International Journal of Scientific Research in Computer Science and Engineering
Research Paper Vol-1, Issue-3 E-ISSN: 2320-7639

An Improved Authentication Technique with OTP in Cloud Computing

Vishal Paranjape [#1], Vimmi Pandey[2]

[#2]Department of Information Technology, Gyan Ganga College of Technology Jabalpur, M.P., India
[2]Department of Information Technology, Gyan Ganga College of Technology Jabalpur,M.P., India

Available online at: www.isroset.org

Received: 08 May 2013 Revised: 16 May 2013 Accepted: 24 June 2013 Published: 30 June 2013

***Abstract*—** Today data security plays an important role in the field of software and quality of service, Cloud computing focuses a new challenging security threats. Therefore, a data security model must solve the most challenges of cloud computing security. Cloud computing is a capable technology to make easy development of large-scale, on-demand, flexible computing infrastructures. The concept of cloud computing has changed the view of infrastructure architectures, software delivery and development models. Cloud computing incorporates elements from grid computing, utility computing and autonomic computing to an innovative deployment architecture. This paper presents an overview and the study of the cloud computing. Also include the several security and challenging issues, emerging application and the future trends of cloud computing. To overcome this I use the concept of Mobile OTP for providing authentication, whose purpose is to ensure security in cloud environment.

Keywords- *Cloud computing security, Authentication, OTP, Dynamic Password, Time Synchronization, Information and communication security, Trust.*

I. INTRODUCTION

Cloud computing is the communal term for a group of IT technologies which in teamwork are changing the landscape of how IT services are provided, accessed and paid for. Some of the supporting technologies have already been available for quite some time, but it is the combination of several technologies which enables a whole new way of using IT. 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, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The concept of Cloud Computing revolves around distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud platforms are offered by the Cloud service providers (CSP's) for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers[1].The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs.. There are also four different cloud deployment models namely.

1) Private cloud. The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.
2) Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns. It may be managed by the organizations or a third party, and may exist on premise or off premise.
3) Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
4) Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public).

BARRIERS TO CLOUD COMPUTING

1. Privacy and Security.
2. Performance, Latency and Reliability
3. Portability and Interoperability

II. METHODOLOGY

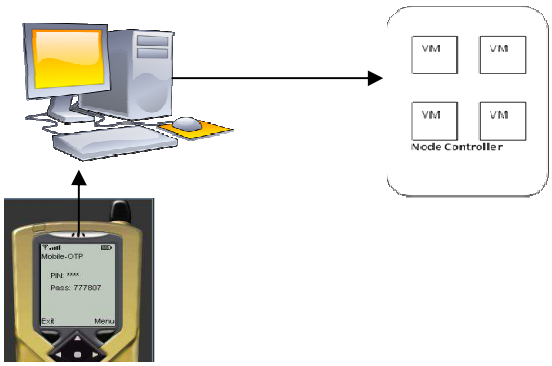
Proposed Working Model

The model which I propose in the present scenario works like this :

i) The user logs in to the system using Mobile OTP.

ii) The OTP algorithm simultaneously executes the code at mobile as well as Server I.

Corresponding Author: *Vishal Paranjape*



One Time Passwords

A onetime password (OTP) is just what the names implies, a password that is only valid for one login. The benefit of OTPs is that it offers much higher security than static passwords, in expense of user friendliness and configuration issues. OTPs is immune against password sniffing attacks, if an attacker use software to collect your data traffic, video records you when you type on your keyboard, or use social engineering, it doesn't matter since the password that the attacker gets hold on will not be valid to use. [2] A OTP can be generated using different methods [2][3], and is often used in conjunction with a device that is synchronized with an authentication server:

Time-Based OTPs In the time-based method, a device with an internal clock generates passwords that are depending on the current time. For example, every minute a new password is generated in the device, and the same password is generated at the authentication server. When the user wants to login to a service or system, the current OTP that is displayed on the device is used .

