# Implementation of Multilevel Authentication Scheme for Multicloud Environment

Ms. Priya D. Thorwat,
Mtech Student (CSE),
Sahyadri College of Engineering & Management

Mr. Sudheer Shetty
Head of the Department of CSE, SCEM
'Sahyadri Campus' Adyar, Mangalore, India

## ABSTRACT
At present cloud computing is a technology which is needed the most for IT industries. Usually service provider is the one who offers services in terms of software, platform and infrastructure on the pay per usage to the end user. Characteristics of cloud computing makes the cloud of an organization to meet all the requirements of an end user. These days organizations prefer to migrate from single cloud environment to multicloud environment. Multicloud reduces security issues in cloud computing and decreases its affect to the cloud user. One of the security issues in multicloud environment is an authentication. This system is designed for a user or client to be authenticated at multiple levels while accessing services from the multicloud environment. Primary step to manage the cloud is by giving username and passwords. But sometimes passwords get hacked so in order to give security one time passwords are generated at. In this paper we have combined one time passwords with session passwords including security at the hardware level. Therefore every time while accessing confidential data from multicloud environment client is authenticated at all three levels by providing the security at the highest level. In this paper multilevel authentication is implemented for the device called as an android mini-PC and strongest authentication is ensured.

## Keywords
One time password, authentication at session level, authentication at hardware level, multilevel authentication, and multicloud environment.

## 1. INTRODUCTION
Cloud computing is obtaining its acceptance in IT market with an elastic, flexible and variable cost way to deploy service platforms using various outsource resources. When we move from single to multicloud the need for governance becomes apparent. We have less hardware , and a scalable infrastructure, falling prices and availability guarantee of services all these things makes cloud computing very difficult to ignore. There is a record of thirty million data security software shipments where clients are assured that security expertise will allow users to confidentially store their personal encrypted data in a cloud with little risk. Now days it is very common to register with multiple service providers. With many username & passwords it is hectic to manage all the accounts. To integrate various resources from multiple clouds infrastructure as a service is provided by multicloud environments. The objective of this multicloud environment is to provide security in terms of data integrity, data intrusion, and service availability and to increase performance and cost reduction[11]. This multicloud is advantageous in case of fault tolerance, availability guarantee of services, performance capability and price. In this system whenever client accesses any data from multicloud environment he is authenticated at three levels of authentication. Security can be provided by giving username and passwords but these alone are not sufficient. Therefore one time passwords (OTP)are generated on to the users mobile. Then session password is generated at the second level which is unique only for that particular session. At the last level this session password is encrypted using motherboard number of an android mini-PC to verify the hardware used by a client.

### 1.1. Android Mini-PC
One of the important factors for personal computing revolution is size. There is transformation that has taken place from desktop powerhouses into devices which are small enough to fit in our pocket. Inexpensive android mini-PC is a dual core running android 4.1 with inbuilt Wi-Fi and Bluetooth. This device requires two extension adopters one for USB and another for HDMI. You can directly pug this device into T.V or monitor with HDMI port. This device is booted directly to the home screen within a minute. Immediately it allows user to upload and download files when it is connected to Wi-Fi and works well with its compatible keyboard.

## 2. RELATED WORK
Richa and Satyakshma have prepared the design of OTP in multi Cloud Environment. They have proposed the working mechanism of OTP in multi cloud. But in their paper implementation of OTP for multicloud environment is still under research [1].

S.Balaji and Lakshmi.A have proposed authentication techniques for engendering session passwords. In this paper pair-based authentication scheme, hybrid textual authentication scheme and draw-a-secret scheme is implemented for generating session passwords [3].

Dinesha H A and Agrawal V K have proposed a technique for multilevel authentication for accessing services from a cloud. But multilevel authentication for multicloud environment still does not exist [6].

## 3. PROJECT WORK
The main objective of this system is to provide the security at multiple levels of authentication for android mini PC that is
First Level-One Time Password (OTP)
Second Level-Authentication at Session Level (AaSL)
Third Level-Authentication at Hardware Level (AaHL)
for accessing services from the multicloud environment using android mini PC and making the system more secure and dynamic. In this system we have implemented OTP for multicloud environment. Later OTP is combined with the next level of authentication that is session level. After generating session passwords generated session passwords are encrypted and decrypted at the client's android mini-PC. While exchanging the key motherboard number of an android mini-PC is fetched internally and used as a secret key for encrypting the session password. Once the authentication at the last level that is hardware level is successful then client is able to access any services from multicloud environment.

