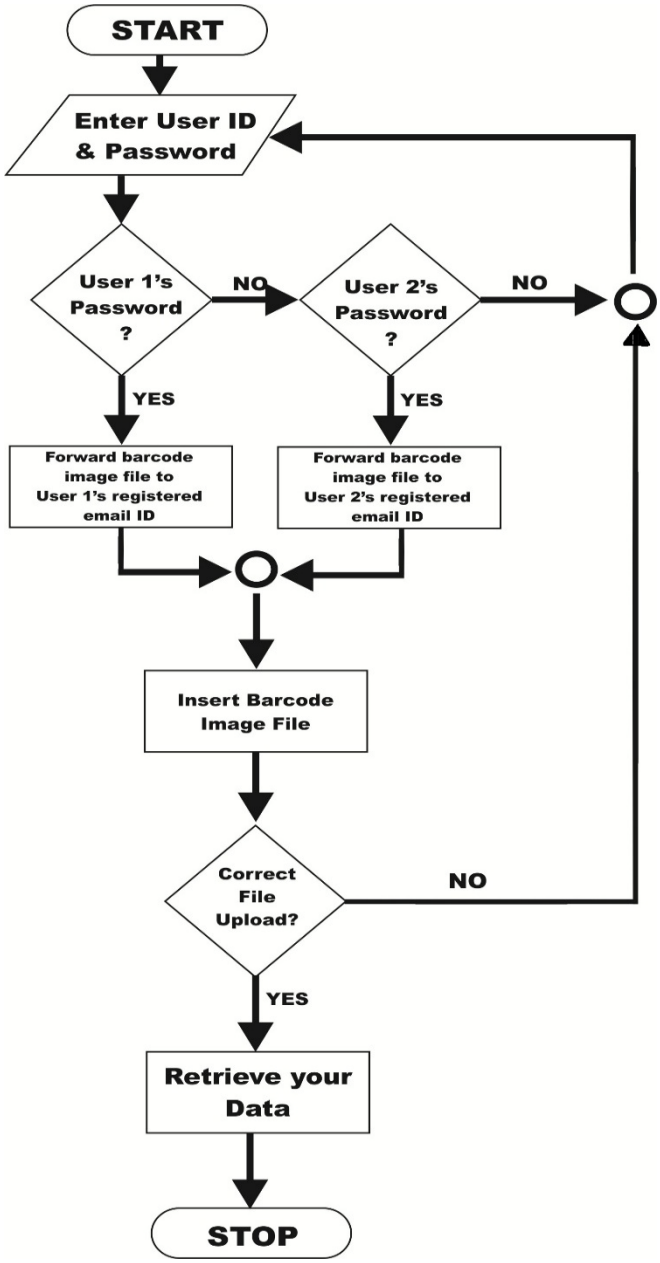

Figure 2:Flowchart of "Joint Access of Cloud Data"

From Figure 2 we can see that, to access any cloud service or data, user needs to enter their Id and Password. In this model, User Id will be shared between multiple users and each user will have their own password. So, when user will enter their user Id and password, web service will check that entered password is of which user. E.g. If Id phd101@exampleuni.ac.in is shared between guide and PhD scholar.

We assume that Guide' password is "guide101" and Ph.D. scholar's Password is "student101". So web service will check that which password is entered by user. If User entered "guide101" then barcode image file will be sent to registered email id of guide. If User entered "student101" then barcode image file will be sent to registered email id of Ph.D. scholar. This registered email id is personal Id of each user. If password is wrong, then web service will assume that user is not valid. So again user will need to enter valid id and password for accessing cloud data.

After accessing barcode image file, user will import that barcode image file (.jpeg) and if that code is valid for that user then that user will access their data. If uploaded file is not valid then user will not be able to access their data.

Sometimes it may happen that "Example University" want to share their Exam schedule between guide and student then they will just mail on jointly access mail id which is phd101@exampleuni.ac.in.

