Authenticating using Variable One Time Password in Cloud Computing over Existing Honey Pot Technology for Framework Improvement

Vasundhara Pandey
PG Student
Department of Computer Science and Engineering
GGCT, Jabalpur, India- 482003

Vimmi Pandey
Assistant Professor
Department of Computer Science and Engineering
GGCT, Jabalpur, India- 482003

Abstract

To increase the security of the data stored in cloud. Cloud computing is the most promising concept, which increase as rapidly as the time passes by. In Cloud computing the data of the user is stored in server and the security of the data is the prime duty of the service provider of the cloud, hence it tries to ensure security of the data of the customer, but generally it fails to do so. As the service provider does not know if the actual user has logged in or not. So as a solution to this problem, the proposal is, the concept of Implementing Variable OTP Authentication over the existing Honey pot mechanism in Cloud Computing. In this proposed work, authentication is done if the actual user has logged in or not by sending an OTP to the registered mobile number, this OTP can be variable in the sense that the user can choose the number of digit of the OTP as to how long must the OTP is to be sent and also the type of OTP whether numeric or alpha numeric. If authentication is successful user can access it's data over the cloud else by the use of Honey pot technology on consecutive three wrong login attempts the users id gets locked and gets stored in the database and further the user is barred from logging. By using this concept security architecture in cloud is increased. This proposed work is more robust and secure than the previous approach.

Keywords: Cloud Computing, OTP Authentication, Honey pot

I. INTRODUCTION

Cloud computing is an impressive and most promising concept. Users today are very aware of this recent technology and it's advantages so they heartily use it. Cloud computing enables us to contact the shared pools of accessible system resources and higher level services that can be quickly provisioned with least management effort, often to the internet. Cloud computing depends on sharing of resources to achieve consistency and economies of scale similar to public convenience.

OTP generation algorithms generally uses randomness, making predictions of the successor OTP by an attacker difficult and hash function.

Approaches to generate OTP are:

- Time synchronization: this OTP is usually related with a piece of hardware known as security token. Inside the token there is an accurate clock which is synchronized with the clock on the authentication server, where the time stamps are been matched and authentication is been done.
- Mathematical algorithms: each new otp shall be created from the past otp used, it is credited to Leslie Lamport which uses a function (f) for generation etc.

Honey pot is a technique which the developers use to lure the intruders by creating a trap of virtual environment.

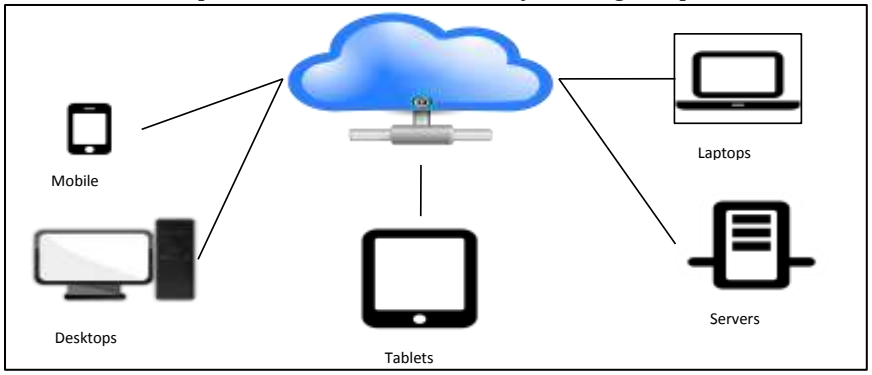


Fig. 1: Cloud Computing

II. LITERATURE REVIEW

1) Matt Guyan and Jeremy Savan, these author focus upon the data security at the place of use. In this work these authors worked by making the analysis of the basic requirements of the user, and keeps a record of his entries and his basic pattern. If certain malicious approach is tracked it traps the user accordingly.
2) Takauya Suzuki and Masayuki Okuhara, these authors had basically discussed about the Security architecture in cloud computing so that, using Access Control, Authentication and ID Management, and Security virtualization mechanisms so that to forbid the unauthentic access in the cloud.

III. OBJECTIVE

1) To enter the email and mobile number of the cloud user into the secure data base.
2) To send the selected variable OTP as desired by the user.
3) To authenticate the OTP entered by the user whether the user is authentic or not.
4) If genuine grant the user the access to the cloud, where the data of the user is already stored.
5) If in case the user is not authentic, and it tries to login again and again, then after three consecutive wrong login attempts bar the user and lock its id and store it in another DB for further action.

