Global Journal of Computer Science and Technology
Cloud and Distributed
Volume 13 Issue 3 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Secure Cloud Architecture for Preserving Privacy in Cloud Computing using OTP/WTP

By Dr. Sandeep Sharma & Navdeep Kaur Khiva

Pune University, India

Abstract - The main objective of the proposed architecture is preserving the privacy of the information ensuring that this information cannot be misused. In this paper we have proposed secure cloud architecture to address the user privacy problem in a cloud. By using OTP and WTP in cloud computing system, our proposed architecture achieves better goal of preserving the privacy of a user.

GJCST-B Classification : C.2.4

Secure Cloud Architecture for Preserving Privacy in Cloud Computing using OTP/WTP

Dr. Sandeep Sharma [α] & Navdeep Kaur Khiva [σ]

Abstract - The main objective of the proposed architecture is preserving the privacy of the information ensuring that this information cannot be misused. In this paper we have proposed secure cloud architecture to address the user privacy problem in a cloud. By using OTP and WTP in cloud computing system, our proposed architecture achieves better goal of preserving the privacy of a user.

I. Introduction

Cloud computing is an On-demand self-service Internet infrastructure where a customer can pay and use only what is needed, managed by an API. The SP plays an active role in transmitting information across the cloud. Privacy for the information through authentication is being considered important. [5]

People can only enjoy the full benefits of Cloud computing if there can address the very real privacy and security concerns that come along with storing sensitive personal information in databases and software scattered around the Internet. There are many service provider in the internet, can call each service as a cloud, each cloud service will exchange data with other cloud, so when the data is exchanged between the clouds, there exist the problem of disclosure of privacy. So the privacy disclosure problem about individual or company is inevitably exposed when releasing or sharing data in the cloud service. Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust, and needs to be considered at every phase of design. [6]

Privacy means that the person to be free from all interference. Privacy control allows the person to maintain a degree of intimacy.[2] Privacy is the protection for the truthful use of personal information of cloud user. Privacy breaches may create a lot of troubles to cloud users.

As more and more sensitive data are shared and stored in the cloud, data security and privacy have been considered as a thorniest problem that may impede the growth of cloud computing. Since all the resources are provided over the Internet, the cloud becomes a single point of access for all the users. The different scenarios are:

a) From the perspective of Individuals connecting to the cloud: [4]

Maximizing individual user control, creating anonymous services for individual users, creating facilities for the use of multiple identities and limiting identity information and authentication to high level transactions are the privacy issues which have to be guaranteed for an individual to feel that the privacy of information submitted to the cloud is ensured.

b) From the perspective of Cloud computing service providers: [4]

Providing facilities for maintaining anonymity of personal information, encryption of data if it contains personal information, compartmentalizing data processing and storage, controlling unique identifiers, managing explicitly the privacy and security requirements between the cloud service providers are the major privacy issues from the point of view of the cloud service provider.

II. Earlier Approach

The user might give his/her identity of proof certificate [1] willingly to a person of his/her trust.

- There might be a case where there is a breach of trust. Hence your secure key lies in the unauthorized person.
- There might be a case where proof of identity is stolen.

In both the cases, the IOP is in the unauthorized person and there might be a case of illegal intrusion.

If IOP certificate is with the unauthorized person, it could be misused to any extent which may prove to be harmful. The personal information and data is now available to the intruder and could be accessed at his/her wish. This information or data could be used in an unethical manner which might harm the credibility of the user.

A careful analysis of literature on the variants and methodologies of privacy preserving in cloud computing reveals the following: Some of the variants of privacy problem are yet to be explored. It includes the problems of misuse of the proof of identity (POI) certificate if fallen into unauthorized person. So this leads us to draft out a scheme or method so that if POI certificate is with unauthorized person, he/she cannot take advantage of it by making some changes to sign in process.

Authors α σ : Dept of CSE, GNDU, GT Rd, Off NH1, Amritsar(PB)-143005, India. E-mails : sandeep_gndu@yahoo.com, navdeep07khiva@gmail.com

In a cloud network, once the user has finished with the sign up process, he/she is provided with the POI certificate using which he/she could sign in and access the information as required. But here arises a problem that what would happen if this POI certificate falls in wrong hands. So here comes an objective to make the sign in process secure enough to prevent an intrusion and keeping the sign in process simple enough to the user as per his/her need.

