Implementation of Variable One Time Password For The Purpose of Authentication In Cloud Computing Above Already Present Honey Pot Technique To Increase Security Mechanism

Vasundhara Pandey[1], Vimmi Pandey[2], Vinamra Bhushan Sharma[3]
[1, 2] Dept of Computer Science And Engineering
[3]Dept Of Civil Engineering
[1, 2] Gyan Ganga College Of Technology Jabalpur(M.P), 482003
[3]Global Engineering College Jabalpur(M.P), 482002

Abstract- *To leverage the level of security to a higher level, of the data stored over the cloud. In today's scenario, the concept of Cloud Computing is increasing widely providing it's users various beneficiary features such as: making the resources available to its users as they require them at very affordable costs, providing them space to store the data of their enterprise without actually purchasing the server etc. However, Cloud Computing faces various security challenges like: traffic handling, access control, application security, authentication issues etc. The genuine user of the cloud will always want that its data is highly secured over the cloud from every aspect. So, here we shall discuss the technology of implementing the concept of Variable OTP over the existing Honey pot to make the authentication and access to the data over the cloud for a genuine user more secured.*

Keywords- Cloud Computing, Honey Pot, Variable OTP Authentication.

I. INTRODUCTION

Cloud computing is designed to meet the increasing demands for internet usage which also describes inter network. There have been many definitions of Cloud Computing those have been used by different research scholars but the most popular defined by National Institute of Standards and Technology (NIST) which describe as: "Cloud Computing is a representation for enabling ever-present, convenient, on demand network access to a shared pool of configurable computing assets that can be rapidly provisioned and released with minimal management attempt of client and service providers communications. The data in the cloud largely deals with crucial three security issues: Confidentiality, Integrity and Availability.

1.1 Cloud Security Challenge

Many challenges are being faced in the domain of cloud computing, some of them are as follows:

- Authentication
- Availability and Reliability
- Security and Privacy etc

1.2 Cloud Computing Benefits

- Flexibility of Work in Practice
- Disaster Recovery
- Reduced Cost

\

1.3 Honey Pot Technique

Honey pot systems are the decoy servers or systems setup to gather information regarding an attacker or intruder into the network, system or cloud. Honey pots and be setup inside or outside in the DMZ of the firewall design or even in the locations. Although they are most often deployed inside of a firewall for control purpose. Various IDS standards are to be met for a honey pot,

1.4 Methods of authentication in Cloud Computing

- **Kerberos:** it is a computer network authentication protocol that works on the basis of tickets to allow nodes communicating over a non secure network to prove their identity to one another in a secure manner.
- **OTP(one time password) authentication:** it is a password which is valid for only one login sessions. It overcomes various shortcomings that were there in the static password based authentication.etc.

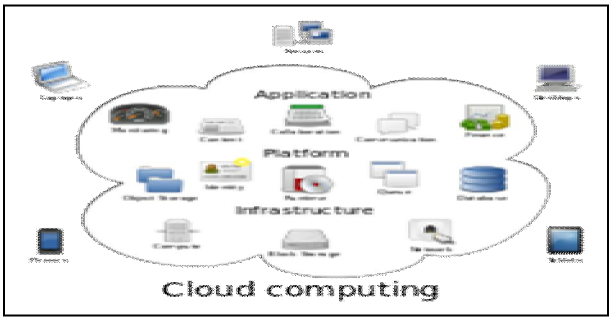


Fig.1 Cloud Computing

II. LITERATURE REVIEW

1. Abdelmajid Hasan Mansour Emam, this author in his research work has provided a security barrier in cloud using the Email authentication part, so that only a valid and legitimate user access the cloud.
2. Deepti P.Theng and Snehal G Kene, these authors in their research took care of the various attacks possible in cloud computing, with respect to these attacks they focused and resolved these issues with the help of Signature Based Detection and Anomaly Based Detection techniques. Which on further elaboration in turn results such that a large database is maintained for keeping the track of previous record of the user.
3. Lynda Sellami and Pierre Tiako, these authors in their research worked upon the Novel Ubiquitous approach for Intrusion detection. In their approach they had discussed about the three phases know as the: Initialization Phase, Detection Phase, and Isolation Phase. In which using algorithms this process is carried out.

III. OBJECTIVE AND METHODOLOGY

OBJECTIVE:

1. To receive the correct information from the legitimate user of the cloud.
2. To send him correct Variable OTP to initiate the process of Authentication.
3. To match the information resent by the user to authenticate if the user is true or not.
4. If the match comes out to be genuine, provide the user an access to his stored data over the cloud.
5. If the mismatch happens for more than the third time, bar the user from accessing his data over the cloud until he contacts the administrator.