IV. METHODOLOGY

As discussed above, discussion about the problems that the users and providers of the cloud are in front of nowdays, so as a solution to these problems, 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 Honeypot technique to provide a secure access to the legitimate user to his data in the cloud.
Here we will discuss about the Honeypot Technique and OTP algorithm.

A. 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.

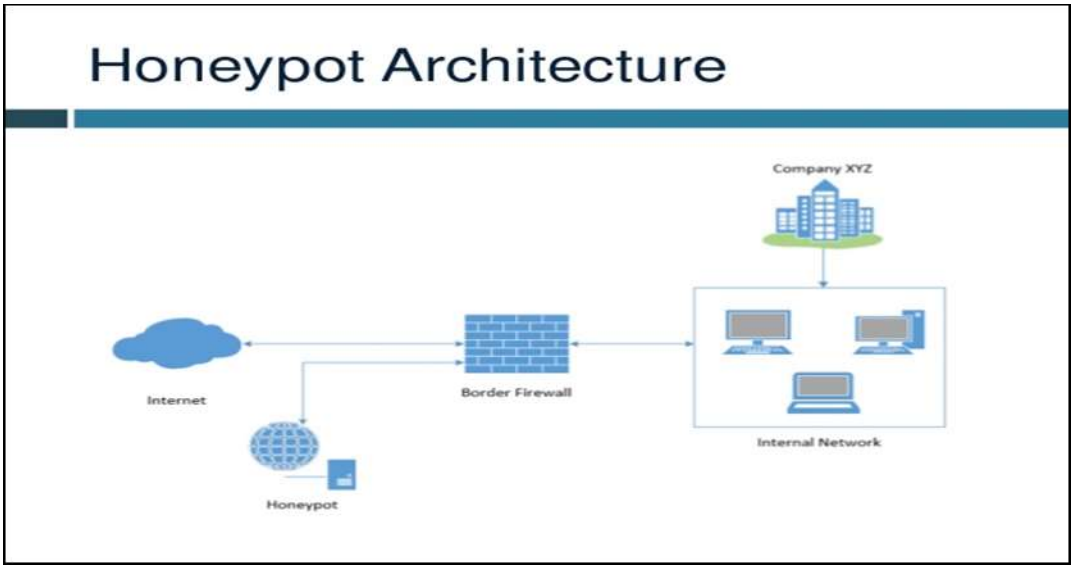


Fig. 2: Honeypot Architecture

B. 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.

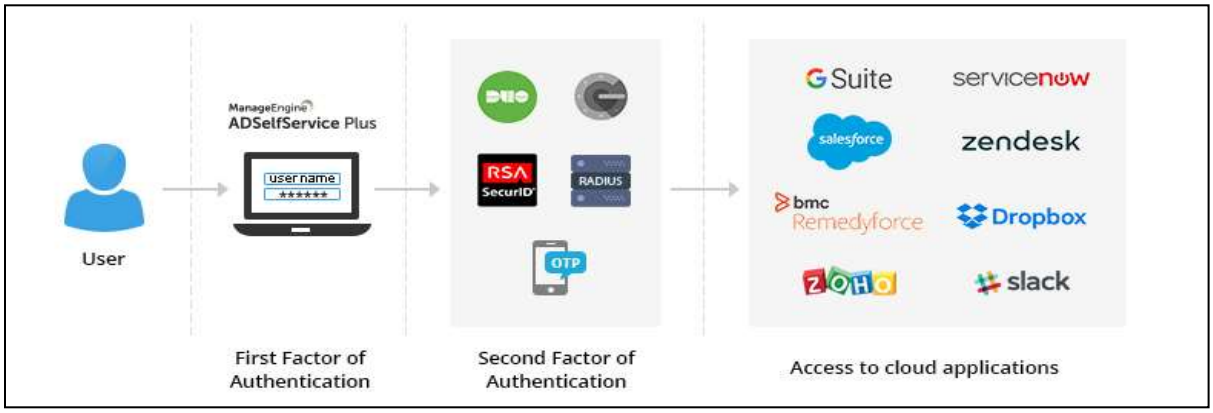
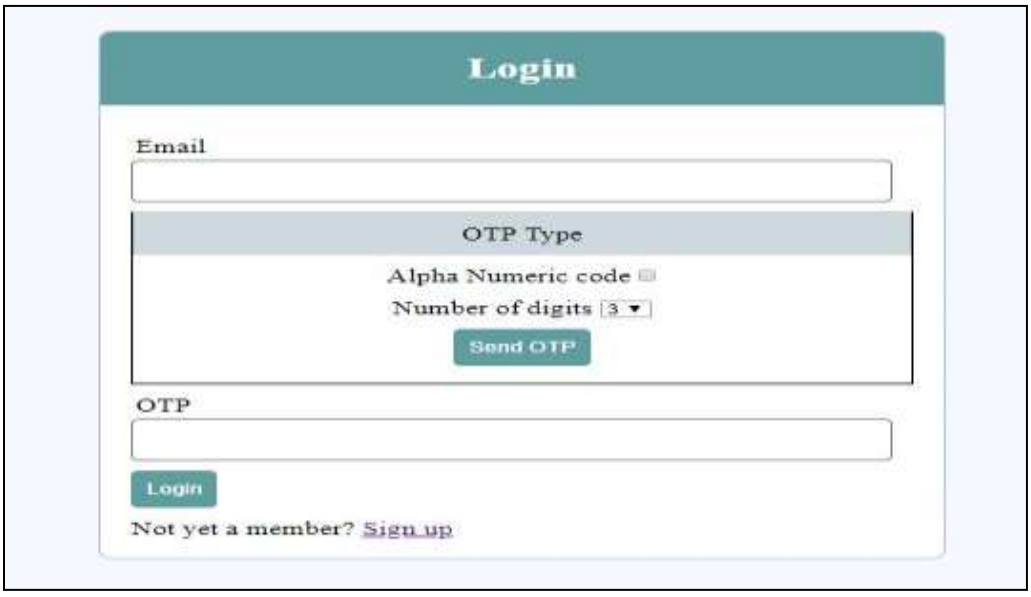


