Access Control in Cloud Computing Environment

Soorat Hussain
Department of Computer Science, Mohammad Ali Jinnah University, Karachi Pakistan
Email: soorat@gmail.com

---**ABSTRACT**--

Cloud Computing is a new technology which is directly connected with the internet which provide on demand self service internet infrastructure where a customer can pay and use only what is needed. Cloud Computing all services are managed by third party cloud service provider. Nowadays majority using static password to login into the system or access the online accounts in cloud but never change the password which is not secure . Since Cloud computing is a quite new subject, most of the cloud providers have not yet tighten up their security and still use insecure or complicated login method. Static password thoroughly investigated and found out that it is not completing the cloud computing security requirement. Proposed solution is One Time Password and One Day Password, OTP will get expire after two minutes, if user again login will request and receive new password via email and ODP will get expire after 24 hours and on request receive new password via email for new login session. OTP/ODP used with AES encryption. This paper focuses the authentication and transmission encryption in cloud computing services.

Keywords - **Authentication, OTP/ODP, AES.**

Date of Submission: March 03, 2014 Date of Acceptance: April 06, 2014

1. Introduction

People can only enjoy the full benefits of cloud computing when third party cloud service providers provide the proper security which can secure people confidential information and data. People lost their control on the their data when it moves on cloud and third party cloud service provider take care of all operations. Cloud computing security should be very secure and reliable otherwise the people confidential information will get compromise. People Still Using the same passwords to access the different accounts on the cloud which is very insecure and third party cloud computing service providers are not providing proper security about static passwords. This his is the big disadvantage of the cloud computing environment because static password can be attacked by unathorised user and account information can be easily taken by hackers. The solution of this security problem is the introduction of one time password/One Day password with AES encryption.OTP validity is two minutes and ODP validity is 24 hours, after the specified time limit the passwords will get expire .The AES encryption algorithm has used to provide the security about authentication. These two security factors AES encryption and OTP/ODP improve the security performance and reliability in cloud computing environment.

2. Static Password

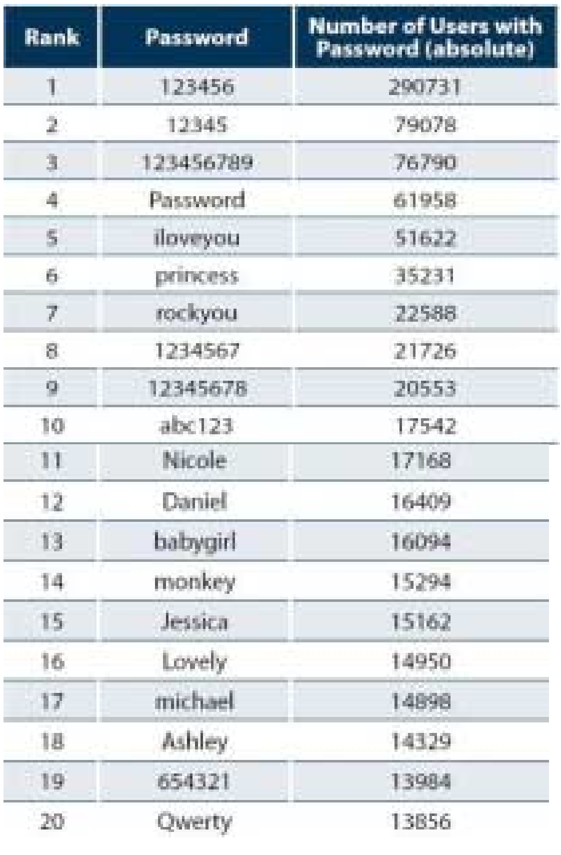
The static password always create problem and people often use the same password more then one account which means that if one account password get hack then rest of the accounts also get compromise on cloud. People rarely change their passwords but not in days, weeks, months but might be in years which is also not safe. Still majority using static password because everybody is not computer professional and unaware about hacking activities. The static password problems have been deeply investigated beside that current problems solution used to login to cloud services have been thoroughly investigated and monitored and finalized that they don't satisfy the needs for cloud service. Some systems are complicated some are costly and some of them are insecure. The main weakness static password is that if it is simple it can be easily attacked by Trojan attacks, password attacks, or by simply guessing it. A static password is the usual way that a user authenticate when log in to a service is needed. The password is usually a secret word or phrase picked by the user and used together with the user's username. It can be used when logging in to your own personal computer, an e-mail system, an online community etc. Even though static passwords is used almost everywhere, from a security point of view it has a lot of problems. The static password can be hacked with very little efforts by attackers because the attackers will not take care of time to decrypt the password and people confidential information will get hack very easily by the unauthrised user.
The picture below shows the typical example of static password.

