Authentication Cloud Computing using chunks of images

Muna Kheder Al-Naamee[1,a]

[1]Department of Computer Science, University of Technology, Baghdad, Iraq
[a]munaiq.nfama@uotechnology.edu.iq

ISSN: 2231-8852

ABSTRACT
Data protecting cloud computing in nowadays become more important to prevent data from unauthorized access and stolen. Many techniques are used to improve authentication methods for achieving high security in cloud computing. For the authorization to access the cloud there are many existing techniques: textual password, biometrics, token based, recognition based. Each one of these techniques has its own advantages and disadvantages. This paper presents an improved way to implement a graphical password which contains a selection of chunks of images which are used to build password to provide a strong authentication. Hence, the proposed technique is used a chunks of images to provide strong password authentication.

***Keywords:* cloud computing, cloud security, authentication techniques, chunk- image password generation**

1. Introduction

Security in cloud computing means, the data stored safely and authenticated to access. In cloud computing various security algorithms are used to store the data in a secure and safe manner. Different methods and different techniques are used to authenticate and to access the data securely (Monjur A., Mohammad A., 2014, Shenbagam, C.Namasivayam, 2014, Daphna, Scott, 2004, Mr. Gayatri D., et al, 2014). This paper explains a new method to produce a password to authenticate accessing data in a cloud.

There are many authentication techniques were introduced such as Graphical password, Text password, Biometric authentication, etc. Graphical password provide a programming alternative traditional alphanumeric password. The basic idea of graphical password is that it is easy to remember than word and decreases the chance to choose assure password (Pawar Poonam A, et al, 2015). So to overcome the problems of authentication methods, an idea of graphical password was introduced by Greg Blonder 1996. Partha Pratim Ray added that graphical password use pictures instead of textual password. At the first contact with cloud provider must password based authentication used, where user presents user ID and a password to the sequence authentication technique based on graphical password. The analysis of graphical password uses pictures are most effective than textual password (Wazir Zada Khan, et al, 2011).

Authentication with graphical password where user choosing image or hotspots of image in virtual environment to create a password (M. Arunmozhi, et al, 2015). In proposed schema, we introduced a chunks graphical password. The chunks graphical password is constructed by observing the actions of the user to construct a password by a sequence of selections for sub parts of images. This scheme is giving user a freedom of selecting from images to construct one password for one user.

The rest of the paper is structured as follows. In Section 2, the related works relevant to this research work is reported. In Section 3, we explain the details steps of the proposed method. Conclusion and future work directions are explained in the final section, 4.

2. Related Works

There are two types of Authentication schemes are available, Recall based and Recognition based. In first one: the user needs to recall or remember the password that created before. In second technique: the user needs to identify, recognize password created before. Many of authentication techniques depend on one of these two types and the other techniques used a combination of them. Secure Authentication with 3D Password, is used a combination of both recall-based (textual password) & recognition based (graphical password, biometrics). This will give a multifactor & multi password authentication scheme (Vishal Kolhe, et al, 2013). Another developed a graphical based authentication mechanism by using puzzle strategy, where the cloud user starts moving the puzzled image to form complete puzzle, then send the puzzle to validate by the provider and return back the authentication for access (Sulochana. V, Parimelazhagan.R, 2013). Kiran and Ragav proposed merges persuasive cued click points on images and password guessing resistant protocol (graphical passwords). This technique gives a large password space over alphanumeric passwords (Kiran T.S, Ragav.R, 2013).

3. Proposed Method

The basic article of authentication is password authentication which happens between cloud user and cloud service provider. If someone wants to store or retrieve data stored in the cloud he should enter the correct graphical password. Only authorized user can access and read the data in the cloud. Developing graphical password authentication system with chunks of images to increase the remembrance of the password. The system consists of chunks in which user select and change the image block for log on process. This article proposes graphical password system with chunks. Chunks of images are arranged in rows and columns, cloud user moves the chunks image to form the complete chunk graphical password and it's solving time and sequence of image block is stored and validated by local server and the cloud user gets authenticated and then he can start accessing the cloud services.

In this paper the chunks password authentication technique generates passwords from multi-pieces and then concatenates into one single password. The distinctive features of this technique make the security measures of the cloud computing more strong. Even if intruder is aware of a piece or more of the particular password, it will not be helpful to him to know which part of password this piece represents.

