Cloud Authentication Method Based on Multiple passwords Technique  
Alaa Al-Hamami, Rafal Al-Khashab  
College of Computer Sciences & Informatics, Amman Arab University  
Alaa.hamami@yahoo.com, rafal_alkashab@yahoo.com

ABSTRACT
The concept of cloud computing is a model for sharing resources like servers, storage, network, and application. Cloud computing made services are available for customers in open environment. Thus, it is important to provide authentication to communicate through cloud. Cloud users feeling that their data will be secured and available to them.  
In this paper, the researcher designed successful method for providing authentication to the cloud; this method used multiple password technique by generating new password every log-in instead of using single password. In other words, user generated multiple passwords from one password to provide more security for the user, application, and cloud. A third party is responsible for checking user authorization; after the checking is successful, it gives identification to the user for safety access to the cloud. The proposed method has been implemented on the personal cloud due to its basic structure for the other clouds deployment. The results are encouraging due to the usage of multiple passwords from one seed.

Keywords: Authentication, Password, Identification, Personal Cloud, and Cloud Computing

1. Introduction

Cloud concept is not a new idea in internet area; it is a combination of several concepts from virtualization, distributed application design, grid computing, utility computing and clustering. It is considered a way to increase the capacity of a network without investing in new infrastructure, training new personnel, or licensing new software. The cloud computing is a set of multiple resources, hardware and software, that is available through the internet and managed by the provider. The customers get all or some of these resources according to the used cloud system (Kumar, A., et al, 2012).

The organization or individual user pays for the access of cloud computing services; these services are present to customer according to the client need. In other words, the customers can satisfy their requirements and pay only for the actual used without needing any details about process. Cloud computing allows providers to develop, deploy and run applications that can easily grow
in capacity, work rapidly, and never fail without any concerns on the properties and the locations of the underlying infrastructures (Rawat, S.S, & Sharma, N., 2012).

Cloud computing technology is deployed over different types of delivery model based on the characteristics and purpose of it, such as: Public cloud, where the resources could make available to multiple customers by a service provider through internet. Private cloud, here the resources could provision for exclusive use by a single organization. Community Cloud, the resources could provision for exclusive use to specified organizations, and managed by one or more of the organization in the community. Virtual Private Cloud, the resources could be provisioned for exclusive use in specific portion of public cloud infrastructure. Personal Cloud, the resources could be provisioned for personal use for helping any user to access the digital files in anywhere by any device. Hybrid Cloud, the resources in this could combine of two or more from deployment model (Boampong, P., & Wahsheh, L., 2012, and Ardissono.L., et al, 2012).

Cloud computing has several characteristics to make the user adapting to this new technology, such as: Reducing the Running Time & Responding Time, Reducing the Cost, Independence Device and Location, Resource Pooling, and Reliability. Also, cloud computing have the following features: Performance and Maintenance, Back – Up Facility, Reduces the Risks of Theft, Availability and Collaboration, and finally, Elasticity and Scalability (Kumar, A., et al, 2012).

2. Security Issue in Cloud Computing

The security issue is considered one of the main concepts in every growing field. The security problem of cloud computing is a hot research topic. Although cloud computing has many benefits, it is still not safe from threats and other attacks that prevent the users from trusted it.

In most cases, the providers must ensure that their infrastructure is secure and their clients’ data and applications are protected. Thus before migration to the cloud, one should focus on some important attacks on cloud computing such as: Denial of Service (DoS), Zombie, Backdoor Channel, Side Channel, Man-in-the-Middle, Phishing, and Authentication Attacks (Munir, K., & Palaniappan, S., 2013 and Global Knowledge Training LLC 2010).

In this paper, we focused on authentication attacks to show users that their information is secured and they have authority to know who access their information in the cloud. The personal cloud will be determined as cloud deployment model.

3. Related Work

The security technologies that developed to enhance cloud computing security have been explained in (Yu, H., et al, 2012). Cisco Secure Data Center Framework provided multiple security
layers to enhance cloud computing security. (Sumter, L., 2010) identifying whether there is a need for some type of security capture device/measure on the cloud, which will allow users to know whether their information is secure and safe without comprising by threats and attacks. A characterization of Dropbox, the leading solution in personal cloud storage in the datasets has been presented by (Drago, I., et al, 2012).

Therefore in this paper, we focused on a method to check the user authority, and present method to the users for secure access to the own data and application in the cloud.