## 3.1. Architecture of the System

The proposed system architecture is given in fig.1 which makes use of three levels of authentication. Multicloud is deployed on servermachine.

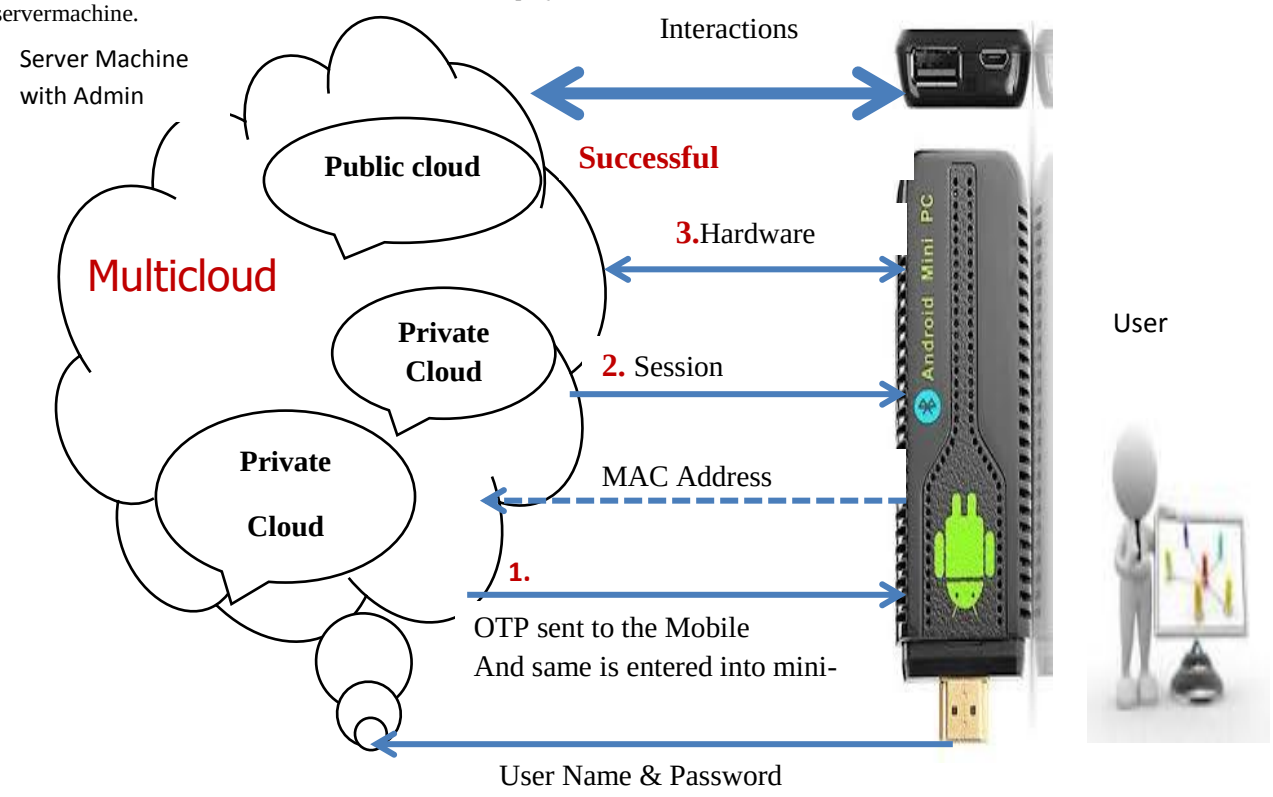


**Fig.1. The architecture of the system**

From the above figure Fig.1. multicloud environment is created on a server machine for the project demonstration and code is written using JDK and Netbeans in eucalyptus. First a private cloud is created using centos 6.3 operating system which provides platform for community enterprise cloud eucalyptus. We have selected eucalyptus for building a private cloud because it is having inbuilt components like node controller, storage controller, cluster controller and cloud controller into a single virtual cloud box. Once the private cloud is built connectify software is installed on another machine. Connectify software is used to share an internet connection with android devices. This Connectify software acts as a router for accessing private cloud through public cloud that is cloud of cloud is multicloud. Now user on the android mini-PC accesses the private cloud through connectify through public cloud. But before accessing all the data from multicloud environment client is authenticated at three levels. User will enter his user name and password. Then OTP is generated and sent it to the mobile. User will enter this OTP into GUI provided on mini-PC. When he clicks on submit MAC address of mini-PC is fetched internally and sent back to the cloud. Next the session password is generated using colors and text. By giving priority to colors a unique password is generated and session password is verified with the entered session password during registration. This session password is encrypted at private cloud using MAC as a secret key for algorithm. Then decrypted successfully only if it matches with the stored MAC address. After the successful authentication at hardware level now user can access all the stored services. He can upload or download files as needed and can create virtual machines and instances as required and can also have an access to the private cloud eucalyptus.

## 3.2 Sequence Diagrams

This section gives the details of admin and user modules.

In the figure Fig. 2. User has to register all his details like username, mobile number etc. All this details are stored in a database created in a private cloud eucalyptus. After Registering user will get the confirmation of registration by database. Admin is responsible for creating all the accounts in the eucalyptus and confirmation mail is sent to the user regarding creation of an account. In the figure Fig.3. Shows the details of a user module. In this section user logs in into the server with all his details. After the successful login user gets the OTP which is generated by the server. User has to enter the session password which he had entered during registration if both the password matches then authentication at session level is successful. Now once the session password is generated. Server uses the stored motherboard number to encrypt the session password .This encrypted session password is sent to the android mini-PC. Now using MAC address of android mini-PC, this session password is decrypted and hardware is verified across the user device android mini-PC. After all three levels of authentication user will get the confirmation from private cloud therefore user can interact successfully with the server in which multicloud environment is created.If the motherboard number does not match with the stored MAC address the authentication at hardware level fails. Even though user gets OTP it is very difficult to cross the second level. Combining all three levels into one system gives a strongest authentication mechanism for accessing services from multicloud.