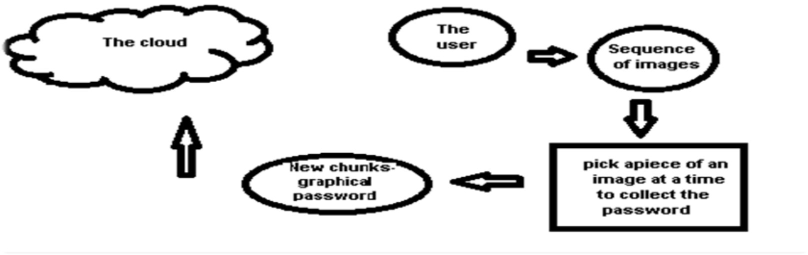
The cloud
The user
Sequence of images
pick apiece of an image at a time to collect the password
New chunks-graphical password

Fig. 1 Data flow diagram

Authentication scheme uses chunks in cloud computing, the user registers himself and solves the chunks (sequence of pieces of images) to produce a password. This sequence of chunks of images is stored in cloud, and then cloud provider give validation and authentication to the user to start accessing the cloud services.

The algorithm used for accessing the cloud as follows:

```
 If the User = New
            The user is register for the first time with:
            ID, password
            Select chunks from series of images
           The user provides authentication for accessing
            Access the cloud
Else
  If the User = Registered
             Enter ID and password
        Select a previous sequence of chunks of images
        Collect the chunks image
        Send the chunks image for authentication
        If the User = Authenticated
        Access the cloud
      Else
            Reject the user authentication
End
```

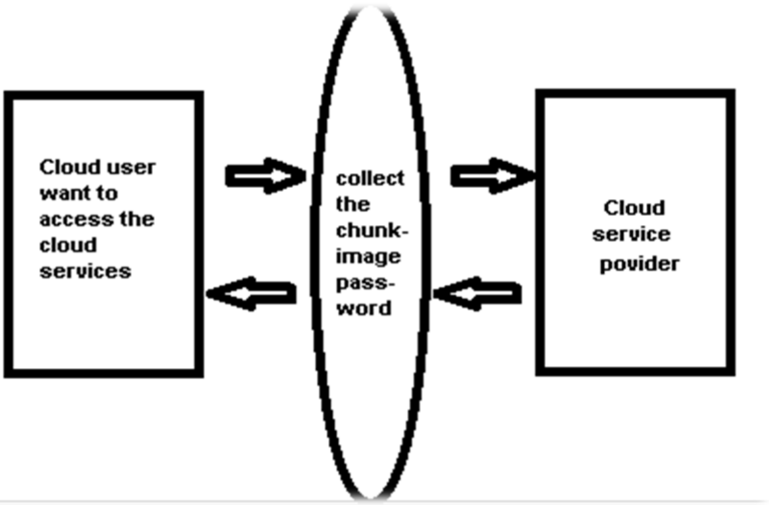
Cloud user want to access the cloud services
collect the chunk-image pass-word
Cloud service povider

Fig. 2 Data flow diagram

To create a chunks image, the user first register himself, need an ID and password to send a request to the cloud provider to enter. If he enter for the first time he need to register , else if he register himself before need only his ID and password to tell the cloud provider that he want to enter to use the cloud services.

After registration, the cloud provider send a sequence of images divided in chunks for each, the user will select sequence of these chunks to create the chunks-image. For registration as new user: the user will choose the size of the chunks image and then select random piece for each space of the chunks image. The user can select each piece more than one time or never select it. The user can leave any piece of the chunks image as empty piece (will be blank). Than the user press login key, now the system will have a sequence of pieces those represent the chunks image which store in the cloud with ID and password of the user. This chunks image will be used for authentication when the user want to login to the cloud for next time.