III. Proposed Architecture

The architecture consists of four main components: the third party website, the cloud Service Provider, the User, and the third party database.

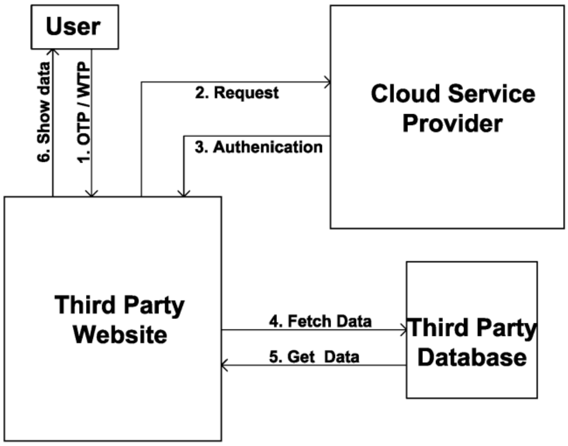

Figure 1 : Proposed Secure Cloud Architecture

An OTP (one-time password) is a password that is valid for only one login session or transaction. WTP (weekly-time password) is a password valid for a week.

a) User Sign up Process

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

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

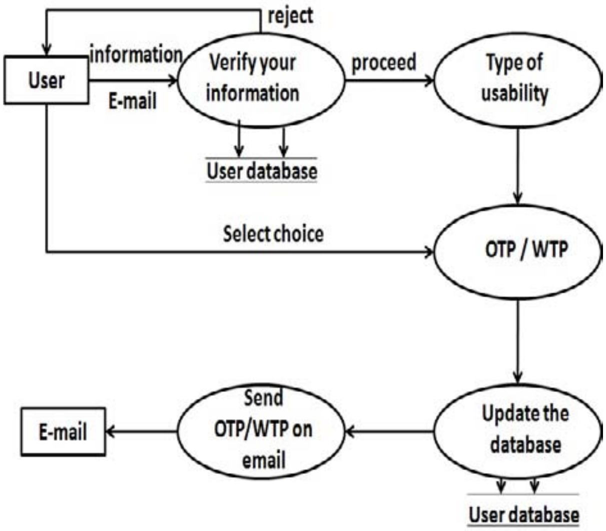

Figure 2 : User Sign Up for Cloud Service

The user sign up process starts with user sign up interface where the user enters its personal and protected information. This information moves for verification to the user database. Once verified, the user proceeds to deciding the type of usability and accordingly the security whether it's an OTP or WTP. The users make their choice depending upon their frequency of sign in and whether to go for OTP or WTP. Once the choice has been made, an OTP/WTP database is updated and their respective OTP/WTP is conveyed securely via E-mail. This password can be used by user to sign in.

b) User Accessing Cloud Services

To access cloud services the users sign in using digital signature or by using OTP/WTP. Request is generated to cloud regarding the access. The CSPs accepts the requests and verifies the certificate and OTP/WTP from user database and proceeds. Any discrepancy regarding the mismatch of certificate and OTP/WTP, user again needs to provide the sign in information.

Once OTP/WTP is verified, they check its validity. If OTP/WTP is valid and if the user is authenticated and then an ok signal is sent to the third party service which allow user to use the service. If authentication fails, a new OTP/WTP is generated and sent to the user through e-mail and mobile, and again make a request to access the CSPs.

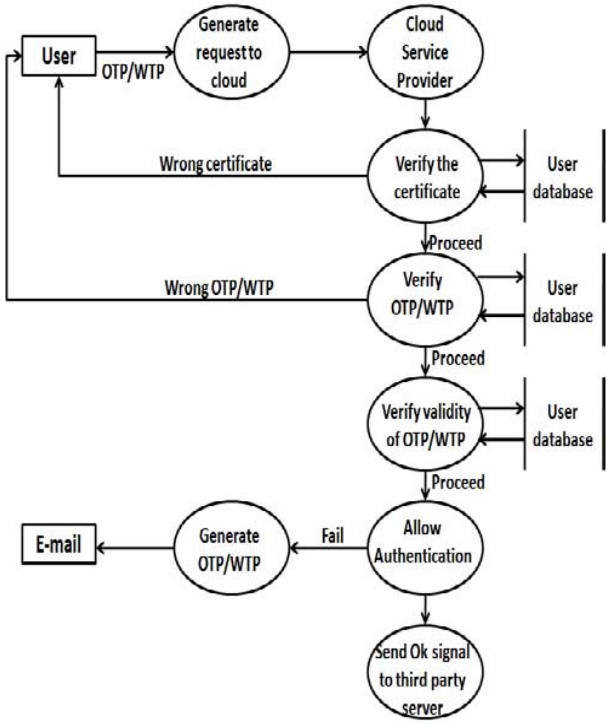

Figure 3 : User accessing cloud services

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work.