Fig. 3: Working of OTP

V. RESULT AND COMPARISON

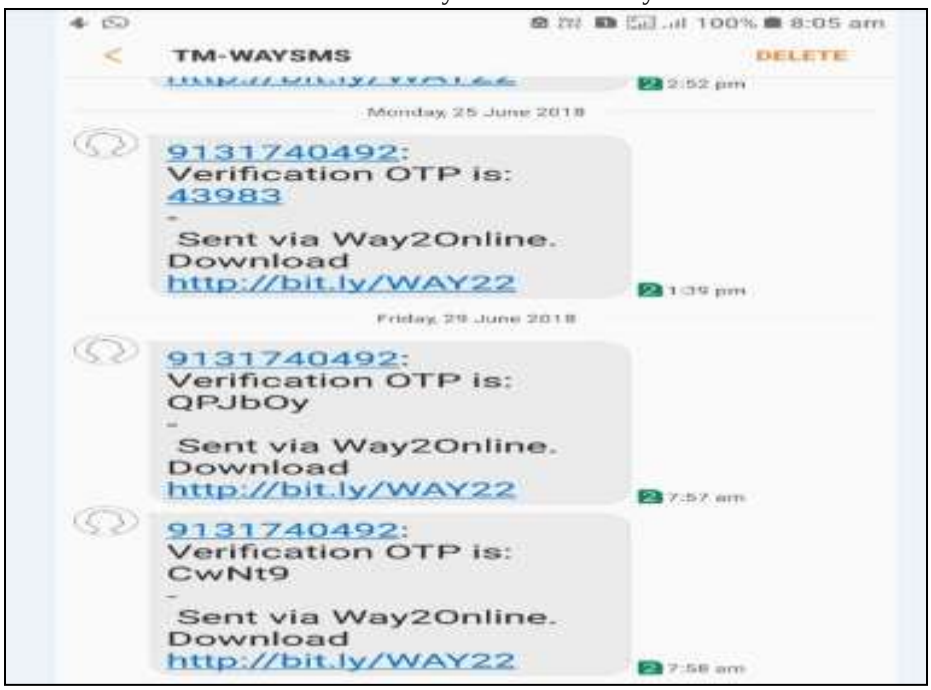
A. Result

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.