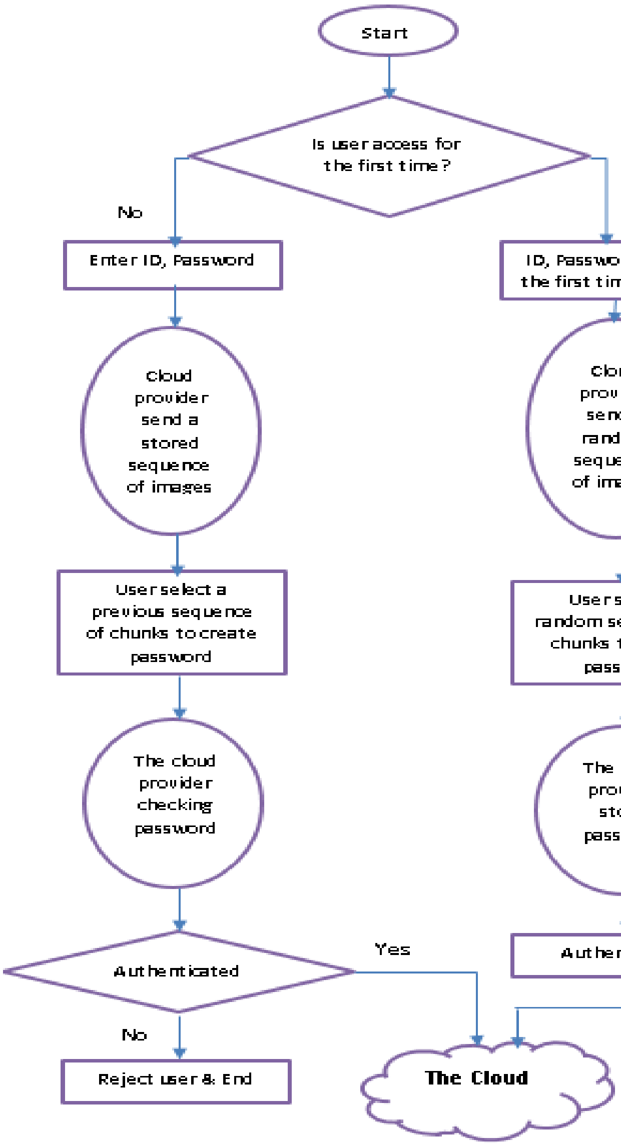
Start
Is user access for the first time?
No
Yes
Enter ID, Password
ID, Password for the first time
Cloud provider send a stored sequence of images
Cloud provider send a random sequence of images
User select a previous sequence of chunks to create password
User select a random sequence of chunks to create password
The cloud provider checking password
The cloud provider store password
Authenticated
Yes
Authenticated
No
Reject user & End
The Cloud

Fig. 3 Flowchart for proposed system

If the user registered before: enter his ID and password , the cloud provider see if this user registered before, than give him authentication to continue and send back the previous sequence of images to create the chunks-image as before. After the user finish his selection will press login key, now the cloud provider will compare the chunks-image with one stored before, if they are same, give him authentication to enter the cloud, else he will be rejected.

Table1. Number of trials

matrix (M[i,j]) that represent the password size					no. of pieces in each password					the number of attempts, for each size of password if the user used full size of that password			
M[1,1]	M[1,2]	M[1,3]	M[1,4]	→	1	2	3	4	→	1	2	6	24
M[2,1]	M[2,2]	M[2,3]	M[2,4]	→	2	4	6	8	→	2	24	720	40320
M[3,1]	M[3,2]	M[3,3]	M[3,4]	→	3	6	9	12	→	6	720	362880	479001600
M[4,1]	M[4,2]	M[4,3]	M[4,4]	→	4	8	12	16	→	24	40320	479001600	2.09228E+13

Table 1 represents the number of attempts needs to reach to the correct arrangement of chunks to collect the password. This technique give the user the ability to select all the chunks, each one represent a chunk from different image or he can repeat choosing the same chunk more than one time or he can leave any piece of the password with empty chunk (its value is zero). For example if the graphical password with size of 1*4 and one or more chunk will be repeated, then number of trials as follows: 4! +3! +2! +1! =33 attempts instead of 24 attempts.