III. PROPOSED SECURITY SOLUTION

Authentication solutions The previous chapter mentioned the problems with static passwords and also other problems associated with different cloud providers' security solutions, and how it can't be used satisfactory in a cloud environment. There are ways to have a secure and easy-to-use cloud service that can satisfy these criteria's:

1. Provide better password solution for login procedures than the insecure method of static passwords.
2. Provide better two-factor OTP authentication solution than those discussed in the previous chapter.
3. Have an easy-to-understand registration system, which at the same time doesn't compromise the security.
4. Use an encryption algorithm that is secure but also fast, to be able to serve the vast amount of cloud users.
5. Offer a solution that is free of charge in order to attract more customers to the cloud services.
6. In overall, the security solution for cloud services must be easy to use, but also be very secure in order to protect the customers' data and gain the trust of the customers.

Proposal – Authentication with m OTP: The authentication method used is two-factor authentication with a one-time password, based on [4] and [5,6,7,8] but with modifications. The user's mobile phone will work as the authentication device, in which the user have to enter a 4-digit PIN code to generate an OTP that can be used for login. This is done by a Java-application running on the phone. The OTP that is generated on the mobile phone is based on three components which will be hashed together with MD5:

1. 4-digit PIN code that the user enter.
2. A secret random number that was created during device-initialization (Init-secret) that only exists on the user's mobile device.
3. The current time

IV. EXPERIMENTAL SETUP & RESULTS

The results obtained and the experimental setup of implementation of two factor authentication using the concept of Mobile OTP to access the private cloud.

Cloud Server Installation

(i) Server

(a) Hardware Configuration

Intel® Core™2 Duo processor

4 GBHard Disk

4 GB RAM

(b) Operating System : Ubuntu 11.04

(c) Software Recommended

1. Lamp Server (Linux, Apache, MySQL Server, PHP)
2. CURL
3. Kaazing Gateway
4. ActiveMQ Daemon

(ii) Step by Step Installation of Own Cloud

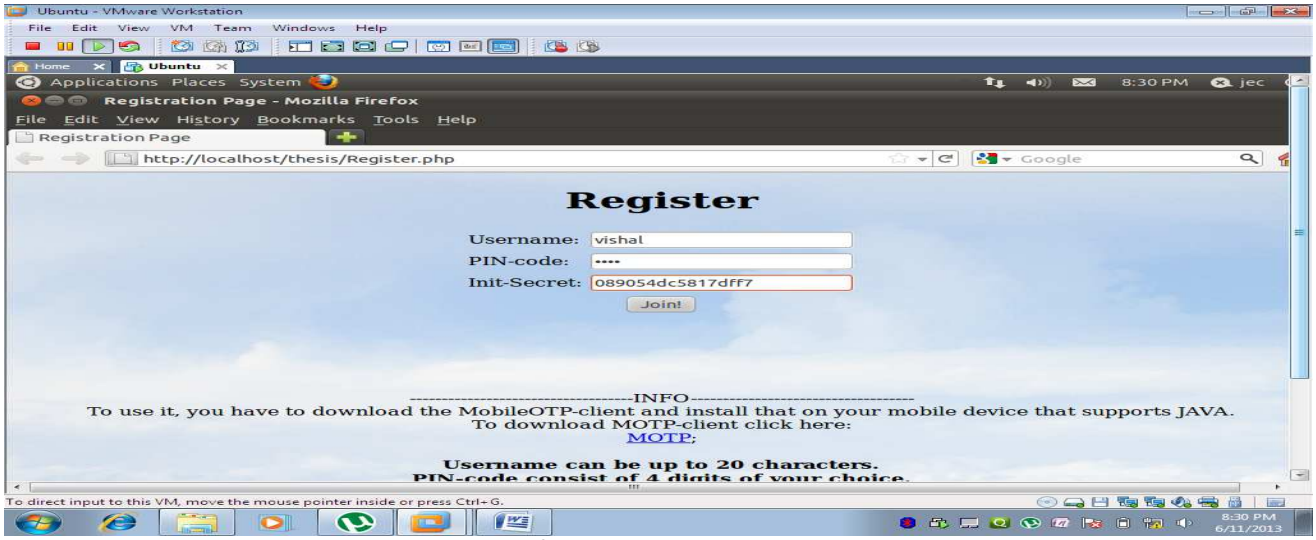
(iii) LAMP Server is a collection of open source software used to create a web server. The collection consists of Linux – the operating system , Apache server – the server, MySQL – the database system , PHP – the programming language