Username: Bob
Password: •••••••
□ Remember me next time

Figure 1. Example of Static Password

3. Top Twenty Password

In an article from January 2010, a list of 32 million passwords that got stolen in an attack, have been examined. The number one most popular password used by most users was 123456, and the top 32 password was all bad from a security point of view. The password list was further studied in a report from the security company Imperva. In that report it is stated that about 30% of the passwords had a length of six characters or below. Furthermore, 60% of the password only used a limited set of the most common characters and half the passwords on the list was based on names, slang, dictionary word or other forms of simple passwords. This shows a clear example on how static passwords can't meet today's security standards. The following picture shows the top 20 passwords from the password list. Table captions appear centered above the table in upper and lower case letters. When referring to a table in the text, no abbreviation is used and "Table" is capitalized.



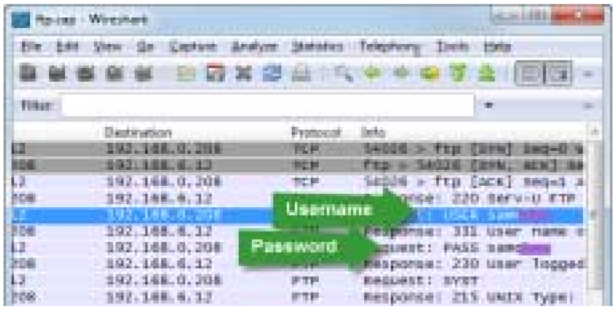
Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Figure 2: Top 20 Password

4. Wireshark Packet Captured

This is very common nowadays hackers use the software's to capture the password and people often don't use SSL and encryption therefore it become very easy for attackers to captured packets from live traffic, the figure below shows the example how wireshirk software capture unencrypted packets in cloud environment.

In the picture it is clearly shown that user id and password has captured.



```
        Destination        Protocol  Info
12      192.168.0.208      TCP       54026 > ftp [SYN] Seq=0 W
208     192.168.6.12       TCP       ftp > 54026 [SYN, ACK] Se
12      192.168.0.208      TCP       54026 > ftp [ACK] Seq=1 A
208     192.168.6.12                 Response: 220 Serv-U FTP
12      192.168.0.208                : USER sam[redacted]
208     192.168.6.12                 Response: 331 User name o
12      192.168.0.208                Request: PASS sam[redacted]
208     192.168.6.12                 Response: 230 User logged
12      192.168.0.208      FTP       Request: SYST
208     192.168.6.12       FTP       Response: 215 UNIX Type:
```

Figure 3: Wirshark Captured packets

5. One Time password/One day password

One time password is best solution as compare to static passwords in cloud environment because in this method every time users get login but with the new password. The password get expire within two minutes but session will be activated but when users again login he/she will be given a new password so this cycle will continue, if hackers capture the packets and decrypt the AES encrypted password and user Id it will be useless because password get change within two minutes. Same procedure apply on one day password after 24 hours password get change. It means that this application can be used in both situations either packets are encrypted or not.

A. User Sign Up Process

This new technique of user sign up has been added with the feature of OTP and ODP by which the users can decide upon their type of the usability and the security.

- A non frequent user uses OTP (one time password) and always gets the new password for each access and hence providing the security with the each access.
- A frequent user go for ODP (One Day Password) so that the user need not change the password on.