4. The proposed method

The security is reduced when users reuse the same password for different clouds or for different log-in at the same cloud, at the same time; we know that people generally have difficulty in remembering multiple passwords. In this research, we will propose more efficient security method for cloud computing that helps users to freely choose single password for multiple uses in the cloud. The process in this research is generating new password every log-in instead of single password. In other words, it is generating multiple passwords from one password.

The proposed model includes three main components:
1- Cloud user: - the individual user can store his/her data and applications in the cloud, also can access them from anywhere and anytime.
2- Third party: - A person who manages cloud server and provide authentication method between user and cloud.
3- Cloud application: - It is the application that allows user to enter cloud computing and have full control over cloud.

The proposed framework of authentication model is designed to prove and generate authentication between user and cloud, all stages in this framework are accrued outside the cloud computing. The authentication model includes two procedures, as shown in Figure (1):-

![Fig.1. The Proposed model](image-url)
1- **Provided authentication:**

This procedure is used when the user is using cloud computing for the first time; it registers its own account on cloud and choosing the deployment cloud depending on the characteristics needed from the user.

When the user is using cloud for the first time, he/she should enter user-name, password, and email and choose an image that represents the user in cloud, the method used this image to increase authentication in the next procedure. The method implements the following algorithm to encrypt password and image then stored it in the database, this encryption to protect the password and image from possible intrusion that may happen in databases.

**Algorithm: proved-authentication:**

```
// - Input: - User Information.

- The function of this algorithm is to use the password and image of the registered user in input and result encryption password and image in output.
- Output: - password and image encrypted //

**Step1:** Start Algorithm.

**Step2:** the user will register all desired information (name, password, email and selected personal image from personal computer gallery).

**Step3:** Encrypt password depending on character position. If the position is even, then increase ASCII of character by 4. Else, increase ASCII of character by 3.

**Step4:** Encrypt personal image by combine between them.

**Step5:** Save the encrypted password and image in the database.

**Step6:** End Algorithm.

2- **Generate Authentication:**

This procedure is used when the user wants access to cloud computing and dealing with own data, the model will implement two algorithms:

- **Generate password algorithm:**

  To increase the system security, the user changes password every time when enters into the system. At the same time, it is difficult for the user to remember all these words. Therefore, the system generates a new password from original password each time the user enters to the
system, by the following algorithm, then sends this password to the user email for using it in access to computing:-

**Algorithm: Generate Password:-**

// - Input: - password.

- The function of this algorithm is to use the original password that is registered by user in input and new password in output.
- Counter from (1 to 100), register the number of times a user log-in to the cloud computing
- Output:- password //

**Step1:** Start Algorithm

**Step2:** The proposed model gets on the user password, counter and length of them.

**Step3:** Check the counter is greater than (100), then make counter =0. Else, Continue.

**Step4:** Encrypt password by two steps:-

**Step4-1:** Combine between each character from password with counter by (XOR) operation.

**Step4-2:** multiplication result from previous step with second system.

**Step5:** Send encrypted password to user email.

**Step6:** End Algorithm

➢ **Personal Image Algorithm:-**

After passing the first stage of the generation authentication, the model displays the personal image of user with a different set of images, and these images change with each entry as well as the order of it is changing, according to the following algorithm and the user choose the correct image of him/her to be able to access cloud computing:-

**Algorithm: Personal Image:-**

// - Input: - images.

- The function of this algorithm is displayed multiple images for the user, and the user will choose the correct image.
- Used minute system and counter of images in cloud table.
- Output:- images //
Step1: Start Algorithm

Step2: The proposed model gets on the personal image for the user.

Step3: The proposed model gets on the different five images from cloud table.

Step4: The model displays six images to the user, and the user choose one of these images.

Step5: If the chosen image is correct, the model allowed the user to use the cloud application. Else, the model prevents the user from used the cloud application.

Step6: End Algorithm

5. Conclusion and Future Scope

The model focused on two points, the first one is to prove authentication through image as determined by user, and the second point is to generate authentication through using multiple password technique in the cloud; it is a new research field which is gaining interest from cloud users because the probability of brute force attack for breaking the password can be reduced when increase generated multiple passwords from single password.

In future, the proposed model suggests two points to provide more trust between user and cloud: the possibility of adding one of the biometric authentication types in addition to the image for more identification of the user, and to provide more security for the generated password, the third party can send the new password to the authorized user by the Mobile phone instead of the email.

Reference