(iv) Mobile Specification: Text Field-input for compatibility with modern touch screen and QWERTY smart phones (down to the simplest J2ME capable phones like the Nokia 6210) usage.

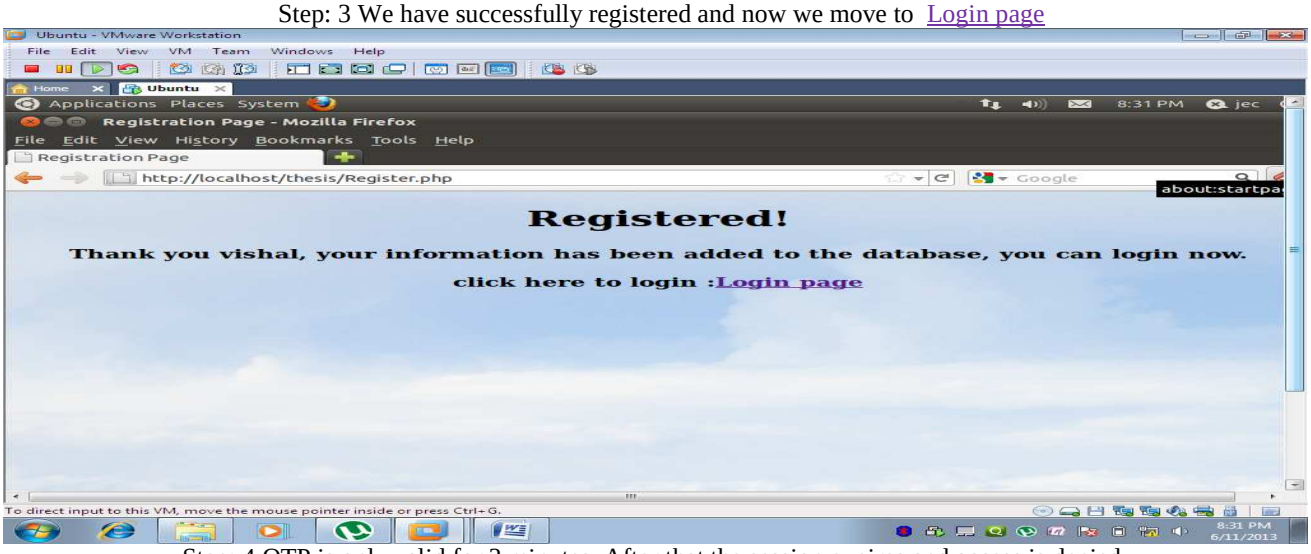
	
We get the Init-Secret on our mobile which we feed in the Registration Page.	On the basis of PIN chosen in the Registration Page we put the password being generated by OTP into Login Page.

	
To get the Init Secret we enter PIN as 0000	To get the Init-Secret, press 0000 in Mobile OTP. Then press 25 random numbers. Write down the 16-digit secret in the Init-Secret field.