Means that according to users designation, level of privileges are defined.

6. Encryption Technique

AES has implemented in this application for authentication during transmission. AES as compare to RSA, DSA, and RC4 is much better encryption technique because its algorithm fast and reliable. We have introduced OTP/ODP with the AES encryption these two security factors together produce firm authentication results. AES is very fast and reliable algorithm which confirm the user authentication in a proper way.

7. Proposed Security Solutions

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. Have an easy-to-understand registration system, that at the same time doesn't compromise the security.
3. Use an encryption algorithm that is secure but also fast, to be able to serve the vast amount of cloud users.
4. Offer a solution that is free of charge in order to attract more customers to the cloud services.
5. 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.

8. Member Login Procedure

This is the first Screen when member will try to login into the system but first the person will receive new password in the email then will get login permission. The user name will be the same as enter during registration but password will be changed within two minutes or 24 hours.

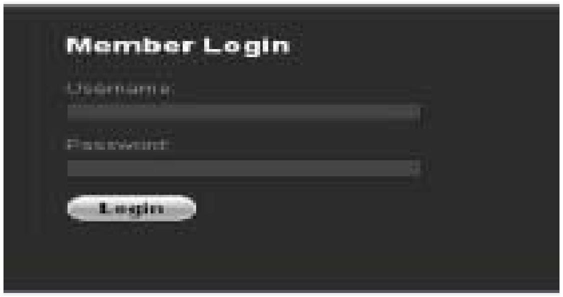


Figure 4. Member Login

9. Post Screen Method

This is the Post Screen the user will enter the user name and token and receive password via email, validity will be two minutes or one day after specified time the password will get expire.

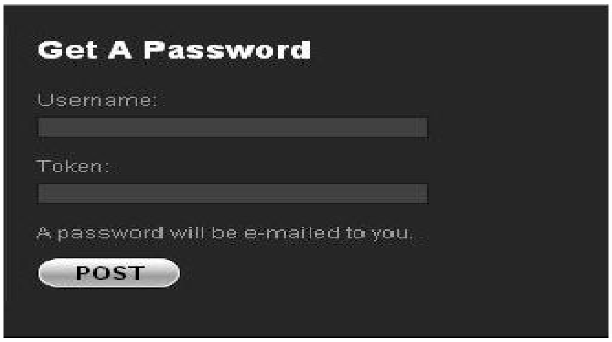


Figure 5: Get a Password

A. User Authentication

The get a password main idea about is confirm the user authentication and then issue a password if user is not genuine then authentication first confirm it then deny the permission otherwise the password will be issued.

B. Additional Security Layer

Get password mechanism is very simple and easy again in this screen not email is available which means that if hacker somehow get the user token and password but not be sure about the email address, this technique add additional security into the application. This application is very secure and capable to secure the companies or individual information and data in a very efficient way in cloud environment.

10. Registration Process

The registration process is very simple which can use by both professional and new user. The below Screen shows the registration process where users enter their details.

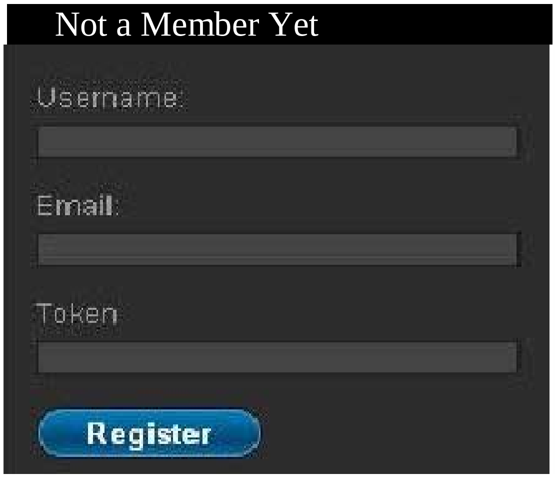


Figure 6: Registration

First user will complete the registration process.

