IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Preserving privacy in Cloud based applications using two-factor authentication (TOTP/WTP)

Pranayanath Reddy Anantula[1], [2]Dr G Manoj Someswar

[1] CSE Department, Alliance University, Bangalore, Karnataka, India

[2] Director General & Scientist-G, Global Research Academy, Hyderabad, Telangana, India

Abstract: Security and Privacy are the major concerns in the current trends of cloud environment. Securing the data and applications from the intruders, Hackers and internal attackers has become a challenge. On the other hand Preserving the privacy of users is also became a challenging task. Most of the cloud based service providers are providing high level of security but privacy of user is done only once at the authentication level. Many of the applications such as Salesforce.com, Google, and Amazon etc are using two factor authentications (TOTP). In this paper we have proposed secure cloud authentication architecture to deal with privacy in cloud applications, by using periodic two factor authentication in cloud systems.

Keywords: TOTP, WTP, Two-factor Authentication, Cloud Security**.**

1. INTRODUCTION

Adaption of Cloud computing has increased drastically in all industries. All the applications are migrating into the cloud based applications. This kind of change is happening because of services provided by the cloud vendors. The major service that is always looked by the customers is security and privacy. Privacy of information through authentication is being considered as vital task. Providing security requires more than user authentication with passwords or digital certificates. [1]. Customers can get trust in cloud vendors if they address how they are maintaining privacy and security of sensitive information in the cloud. There exists a problem of cross-data exchange as data has been stored in a multi tenancy framework. This raises the question of privacy of data when sharing the data in the cloud environment.
Privacy is one of the aspect that need to be dealt in cloud computing, both in terms of legal compliance and user trust, and privacy needs to be considered at every phase of design [2]. Privacy means protecting user information from intruders. A privacy breach is not acceptable in cloud environment it may lead to a great loss to the cloud vendors. Privacy control allows the person to maintain a degree of intimacy [3].

As data is growing exponentially in cloud, data security and privacy has been considered a major issues that hamper the growth of cloud computing, if it is not dealt with proper process. Various attempts have been made in the past to safeguard the privacy of the individual or agency trying to utilize the services being provided by the cloud [4].

Users must guarantee for feeling that privacy of data has been ensured in cloud environment [5]. One of the process to ensure the user about the privacy of data is through two factor authentication.

2. TWO-FACTOR AUTHENTICATION

In the present trend most of the transactions are done through digital mode. Transactions such as banking, retail orders, transportation etc. and doing transactions over a digital medium has become a natural phenomenon; this has brought huge challenges to the organizations that are providing the services. Stakeholders are expecting transactions to be secure and provide privacy for their data. From the time OTP has come in to picture, it has been used as one of the authentication level in doing the transactions. OTP has gained huge popularity and almost all applications are using OTP as additional level in authentication process.

A one-time password is a key value pair that is created every time a user login or request any transaction which require valid user authentication to complete the transaction. OTP are used only for digital systems and these are valid only for one transaction or login session. OTP's are incorporated in number of applications and also used in two factor authentication.
By implementing authentication, it can ensure that system's resources are not obtained fraudulently by illegitimate users [6].

The advantage of OTP is generating dynamic password in contrast to static passwords, and these code cannot be used for replay attacks. Even if Hackers or intruders capture an OTP that was already used for some transaction, that same OTP is not valid for other transactions, so they cannot use

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

it again, since it will no longer be valid OTP. OTP's has become a mandatory for almost all transactions which are done through online or digital medium. Every person is equipped with a digital gadget which can receive text messages and also these have replaced to remember the password to login into the systems.

2.1 Generation of OTP's

OTP's are generated with various algorithms, typically using randomness or hash functions. Those are used to derive a value that is difficult for an attacker to capture and regenerate them. Various approaches are available for generation of OTPs, some of them are:

1) Time-synchronization based - OTP;s are valid only for short period of time i.e., between client and server.

2) Mathematical algorithm to generate new OTP based on Old OTP

3) Mathematical algorithm to generate new OTPs (Randomly).

There are some electronic security tokens that are used to generate OTP's such as small gadgets with small display, these gadgets are embedded with software to generate random tokens and these tokens are already liked with user in the application servers.

Other systems consists of software's that runs on mobile phones, and some systems generate OTP at server side and send them to user using SMS messaging. And some systems earlier used are OTP's printed on papers.

Using OTP alone is not safer; it must be used in combination with a password or any other user identity functionality. In General one-time passwords are representation of two-factor authentication (2FA) or (T-FA). It forms an extra layer of security, where attackers cannot hack the application with just user password or using only one type of attack. One-time password technology is often used with a security token.