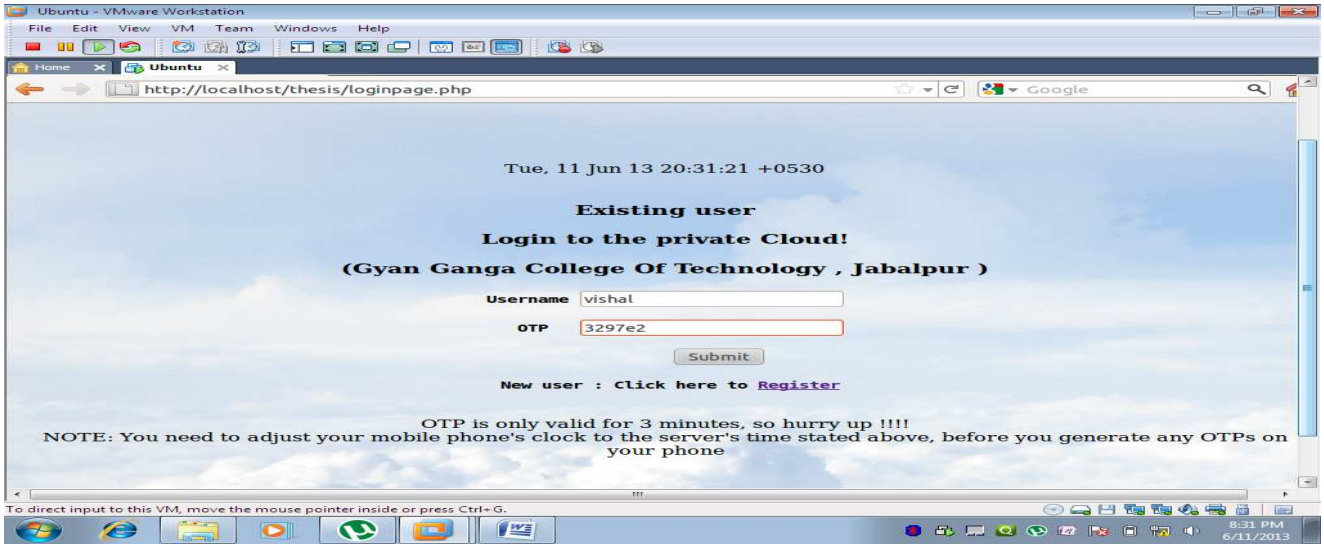
STEP: 2 NOW WE PUT THE INIT-SECRET IN THE REGISTER PAGE AND JOIN.



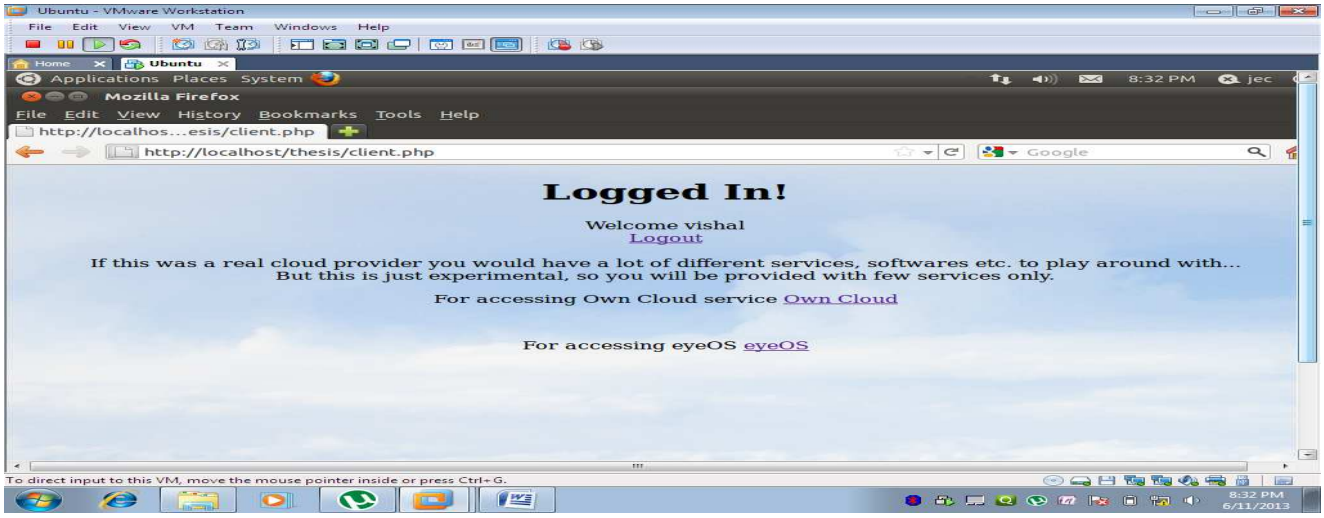
Step: 3 We have successfully registered and now we move to Login page