1. User Enter The name
2. User will Enter Email address
3. User will put Token Number.

In this process after registration the Email address will never travel only user name and token number will move source to destination. If email address will not travel then attackers will not hack the password because user will receive the password via email and if hackers does not have email address then they can not hack the password for that they need email addresses of the accounts. Registration process is very easy all type of customer easily can get register with the application in cloud. The main advantage of this application is that its not too heavy as compare to other systems. Often applications get heavy by putting too much validation checks which effect on the terminal processing. This application has designed according to the security and user requirements.

11. Database containing user credential

```
Mysql> SELECT * from users;
```

USER	EMAIL ADDRESS	TOKEN
SOORAT	Soorat2@hotmail.com	1245
ATIF	atif@yahoo.com	4637
Raheel	raheel@gmail.com	8867
Kashif	kashif@secure.com	5467

A. Database Authentication

Database confirm the user authentication by token number, user name and email address. If user enter wrong token number or user name then access will be denied otherwise user will be given permission to use the system.

12. Conclution and Future Works

In this paper has looked at the current security situation in cloud computing. Proposed ways to securely and easy login to a cloud service using one time password and one day password which the user use. The best encryption algorithm to use in cloud services, with regards to safety and speed, have been evaluated. The proposal ended up in a working solution that use OTP/ODP authentication for the login procedure, a very secure registration system and with all traffic transmissions encrypted with AES. The implementation provides high security for the users while it is still easy to use. It provides benefits over the current security solutions for authentication that is used today. The big difference from solutions with static passwords is that the passwords in this solution are only valid for specified time limit only, which is big advantage in security. Since cloud services is used by millions of users, the security must be very good in order to protect private data, and also be fast, flexible and easy to use for all of the different users with different technology skills. For future work the time synchronization between the email and server should be fixed. It should be also investigated if it is needed to implement a more secure algorithm.

References

[1] Syed, M. R.; and F, Mohammad; "PccP: A Model for Preserving Cloud Computing Privacy", 2012 International Conference on Data Science & Engineering(ICDSE), 2012 IEEE.

[2] Wang, B.; Baochun; wang, H.L.2012 Oruta: Privacy-Reserving Public Auditing for Shared Data in the Cloud, IEEE Fifth International Conference Cloud Computing, 2012 IEEE, DOI 10.1109/ Cloud .2012.26.

[3] Performance Analysis of Advanced Encryption Standard (AES) , Y. X. Guizani & S. Bo Sun Hsiao-Hwa Chen Ruhai Wang, Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE .page(s): 1.

[4] Dynamic Authentication: Need than a Choice, A. Saxena, Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference, 10 (1) (2008), 214

[5] Safer Authentication with a One-Time Password Solution D. Griffin, MSDN Magazine, Issues. Published May 2008.

[6] Analysis and Research of Cloud Computing System Instance", S. Zhang & S. Zhang & X. Chen, Future Networks, 2010. ICFN '10. Second International Conference. 22-24 Jan. 2010.page(s): 88.

[7] The Comparison Between Cloud Computing and Grid Computing", S. Zhang & X. Chen, Computer Application and System Modeling (ICCASM), 2010 International Conference. 22-24 Oct. 2010.Page(s): V11-72.

[8] If Your Password Is 123456, Just Make It HackMe", A.Vance, The New York Times.Published 20/01/2010.

[9] A Novel Web Security Evaluation Model for a One-Time-Password System", B. Soh & A. Joy, WI 2003. Proceedings. IEEE/WIC International Conference, 13-17 Oct. (2003), 413.

[10] A Two-Factor Mobile Authentication Scheme for Secure Financial Transactions", R. Di Pietro & G. Me & M. A. Strangio, ICMB 2005. International Conference. 11-13 July (2005), 28.

Authors Biography

Soorat Hussain has completed his masters degree in telecommunication and Networks from Mohammad Ali Jinnah University and Bsc(hons) from London Metropolitan university. He is currently working as a lecturer. His interest about cloud computing security, Spectrum Allocation.