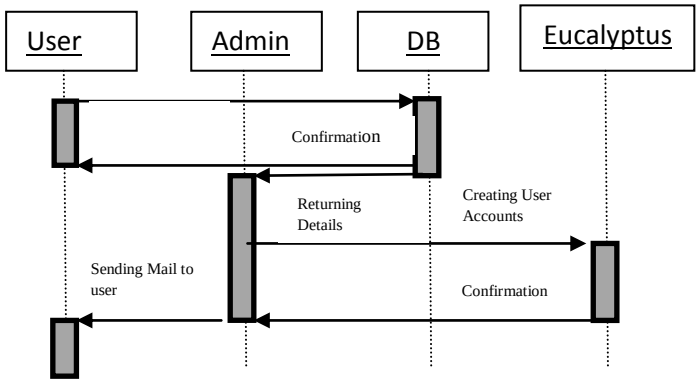


**Fig.2. sequence Diagram for Admin**

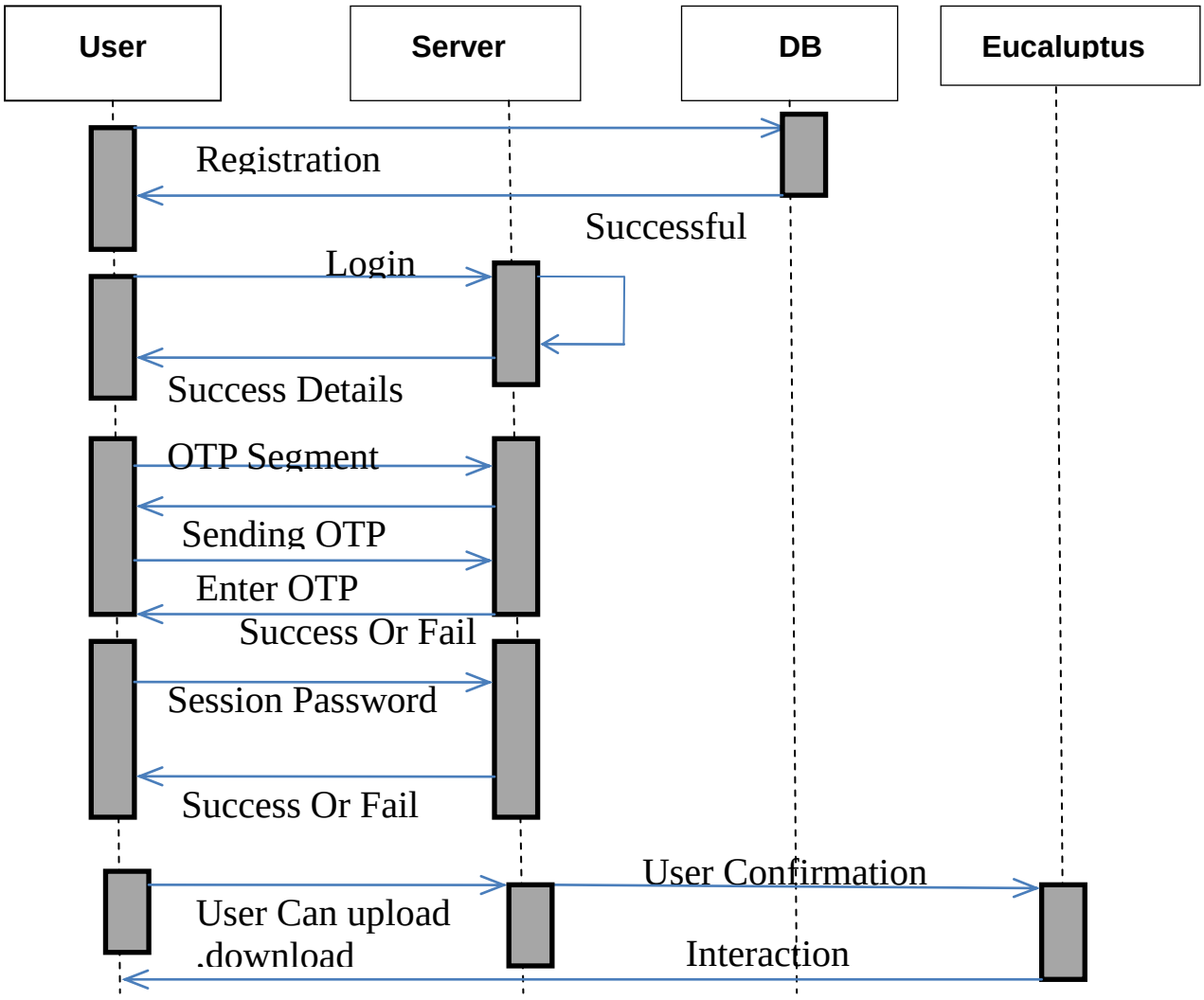


**Fig.3 Sequence Diagram for User**

# 4. IMPLEMENTATION DETAILS

User has to connect his android mini PC to a monitor which is having HDMI port. A PC with connectify software installed must be active to share the WI-FI connection with android mini pc. Private cloud is already built using Eucalyptus on another machine.

Step 1: User has to login with his details and fill the form by selecting images. User will get OTP on his mobile. Now he has to type the password in the text field. If password matches then authentication at first level is successful. Output form is given below in fig.5.