c) Hospital Management System

In this scenario, two sites are built: one is Medical Health Service/National Health Service (MHS/NHS) and another is the Laboratory Service (LS).

The actual scenario and its working is explained below:

1. First of all, the patients go to meet the doctor for the treatment. Doctor checks them and asks for some tests which are done by the Laboratory.
2. The patient has to give the personal information to the admin of the NHS so that he/she can add it into the database of NHS and gets the NHSId.
3. Admin logs in and adds the personal information of the patient into the database given by the patient and sends the NHSId to their respective e-mail.
4. Then an employee of the laboratory logs in and adds the patient's tests report into the database of LS. After that an employee of laboratory gives the PatientId (PId) to the patient.
5. Now it's the turn of the patient to generate the OTP/ WTP. Now the patient will sign up in the NHS to get the password to see their tests report. By this the patients gets the password on their respective e-mail.

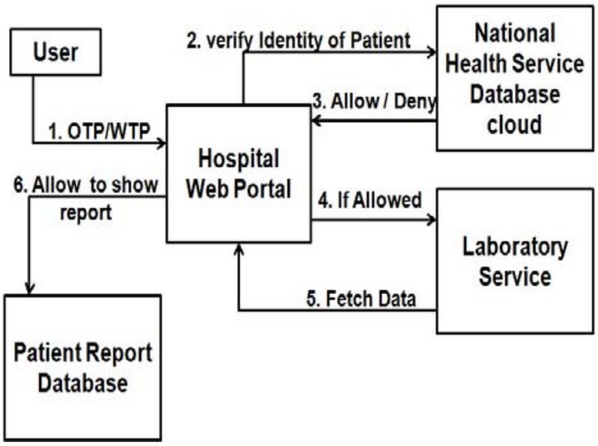

Figure 4 : Hospital Management System

An OTP (one-time password) is a password that is valid for only one login session or transaction.[5] WTP (weekly-time password) is a password valid for a week.

A non frequent user uses OTP and always gets the new password for each access and hence providing security with each access.

Frequent users go for WTP so that the user need not change the password on each access rather weekly.

6. Patient logs in to the LS by entering the NHSId, PId and password and gets the test reports.

IV. Experimental Results

To test this architecture we have built a National Health Service cloud with secure authentication.

As the admin logs in, he will create the clients account and enter his details which were given by the patient and then patient gets the National Health Service Id (NHSId) on their respective e-mail.

The employee of the laboratory then logs into the laboratory service (LS). He will enter the test results of the patient and give one ID of the LS as PatientId (PId) to the patient.

Patient will log in to the National Health Service to generate their type of usability i.e. OTP or WTP. After getting the NHSId, PatientId and the password which was send on mail can logs into the LS and see the test reports.

V. Conclusion and Future Work

Data privacy is one of the biggest challenges in Cloud Computing. By the introduction of the OTP/ WTP password protection schemes, the privacy of the user will now be assured to a great extent. The OTP provides a user new password each time and WTP provides the task for a frequent user to use OTP so he/she would opt for WTP.

In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation.

References Références Referencias

1. Bertino, E.; Paci, F.; Ferrini, R. 2009 Privacy-preserving Digital Identity Management for Cloud Computing, IEEE Computer Society Technical Committee on Data Engineering.
2. 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.
3. Yassin, A. A.; Jin, H.; Ibrahim, A.; Qiang, W.; Zou, D. 2012. A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing, IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum, 2012 IEEE, DOI 10.1109/IPDPSW.2012.148.
4. Syed, M. R.; and F, Mohammad; “PccP: A Model for Preserving Cloud Computing Privacy”, 2012 International Conference on Data Science & Engineering (ICDSE), 2012 IEEE.
5. 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.
6. 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.
7. Wikipedia-One-time_password