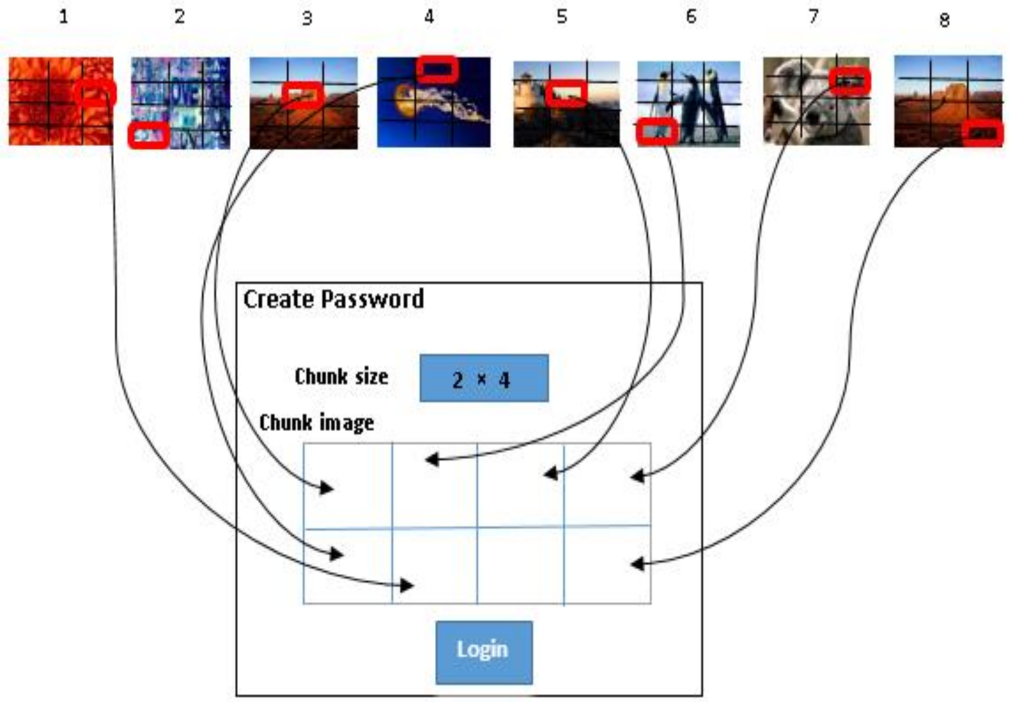

Fig. 4 Chunks – graphical password screenshot

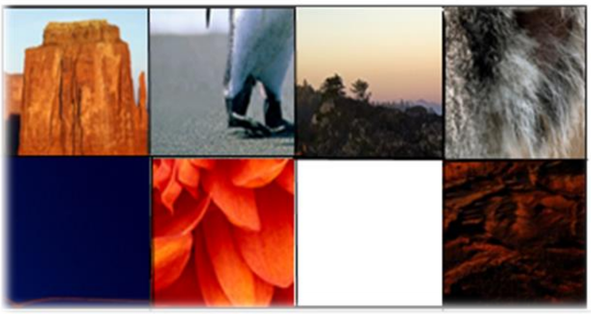

Fig. 5 Chunks – graphical password

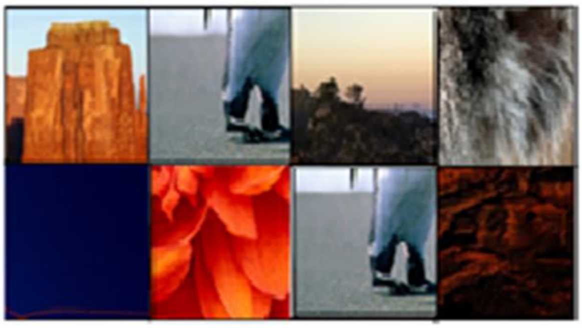

Fig. 6 Chunks – graphical with repeated chunk

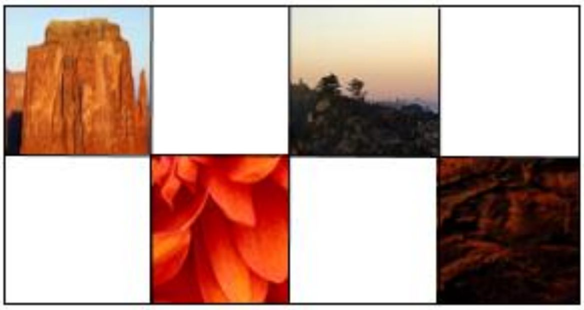

Fig. 7 Chunks – graphical password with one or more empty chunk

All the existing techniques have its own advantages and dis advantages, in new technique give any cloud computing system more security against thwarts. It's easy to implement, need less time to create password and less time for execution than multilevel authentication or 3D, 4D, … password authentication, easy to remember, and has a wide range of selection (no limit of chunks). This technique will be stronger against thwarts like shoulder attack (An attacker can pick up password by direct observation or by the individual authentication session recording) (Arash Habibi Lashkari, 2009), dictionary attack where the attacker creates a dictionary of popular spots of image or points which can attract the user (Farnaz Towhidi, et al, 2011). So new proposed technique will give more flexibility and complexity which are need in nowadays in cloud computing.