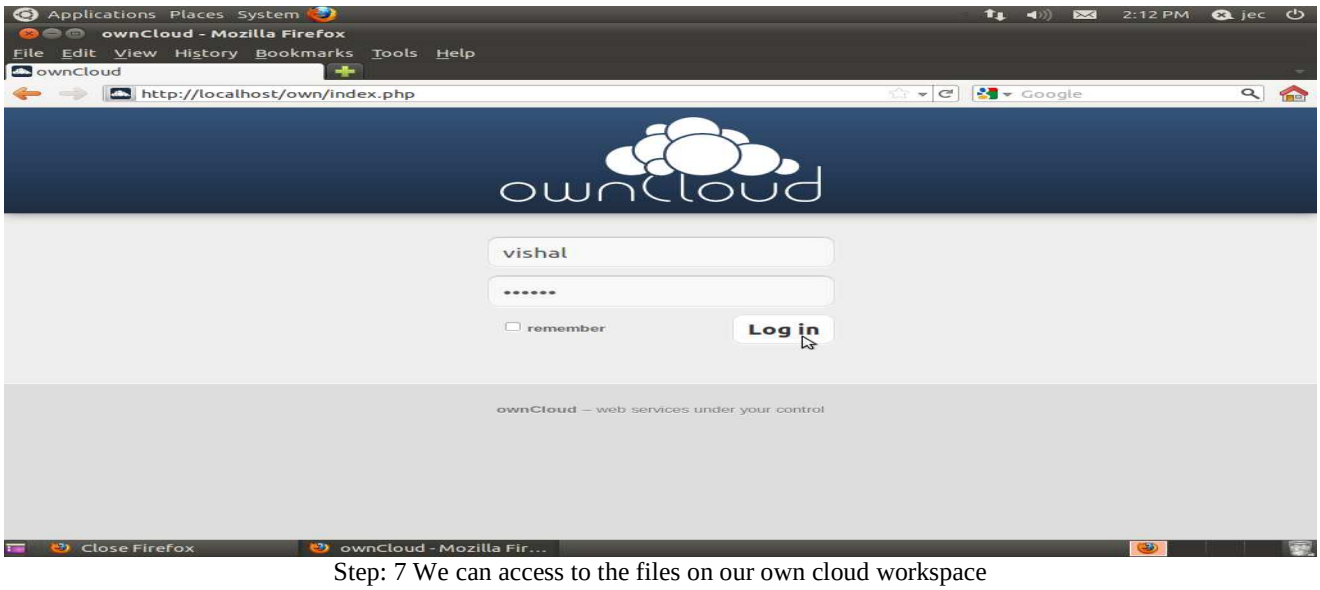
Step: 4 OTP is only valid for 3 minutes. After that the session expires and access is denied.