3. RELATED WORK

A common mode of delivering of OTPs is text messaging. Text messaging is directly available in all the mobile gadgets; it has great potential to reach to consumers with low cost of implementation. OTP through text messaging may be encrypted using some standards algorithms such as A5/x.
As text-based passwords continue to be the dominant form for user identification today, services try to protect their customers by offering enhanced, and more secure, technologies for authentication [7].

In 2011, Google has started offering OTP to mobile and landline phones for all Google accounts. [8] OTPs are delivered either as text or via automated call.

Among the above mentioned generation of OTP's time-synchronization based are most popular as they are more secure as it is maintain a clock in the electronic tokens. It is reducing the degree of vulnerability. If the user doesn't enter the OTP within the specified time it gets expired and no longer can the same OTP be re-used.

The Time-based One-time Password Algorithm (TOTP) is an algorithm that generates one time password which is a combination of current time and secret key that has been shared by both the parties. This is adopted from IETF standard RFC 6238. And it is used in two-factor authentication systems. It is an example of HMAC, which generates password with the combination of hash function, time stamp and secret key. The timestamp can be changed according to the requirement of the systems.

For this to work, the clocks of the server and user system must be roughly synchronized (the difference can be plus or minus 1 time interval). TOTP is based on HOTP with a timestamp replacing the incrementing counter. The current timestamp is converted into a time counter (TC) by defining the start time (T0) and counting in units of a time step (TS). For example:

TC = floor ((server_time (now) – server_time(T0)) / TS),
TOTP = HOTP(SecretKey, TC),

TOTP-Value = TOTP mod 10^d, where d is the required number of digits of the one-time password.

Default hash method used is SHA-1 and default number of digits to be generated is Six [8].

After generating the token it is sent to user through SMS messaging. User submits the TOTP to server. Server checks if the token is matching with the generated token for the requested user. If it is a valid token server give access to the user to proceed further. If token doesn't match it sends a negative acknowledgement to the user and ask for re enter the TOTP. The token is valid only for a specific time stamp. The token will be expired when the time stamp is reached or the token has been used up within the time stamp. Some server generates the TOTP considering the delays that may occur due to synchronization of client time, network latencies or user delays.

This paper is a proposal to use OTP/WTP at periodic intervals to maintain the security of the transactions and privacy of the users. The periodic generation of OTP and validation assure that a valid user is operating the system.

DOI 10.17148/IJARCCE.2016.51289

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

4. PROPOSED ARCHITECTURE

The proposed architecture is as shown in figure 1. The architecture consists of four main components: the CRM application, the OTP generator/ Validate, the User, and the force.com database.

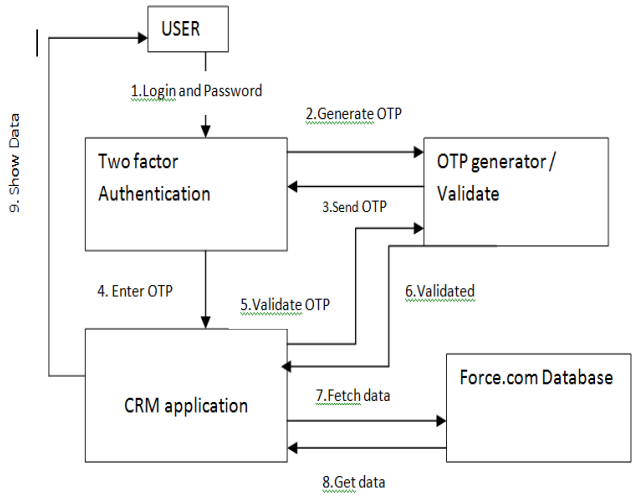

Fig 1: Proposed Secure Cloud Architecture

A TOTP (Time based one-time password) is a password that is valid for only a short period of time or one time use within the time period. WTP (weekly-time password) is a password valid for a week from the time of generating the OTP or one time use within the time period [10].

4.1 Assigning TOTP/ WTP to User

This new technique of sign up of users in to the application has been enhanced with feature of OTP and WTP, where administrator will decide the usability and security based on the role of the user.

Type of Usability:

i) Non frequent users are allotted TOTP (time based one time password) and they always gets the new OTP when ever user want to access the system.
ii) Frequent user is allotted WTP (weekly time password), so that the user can use the same OTP for One week from the time of last validated OTP, so no need to generate OTP for every time the user access the system this reduces the workload on the system.

Administrator of the organization create the user profiles and roles, according to the roles admin will select the type of usability i.e. either frequent user (WTP) or non frequent user (TOTP). After making the choice OTP/WTP is sent to the users email id and phone number. This OTP is used by user to sign in. Both emails an phone OTPs are required for authentication of user. By validating the OTP of email and SMS we are enhancing the privacy of the user and providing security from intruders. The process of sign up for cloud service is as shown in figure 2.