METHODOLOGY:

We are proposing a concept such that to make the data over the cloud secure using the technique of One Time Password(OTP) merging it with the existing Honey pot technique to provide a secure access to the legitimate user to his data in the cloud.

Here we will discuss about the Honey pot Technique and OTP algorithm.

Working Of a Honeypot:

Honeypot works in three respective phases such as:

1. Detection: it looks for convergence with existing technology
2. Honeypot Farm: a virtualized trap is created to lure the intruder
3. Traping: track and eradicate the intruder.

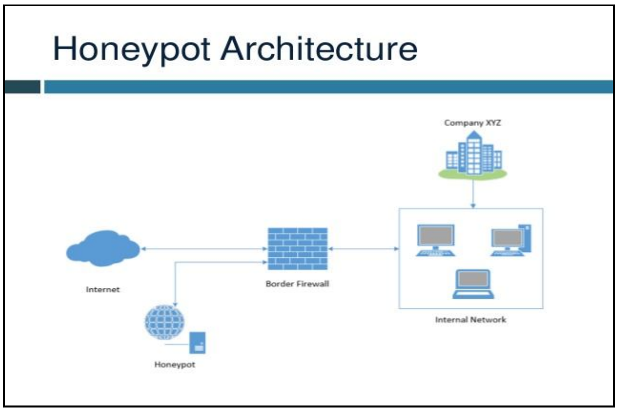


Fig. 2 Honeypot Architecture

OTP Algorithm:

In this algorithm One Time Password has been used to authenticate the user. The password is hence used to keep the user account secure from the unauthorized user. But the user defined password can be compromised. To overcome this difficulty, OTP is used in the proposed security model. Thus, whenever a user logs in the system, he will be provided with the random 6-digit code by the system with the help of the service providers gateway, this password shall be randomly generated.

The previous record of the user shall be stored and at every new entry by the user shall update the existing record of the user. As a result only authorized user with a valid mail will be able to connect to the cloud system.

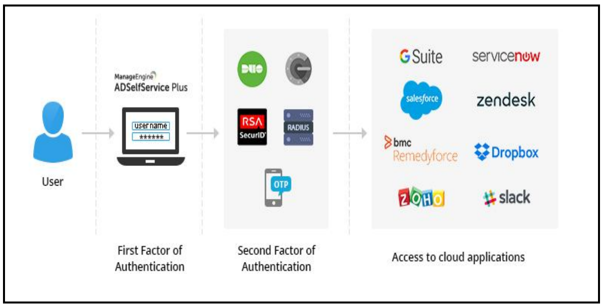
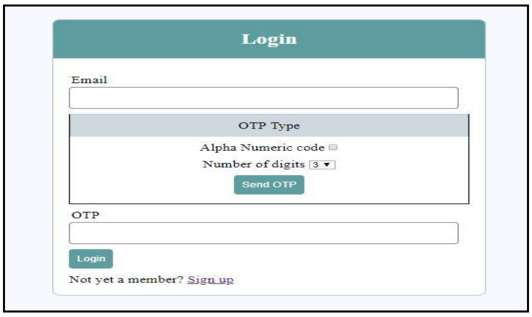

User
ManageEngine ADSelfService Plus
user name
******
DUO
RSA SecurID
RADIUS
OTP
G Suite
servicenow
salesforce
zendesk
bmc Remedyforce
Dropbox
ZOHO
slack
First Factor of Authentication
Second Factor of Authentication
Access to cloud applications

Fig 3 Working Of OTP

IV. RESULT

RESULT OBTAINED AFTER IMPLEMENTATION:

1. **Login Page** it is the page which the user of the cloud shall access for logging into his account to retrieve it's data which is stored on the cloud.