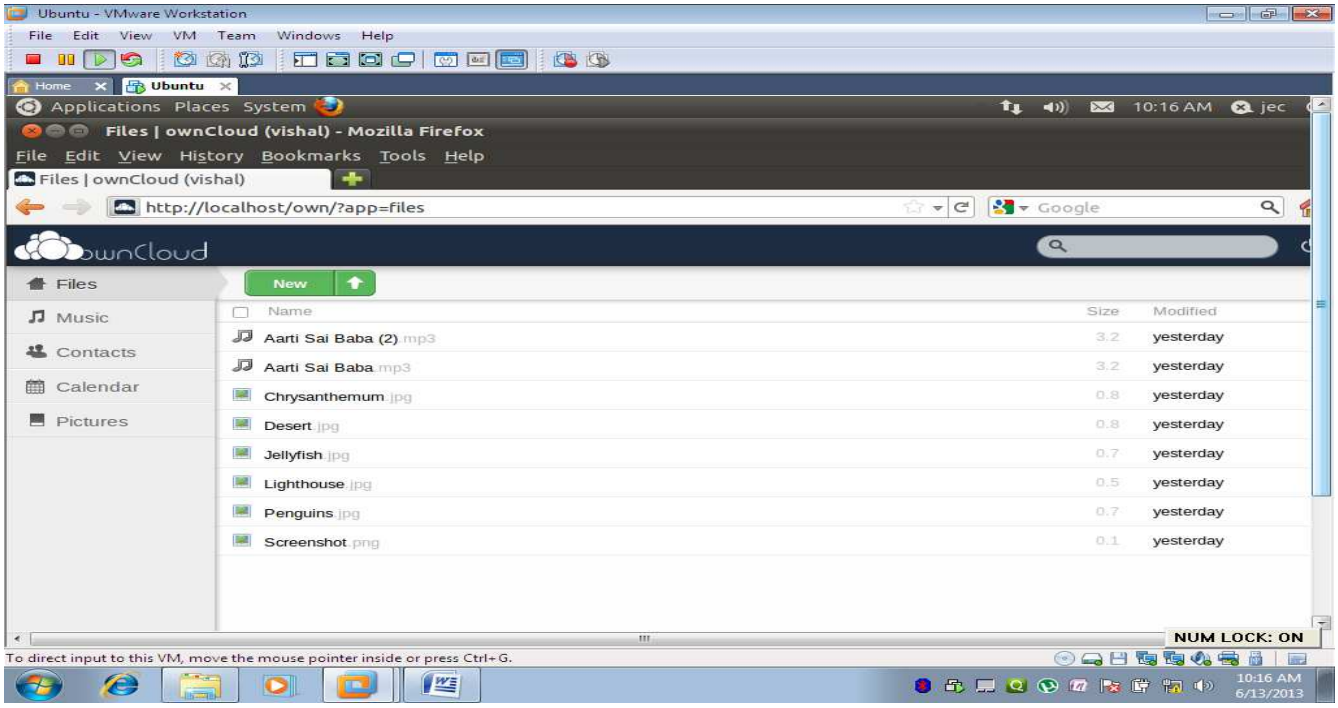
Step: 5 Now we access our Own Cloud Workspace by navigating Own Cloud



Step: 6 Now we can access to our Own Cloud by Log in with Uname & Password



Step: 7 We can access to the files on our own cloud workspace



V. CONCLUSION & SUGGESTION FOR FUTURE WORK

Inevitably cloud computing will support a surplus of information systems as the benefits outnumber its shortcomings. Cloud computing offers deployment architecture, with the ability to address vulnerabilities recognized in traditional IS but its dynamic characteristics are able to deter the effectiveness of traditional countermeasures. In this thesis we have identified generic design principles of a cloud environment which stem from the necessity to control relevant vulnerabilities and threats. To do so, software engineering and information systems design approaches were adopted. Security in a cloud environment requires a systemic point of view, from which security will be constructed on trust, mitigating protection to a trusted third party. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh through federations, within which essential trust is maintained.

REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009).

[3] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[4] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.

[5] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[6] Shivlal Mewada, Umesh Kumar Singh and Pradeep Kumar Sharma, " A Novel Security Based Model for Wireless Mesh Networks", ISROSET- IJSRNSC, Vol-1, Issue-1, pp(11-15), March-April 2013.

[7] Shivlal Mewada, Umesh Kumar Singh, Pradeep Sharma,"Security Based Model for Cloud Computing", Int. Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1, pp (13-19), December 2011.

[8] Rajesh Piplode, et al. , "Study of Threats, Risk and Challenges in Cloud Computing", IJSRCSE Vol-1, issue-1 pp (26-30) Jan- Feb 2013