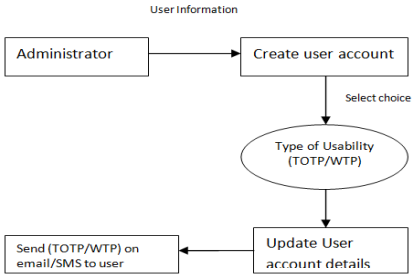

Fig 2: User sign up for cloud service

4.2 Accessing Cloud Application

To access cloud services the users need to sign in using two factor authentications. i.e., by using user credentials and OTP/WTP. Every time user wants to enter the cloud system, a request is generated to cloud regarding the access. The application accepts the requests and verifies the credentials, OTP/WTP with user database and proceeds. Any discrepancy regarding the mismatch of credentials and OTP/WTP, user is navigated to sign in page. If the OTP/WTP doesn't match, the application generates new OTP and the process continues until the credentials and OTP are matched with the user database. The process of accessing the cloud application is shown in the figure 3.

4.3 Periodic generation of OTP/ WTP

As mentioned earlier how OTP/WTP are used in two factor authentication, we have introduced a periodic check of user credentials by generating OTP for every 30 mins for non frequent user and every one week for frequent users.

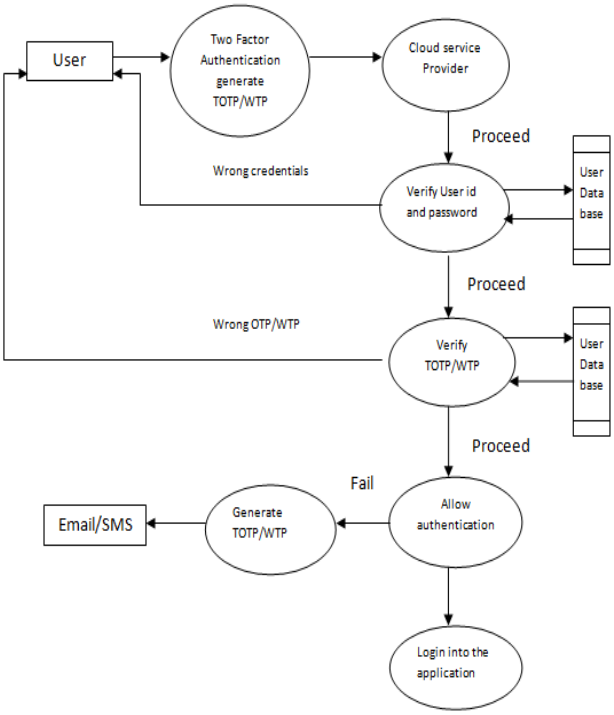

Fig 3: User accessing cloud application

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

The session time is tracked for every successful sign up of user in to the application and periodically the system will generate OTP to check whether the user who is using the application is a valid user or not. If the entered the OTP is a valid, session will be updated and user is continued to use the application. If the OTP is not matched then the user is logged out from the system and navigates to the sign up page. The process of periodic checking of User is shown in figure 4. This periodic check will assure that the user who is using the application is a valid user and not an intruder.

5. EXPERIMENTAL RESULTS

We have built a CRM application - Pharma DISCO Service cloud with secure authentication to test this model. Administrator of the organization create the accounts for all the users of various roles in the application. Ever user gets a unique Id (DISCO _Id) on their respective e-mail. Considering one scenario where customer representative will create a lead when he/she approaches a pharmaceutical vendor and generates a VendorId in Vendor services. Representative will enter the purchase indent order and give one ID of the Vendor as PIOId to the vendor. Vendor will log into the application to view / edit/ update the purchase indent order he need to go through the two-factor authentication. Vendor will log in to the application with his VendorId and the OTP or WTP is required to login into the application. Once the OTP is matched the vendor can logs into the Pharma DISCO application and can see his details. If the vendor is using the application for more than 1 hour, again an OTP will be generated to verify whether the user who is operating the application is a valid user or not. Once the OTP is matched the user can resume the session from where he left. If OTP is not matched the user will be logout from the application and general authentication procedure is followed to access the application again.

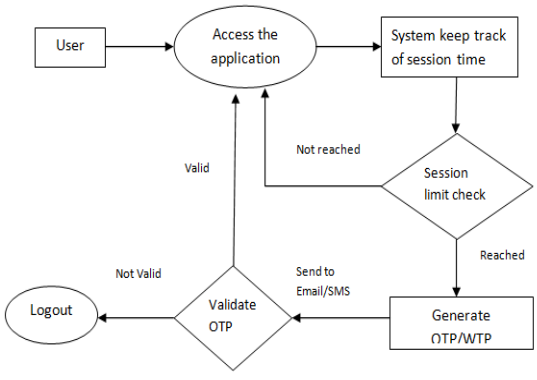

Fig 4: Periodic Generation of OTP/WTP

In case of representative, the OTP generation varies. Administrator will change the TOTP to WTP so that representative can use the application without signing for more than a week. Once the session is reached the limit of one week, automatically OTP is generated and user needs to validate his authentication by entering the new OTP.