4. Conclusions and Future Works

Cloud computing provides variety of services like software applications, hardware devices, and data storage. To provide secured services to the user, it's important to make the dealing between the user and the cloud provider based on authentication. Authentication is a weak point and is frequently targeted by attackers. There are many different ways to authenticate users. Most user today still use simple username and password type of knowledge-based authentication, except some financial institutions which have develop various forms of authentication depends on textual password , graphical password , or use both of them to make it a bit more difficult for popular phishing attacks. The chunks- image password generation technique are used in this research for authentication. The chunks-image password is generated by choosing a number of chunks of a series of images and collecting the chunks password as input for authentication. Using this technique will reduce the probability of thwarting Shoulder attack, brute force attack and dictionary attacks for breaking the password. For further work we can encrypt the chunks-image password before transmit to the cloud provider for more security.

References:

Monjur Ahmed, Mohammad Ashraf Hossain. (2014). Cloud Computing and Security Issues in the Cloud. *International Journal of Network Security & Its Applications* (*IJNSA*), vol.6, no.(1), (2014), pp. 25- 36.

Shenbagam, C. Namasivayam. (2014). 4 Level Authentication Security in Cloud Computing. *International Journal of Innovative Research in Computer and Communication Engineering*, vol.2, no. (1), pp. 304-309.

Daphna Weinshall, Scott Kirkpatrick. (2004). Passwords you'll never forget, but can't recall. *In the CHI 2004 International Conference on Human Factors in Computing Systems*, Vienna, Austria, 24- 29- April- 2004, pp. 1399-1402.

Ms. Gayatri Dhavale, Rajnish Kumar Baranwal, Kapil Nagare, S.N. zaware. (2014). 3-D (Dimensional) security in Cloud Computing. *International Journal of Computer Science and Information Technology Research*, vol. 2, no. (2), pp. 47-52.

Pawar Poonam A, Gayake Nalini B, Mane Kalpana T, Mudpe Ashwini M. (2015). Graphical Password Authentication with Cloud Securing Method. *International Journal of Multidisciplinary Research and Development*, vol. (2), no. (3), pp. 763-768.

Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang. (2011). A Graphical Password Based System for Small Mobile Devices. *International Journal of Computer Science Issues,* (*IJCSI*), vol. 8, issue (5), no. (2), pp. 145 – 154.

M.Arunmozhi, V. Gomathi, K. Prem Kumar, E.meera, K.Priyanka, and R. Ramachandiran. (2015). Two Level Security with Image Hotspots and Hidden Patterns. *In the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET),* Unnao, India, 6-7- March- 2015.

Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod. (2013). Secure Authentication with 3D Password. *International Journal of Engineering Science and Innovative Technology* (*IJESIT*), vol. 2, issue (2). pp. 99 – 105.

Sulochana.V, Parimelazhagan.R. (2013). A Puzzle Based Authentication Scheme for Cloud Computing. *International Journal of Computer Trends and Technology (IJCTT)*, vol. 6, no. (4), pp. 210 – 213.

Kiran Babu T.S, Ragav Krishna.R . (2013). Protection against Online Password Guessing Attacks by Using Graphicals Passwords. *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*), vol. (3), issue (7), pp. 185 – 187.

Arash Habibi Lashkari , Samaneh Farmand , Omar Zakaria and Rosli Saleh. (2009). Shoulder Surfing attack in graphical password Authentication. *International Journal of Computer Science and Information Security*, (*IJCSIS*), vol. 6, no. (2), pp. 145 – 154.

Farnaz Towhidi, Azizah Abdul Manaf, Salwani Mohd Daud, Arash Habibi Lashkari. (2011). The Knowledge Based Authentication Attacks. *In the 2011 International Conference On Security & Management*, 18- 21- July, Las Vegas, Nevada, USA, pp. 1-5.