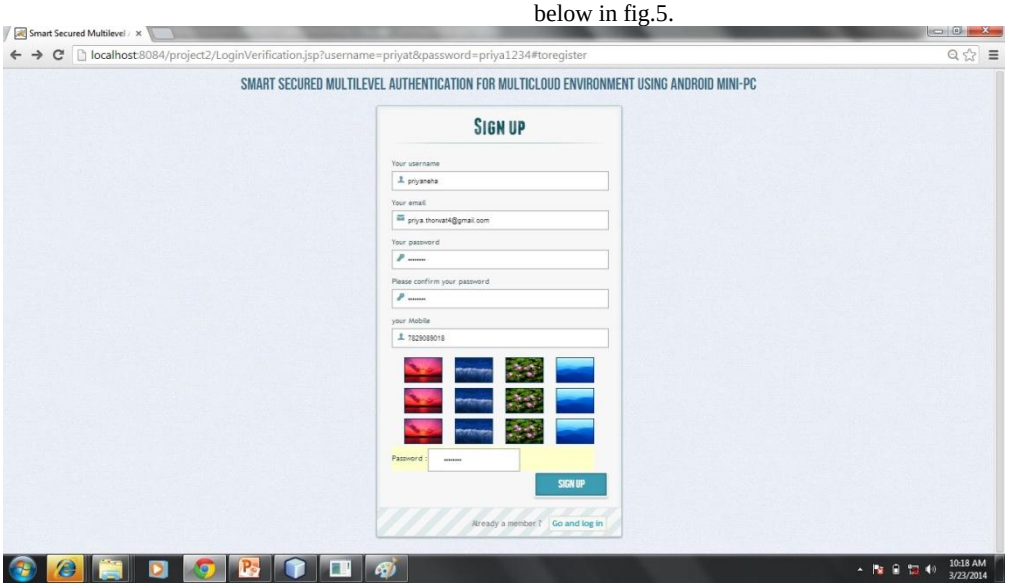


**Fig.4 Registration Form for the User**

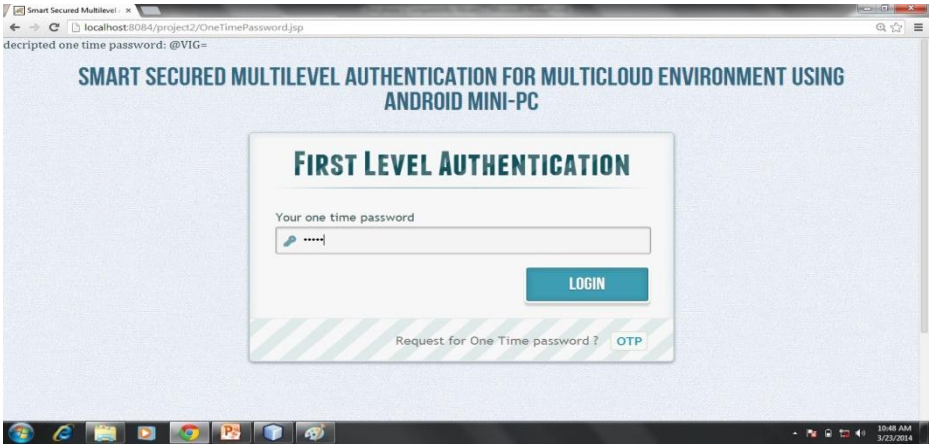


**Fig.5 First Level of Authentication**

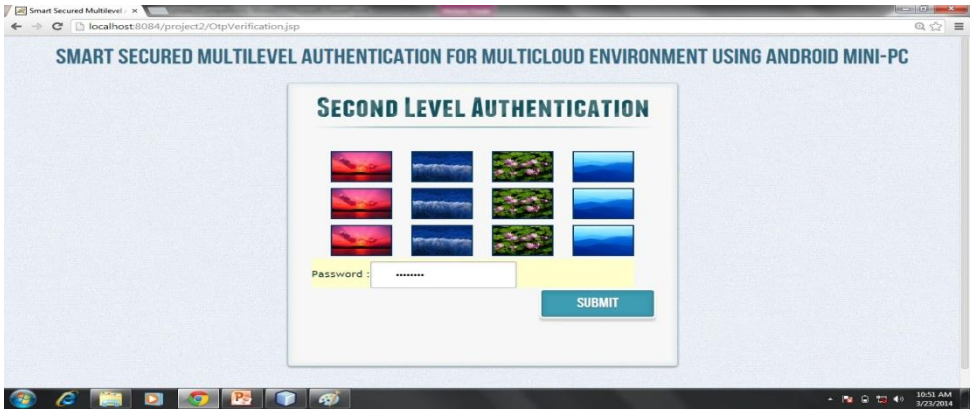


**Fig.6 Second Level of Authentication**

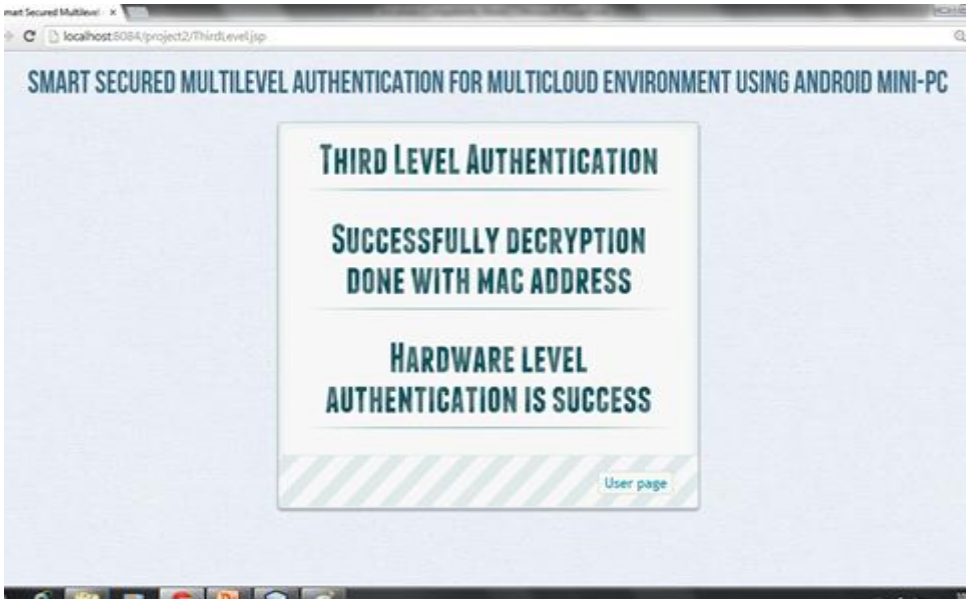


**Fig.7 Third Level of Authentication**


**Fig.8 User Can Upload,Download,Access Eucalyptus and Log Out**

Step 2: It is necessary for a user to select the same images as in he had selected in login form. Therefore session password is generated. At last after clicking on submit if entered session password is correct then authentication at second level is successful. As shown in the above Fig. 6.

Step 3: The session password in the step 2 is encrypted with motherboard number and if user is using the same android device then authentication at third level is successful after decryption. As in the Fig. 7.

Step 4: After all three levels of the authentication user or client can access any confidential data stored in private cloud through public cloud. He can upload the files in private cloud. Also he can download any required file from private cloud. User can access the data from private cloud through public cloud using a router as connectify software installed in a computer. As shown in the Fig.8

## 5. CONCLUSION

There are many drawbacks with the textual passwords therefore session password and OTP are combined together to provide more security. Then the session password is encrypted using MAC address to give security at the hardware level.One of the advantage of this system is that employees in a organization can have their own android mini PC and authentication for this mini PC can be provided at all three levels. As this android mini PC is portable with quad processor client can carry this device which fits in his pocket. The performance of android mini PC is far more better than the normal PC. If client wants to access any confidential data from the organization which