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

3) The Screenshot of the SMS of the Mobile OTP received by the SMS Gateway



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

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

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

B. Result Graph

As the part of Implementation we have tested the performance of the security of the users data before implementation of the OTP and after the implementation of the OTP. The below graph depicts the following:
The comparison of performance is depicted by the graph below:

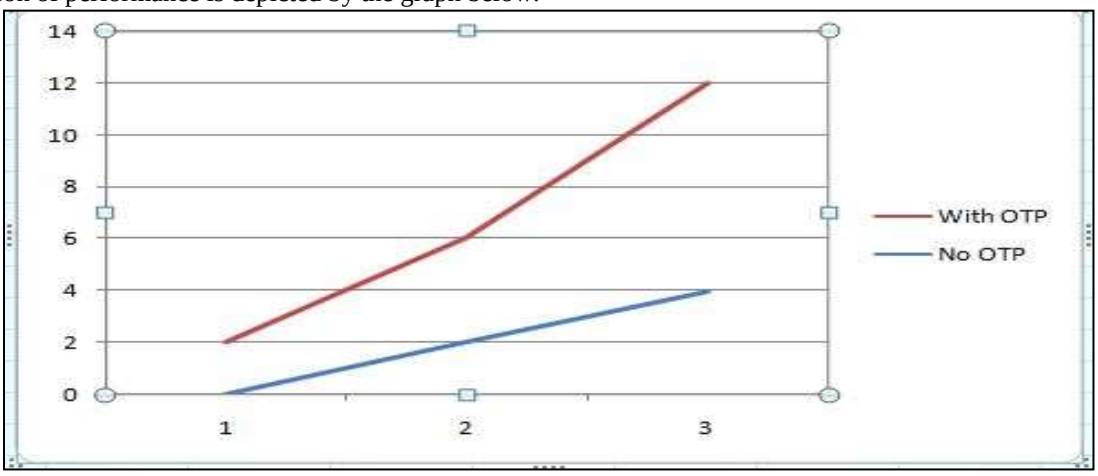


Fig. 10: Comparison of Performance

The comparison of the query execution time before and after is depicted by the graph below:

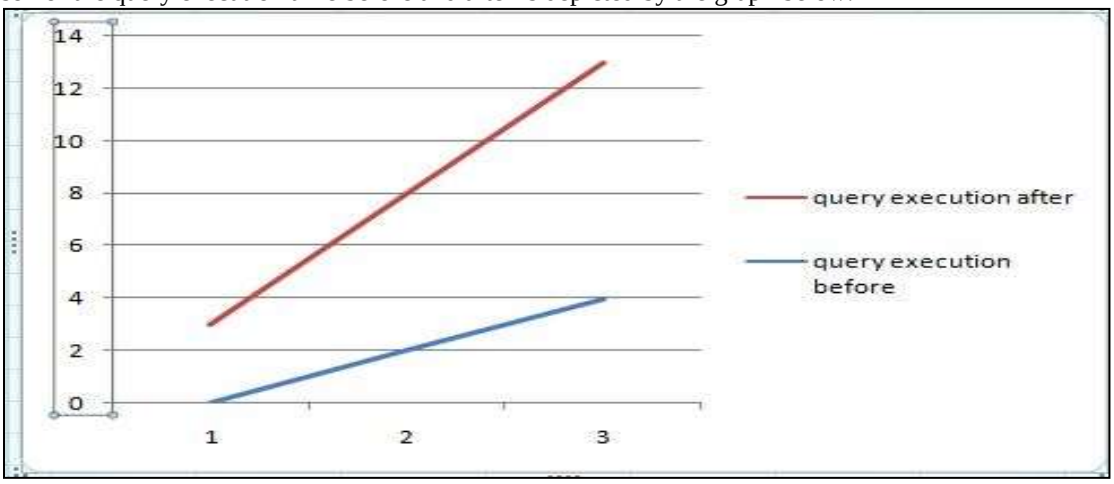


Fig. 11: Comparison of Query Execution Time

VI. 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] Syed Rizvi, Gabriel Labrador, Matt Guyan, Jeremy Savan "Advocating for Hybrid Intrusion Detection Prevention System and Framework Improvement", conference organized by Missouri University Of Science and Technology – 2016 Los Angeles, CA.
[2] Rizwana Shaikh, Dr. M. Sasikumar, "Data Classification for achieving Security in Cloud Computing", International Conference on Advanced Computing Technologies and Application ICACTA-2015 Bangalore, India.
[3] B.Meena, Krishnaveer Abhishek Challa, "Cloud Computing Security Issues with Possible Solutions", International Journal of Computer Science And Technology (IJCST), ISSN:0976-8491 (Online) | ISSN : 2229-4333 (Print) Vol. 3, pp. 340-344, Issue 1, Jan. - March 2016.