Whenever guide or student needs to access this account they will enter joint id and their own password. If they forget their password then they can request their admin to send reset password link into their registered email id.

4.1 Advantages and Disadvantages of Proposed Model

Advantages

- It is not costly compare to other high security methods.
- This model reduces number of email ids. (I.e. sharing of email id reduces numbers of email ids).
- This model is easy to implement.
- It provides high security then single factor authentication.
- Barcode cannot be altered or predicted by human being. So, if text based security is provided to user then code can be altered by human being intentionally or unintentionally.
- This model is reliable.
- Any organization or person can share data with multiple users having same id and different passwords.

Disadvantages

- Sometimes user may feel bore to upload and download barcode image file.
- Many times users don't like to have same email id.
- Network overhead will be increased compare to Present System of 2 Step Verification.

5.0 CONCLUSION AND FUTURE WORK

In this paper, three main cloud service models are described. Data security is big hurdle in cloud. It is cloud provider's duty to keep user's data safely. This model is helpful to those organizations where single cloud based data need to be shared between multiple users. But, sharing should be securely. These users can be of same field, same region or from same caste or community. Here, multifactor authentication is used to add

second layer of security while sharing data with people.
This model is one of the small steps from our side to enhance cloud security and accessing jointly access of cloud based data. Presently we had proposed this model, but in near future we have plan to test this proposed model on live cloud.

6.0 ACKNOWLEDGEMENT
We would like to thank Mr. Raghu Khimani – Cyber Crime Expert - for their valuable suggestions.

7.0 REFERENCES

[1]. http://www.nist.gov/itl/cloud/ US: Department of Commerce.: viewed on 14-November-2014
[2]. http://searchcloudprovider.techtarget.com/definition/cloud-services/:viewed on 15- November-2014
[3]. http://www.secureauth.com/blog/cloud-storage-2-factor-authentication-review/:viewed on 10-December-2014
[4]. "Benefits of Methode Biometric Verification Technology" Article of "Methode Electronics, Inc."http://www.methode.com/Documents/TechnicalLibrary/Methode_Biometrics_-_Benefits_&_FAQs.pdf viewed on:18-November-2014
[5]. A Mohammed, P Eric, S Ben, T Hanes, "Cloud computing security: From single to Multi – Clouds", 2012 45th Hawaii International Conference on System sciences, pp.5490-5499, 2012
[6]. S Hemalatha, R Manickachezian, "Present and Future of cloud computing: A collaborated survey report", IJITEE, Vol 1, Issue 2, pp. 216-223, July 2012
[7]. H Ashema , "Study of Impact of Mobile Ad – hoc networking and its future Applications", BIJIT – BVICAM's International Journal of Information Technology , Vol 4, Issue 7, pp. 439- 444, January – June 2011
[8]. R Vaibhav, "Innovative Use of cloud computing in Smart Phone Technology", BIJIT – BVICAM's International Journal of Information Technology, Vol 5 No 2, pp. 640-648
[9]. S Sirsendu , K Sunil, "Applications of Public Key Watermarking for Authentication of Job-Card in MGNREGA", BIJIT – BVICAM's International Journal of Information Technology, Vol 4 No 1, pp. 435 – 438 , January – June 2012
[10]. S Dilbag, S Ajit , " An Effective Technique for Data Security in Modern Cryptosystem" , BIJIT – BVICAM's International Journal of Information Technology, Vol 2 No 1, pp. 189- 194, January – June 2010
[11]. D Meenu, D Mikku, Y.S.Shishodia, "Cloud Computing and Knowledge Management as a Service: A Collaborative Approch to Harness and Manage the Plethora of Knowledge", BIJIT – BVICAM's International Journal of Information Technology, Vol 5 No2, pp. 619-622, July – December 2013.
[12]. http://www.pcadvisor.co.uk/features/internet/3506734/best-cloud-storage-dropbox-google-drive-onedrive-icloud/: visited on 15/02/2015