is making use of multicloud environment then client is authenticated at multiple levels of authentication as described. In this paper highest level of the security is provided for authentication for accessing the data from the multicloud environment. After the successful authentication various services like IaaS, PaaS, and PaaS are accessed from the multi-cloud environment.

## 6. ACKNOWLEDGMENTS

My sincere thanks to sir, Mr. Sudheer Shetty, associate professor and head of the department of computer science and PG coordinator Professor B.S.Umashankar sir in Sahyadri college of engineering, Mangalore, for their constant support and encouragement.

## 7. REFERENCES

[1] Richa Chowdhary, Satyakshma Rawat " One Time password for Multi-Cloud Environment" IJARCSSE , Vol.3,issue 3March 2013.

[2] T.Pavan Kumar, Nagesh Vadaparthi, A.Manvi , A.Alekhya "Secure Session based Authentication Schemes " IJERA, March-April 2013.

[3] S.Balaji, Lakshmi.A, V.Revanth"Authentication techniques for Engendering Session Passwords With Colors And Text" Advances in Information Technology and Management Vol.1,No.2,pp 71-78, 2012.

[4] Vijayakrishnan Pasupathinathan "Hardware-based Identification and Authentication Systems", Dec 2009.

[5] Rupesh Tapkiri, Shubhangi Khalate, Priyanka Sarade "Two Level Authentication Schema" IJERT March 2013.

[6] Dinesha H A and Agrawal V K: "Multi-level Authentication Techniques for Accessing Cloud Services". CORI, Bangalore. Karnataka, 2013.

[7] Mini Android PC user manual Copyright © Edis Trading (HK) Limited 2008-2012, pp. 1-23.

[8] Android mini PC user manual,pp 1-26,Model : MK802 Ver.01 www.unisen-usa.com.

[9] Tanvi Naik, Sheetal Koul "Multi-Dimensional and Multi-Level Authentication techniques" IJCA August 2013 Vol.75,No.12.

[10] Dinesha H A,Dr.V.K.Agrawal "Multi-Dimensional password generation techniques" IJCCSA June 2012 Vol.2,No.3.

[11] Kalyani.M.Borse, Ankita.G.Deshpande" Security In Multi-Cloud Data Storage With Sic Architecture",IJERT 2014