Login

Email

OTP Type

Alpha Numeric code □

Number of digits 3 ▾

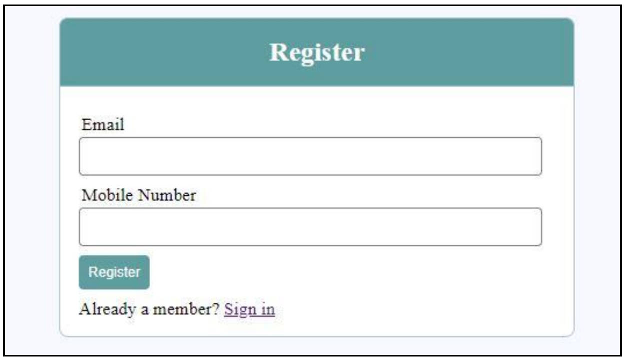
Send OTP

OTP

Login

Not yet a member? Sign up

2. If the member is not registered he will be redirected to the **Registration Page.**



Register

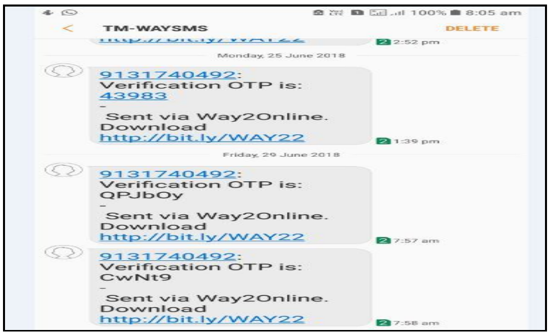
Email

Mobile Number

Register

Already a member? Sign in

3. The Screenshot of the SMS of the **Mobile OTP received by the SMS Gateway**



TM-WAYSMS DELETE

8:05 am

2:52 pm

Monday, 25 June 2018

9131740492:
Verification OTP is:
43983
-
Sent via Way2Online.
Download
http://bit.ly/WAY22

1:39 pm

Friday, 29 June 2018

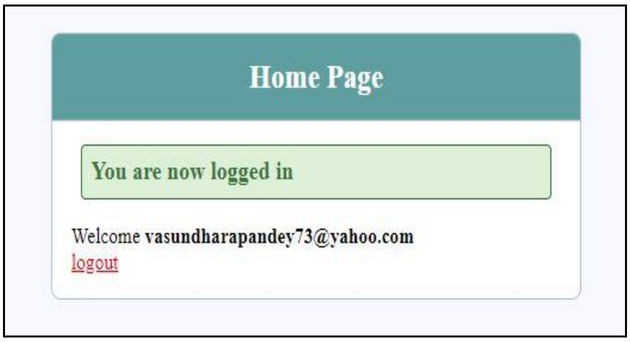
9131740492:
Verification OTP is:
QPJbOy
-
Sent via Way2Online.
Download
http://bit.ly/WAY22

7:57 am

9131740492:
Verification OTP is:
CwNt9
-
Sent via Way2Online.
Download
http://bit.ly/WAY22

7:58 am

4. If the user had entered all the entries correctly then he is successfully **logged in** to its stored cloud data.



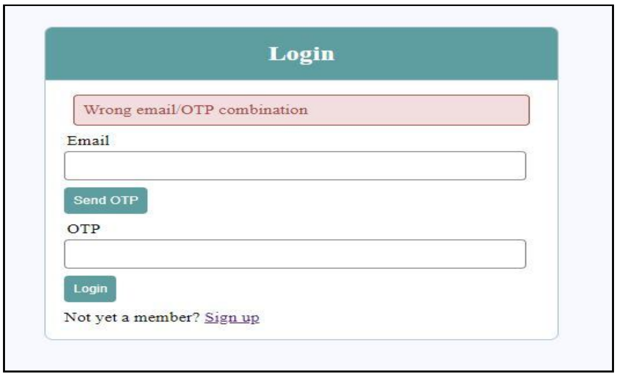
Home Page

You are now logged in

Welcome vasundharapandey73@yahoo.com

logout

5. If the user fails to login due to some incorrect entries



Login

Wrong email/OTP combination

Email

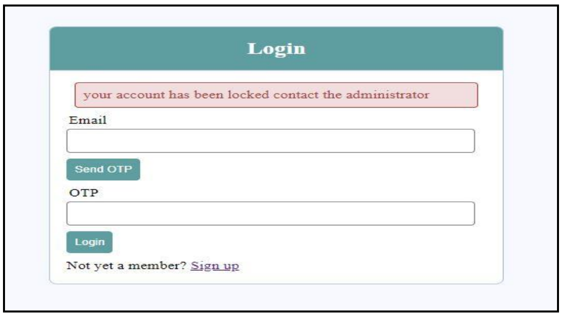
Send OTP

OTP

Login

Not yet a member? Sign up

6. On multiple fail in login attempts the users id gets locked.



Login

your account has been locked contact the administrator

Email

Send OTP

OTP

Login

Not yet a member? Sign up

V. CONCLUSION

Cloud Computing is an emerging IT concept and as per the budding time, it is also getting extended. Now a days, the users in the cloud are tremendously increasing with time and hence this is a serious concern about the cloud security, which is the prime concern for all its users. In our work we have discussed the security of the users data over the cloud by implementing the OTP technology over the Honey Pot to provide a safe and secure access to the user.As the requirement of the information the designed framework portrays that the our work, which proposes to provide a better security in comparison to other work.

REFERENCES

[1] Deepti P. Theng, Snehal G. Kene "A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges", conference organized by ICECS and IEEE – 2015 Hyderabad, India.

[2] Ajey Singh, Dr. Maneesh Shrivastava, "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume 1, Issue 4, pp. 321-323, April 2016

[3] Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd AlDosari, "A Secure Cloud Computing Model based on Data Classification", 1st International Workshop on Mobile Cloud Computing Systems, Management, and Security (MCSMS-2015).