6. CONCLUSION AND FUTURE SCOPE

Privacy of user's data and organization's data is the biggest challenge in Cloud environment. By using TOTP/ WTP in salesforce.com, privacy is maintained by periodically checking whether the user is a valid or not. Whenever the session time reaches a particular limit i.e. being set by the administrator OTP is sent to the user to validate him/her self by entering the text/number sent by the OTP server. This will make sure that the valid user is operating the cloud application. Similarly WTP provides the privacy for the frequent users, and to avoid multiple TOTP while using the cloud system. In future, this proposed model could be enhanced by taking the bio metric or face recognition techniques to secure cloud computing environment.

REFERENCES

[1] D Jayalatchumy, P Ramkumar, and D Kadhirvelu, "Preserving Privacy through Data Control in a Cloud Computing Architecture using Discretion Algorithm", Third International Conference on Emerging Trends in Engineering and Technology, 2010 IEEE, DOI 10.1109/ICETET.2010.103.
[2] W, Jian; Y, Wang; J, Shuo and Le,Jiajin; "Providing Privacy Preserving in cloud computing", 2009 International Conference on Test and Measurement, 2009 IEEE, ICTM 2009.
[3] Wang, B.; Baochun; Wang, H. L. 2012 Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, IEEE Fifth International Conference on Cloud Computing, 2012 IEEE, DOI 10.1109/CLOUD.2012.46.
[4] Syed Mujib Rahaman, Mohammad Farhatullah "A framework for preserving privacy in cloud computing with user service dependent identity" , ICACCI '12: International Conference on Advances in Computing, Communications and Informatics, ACM 2012.
[5] Syed, M. R.; and F, Mohammad; "PccP: A Model for Preserving Cloud Computing Privacy", 2012 International Conference on Data Science & Engineering (ICDSE), 2012 IEEE.
[6] Delina Beh Mei Yin, et.al, "Electronic Door Access Control using MyAccess Two-Factor Authentication Scheme featuring Near-Field Communication and Eigenface-based Face Recognition using Principal Component Analysis" , 10th International Conference on Ubiquitous Information Management and Communication, ACM January 2016.
[7] Thanasis Petsas, et.al, "Two-factor authentication: is the world ready?: quantifying 2FA adoption", Eighth European Workshop on System Security,ACM April 2015 EuroSec '15.
[8] Website:https://en.wikipedia.org/wiki/One-time_password.
[9] Ding Wang, Qianchen Gu, Haibo Cheng, Ping Wang "The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes", 11th ACM on Asia Conference on Computer and Communications Security,ACM May 2016 ASIA CCS '16.
[10] Dr. Sandeep Sharma, Navdeep Kaur Khiva," Secure Cloud Architecture for Preserving Privacy in Cloud Computing using OTP/WTP", GJCST, 2013.

BIOGRAPHIES

Pranayanath Reddy A B.Tech, M.Tech ,(Ph.D.) is a Research Scholar under the Guidance of Dr.G.Manoj Someswar. He did his M.Tech degree in Software Engineering and B.Tech degree in Computer Science and Information Technology. Presently, he is working as an Assistant Professor in CS Department at Alliance University,

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Bengaluru, Karnataka, India. His research interests include Cloud Computing, Software Engineering, Software Testing, and Database Management Systems.

Dr.G.Manoj Someswar B.Tech., M.S.(USA), M.C.A., Ph.D. is having over 30 years of relevant work experience in Academic Administration, General Administration, Academics, Teaching, Industry, Consultancy, Research and Software Development. At present, he is working as Director General & Scientist'G', Global Research Academy, Hyderabad, Telangana, India and utilizing his research skills, teaching skills, knowledge, experience and expertise to achieve the goals and objectives of the Research Organization in the fullest perspective. He has attended more than 100 national and international conferences, seminars and workshops both in India & Abroad. He has more than 250 research paper publications to his credit both in national and international journals. He is also having to his credit more than 100 research articles and paper presentations which are accepted in national and international conference proceedings both in India and Abroad. He received National Awards like Rajiv Gandhi Vidya Gold Medal Award for Excellence in the field of Education and Rashtriya Vidya Gaurav Gold Medal Award for Remarkable Achievements in the field of Education, National Award for Research Excellence, Sardar Patel International Award for Academic Leadership, Distinguished Professor Award from Computer Society of India.