Implementation of Chunks of Image Password in Cloud Computing System

V. Sulochana

Assistant Professor, Kathir College of Arts and Science, Coimbatore, Tamil Nadu, India
Email: sathvika_2016@yahoo.com

Abstract - **This article proposed a graphical password authentication which uses chunks of images to overcome the loopholes present in the traditional authentication methods. The graphical password contains a selection of chunks of images which creates password for authenticating cloud users for accessing cloud services. The article includes the details of chunks of images authentication, algorithm and implementation of chunk of images.**
Keywords: **Cloud Computing, Cloud Computing Security, Chunks of Image Password Generation, Brute Force Attacks**

I. INTRODUCTION

Cloud computing is adoptable technology for many organizations with its dynamic scalability and usage of virtualized resources as a service through the internet. To utilize the cloud services by authorized customer, it is necessary to have secure authentication system. The most common authentication system is text password which is easy to break and vulnerable to dictionary or brute force attacks [7]. To overcome the problem of textual password, an idea of graphical password was introduced by Greg Blonder [G. Blonder, Graphical Passwords, United States Patent 555996 1(1996)]. In graphical password human beings have the ability to remember faces of people, places visited and things seen for a longer duration which make user friendly and increases the level of security[12]. Phad Sunil [3] presented graphical security by means of image password. First method depends on selection of username and images as password. Second method is grid algorithm, Third method is color intensity algorithm, and Fourth method is chameleon for graphical password authentication. Muna Kheder Al- Naamee [2] designed graphical password which contains a selection of chunks of images which used to build password to provide a strong authentication.

Sangore [6] proposed a new image password scheme; user can give password in combination of images and secret pattern. This scheme combines recognition base technique and secret code (alphanumeric) password, recall based technique and secret code (alphanumeric) password or recognition based technique and recalls based technique removes the problem of mouse logger and shoulder surfing. Utkarsha Padhye [11] presented a new security primitive based on hard AI problems, this system is named as Captcha as graphical passwords (CaRP). CaRP symbolize a number of security problems together, such as online guessing attacks, relay attacks, and shoulder-surfing attacks. Sulochana .V [9] presented secured authentication system

by using sequence level authentication technique which creates/authenticates the password in sequence levels to access the cloud services.

Ramandeep Kaur[5] proposed a technique using one level double trap image based authentication for the login protection in cloud platforms on mobile devices. The one level authentication scheme consists of various small images, which are made of single numerical or alphabetical characters each, in 3x3 point grid formation. The second level password is a 9 clue points grid based password scheme for pattern passwords. Anitha [1] proposed system combines the existing cued click point techniques with the persuasive feature to influence user choice along with image steganography techniques, encouraging user to select more random click point which is difficult to guess. Image steganography, the art of hiding data within an image is used to improve the security of the authentication system. Textual passwords are stored within the images using the steganography techniques. Ramandeep Kaur [4] proposed circular point model where the points are placed on the circle and the images are drawn on the given points. The user has to input the graphical pattern by joining the images with each other in the certain sequence. Sulochana.V[8] presented puzzle based authentication scheme in which cloud user registers and solves the puzzle, puzzle solving time and sequence of image block is stored and validated by local server and cloud user get authenticated and start accessing the services.

The proposed authentication process consists of chunks of images in which cloud user select and change the image block for accessing cloud services. The chunks of images are arranged in rows and column, cloud user moves chunk image to form the complete chunk graphical password which is stored and validated by cloud provider. Cloud user gets authenticated start accessing the cloud services. This graphical password authentication generates passwords from multipieces of images for authenticating the cloud user. This authentication will reduce the probability of thwarting shoulder attack, brute force attack and dictionary attack for breaking the password.

II. DESIGN OF CHUNKS OF IMAGES GRAPHICAL PASSWORD

The graphical password authentication happens between cloud user accessing cloud services and cloud provider.

Fig.1 shows the DFD level 0 for the chunks of images password authentication. Figure 2 shows the DFD level 1 for chunks of images password authentication. This DFD describes detailed flow of graphical password authentication process.
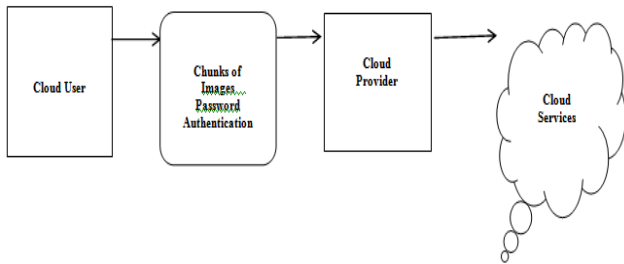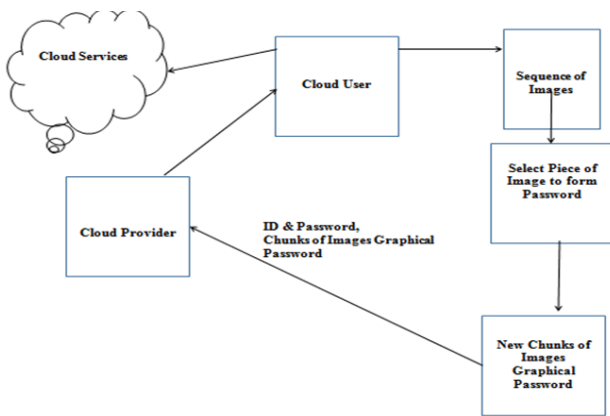

Fig.1 Data Flow Diagram Level 0

Fig.2 Data Flow Diagram Level 1

The algorithm for chunks of images password authentication are given below: if the cloud user is new, registers the ID and Password, new chunks of images password stored in cloud provider. For registered cloud user, ID and password, choosen chunks of images password validated with previous choosen chunks of images password stored in the cloud provider get authenticated start accessing the services else rejected by cloud provider.

Step 1: If (Cloud User=New),

ID & Password are Registered
Cloud Provider Provides Random Sequence of Images
Cloud User select a Random Sequence of Chunks of Images to Create Password
Cloud Provider stores the Chunks of Images Password
Cloud User access the Cloud Services

Else
If (Cloud User=Registered)
        Enters the ID & Password
Cloud User selects Previous Sequence of Chunks of Images
Cloud Provider Validates Chunks of Images Password
Cloud User access the Cloud Services
Else
     Cloud User is Rejected
End.

Step 2: Exit

The next level is implementation of chunks of images graphical password authentication, can be done by using Java, MYSQL, jdk, jsp, Tomcat Server. The sequences of images are splitted using Java imageio Package and images splitted into several chunks. The source image, chunk height, chunk width, rows an d column to be specified by the user. The below is the sample program for splitting Seed.jpg image file into 9 chunks (3 rows and 3 columns). The output of the chunks of image file is shown in Figure 3.

Table I consists of matrix that represent the password size, no of pieces in each password, number of trails for each size of password. The cloud user has 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). The sequences of independent and identical Bernoulli trails are applied to the chunks of images graphical password authentication. The trails are independent with two possible outcomes (1 represent success or 0 represent failure). The geometric probability model for Bernoulli trials. $P(X = x) = p\,q^{x-1}$ Where p-probability of success, $q=1-p$=probability of failure, X=Number of trials until the first success occurs. In this authentication, number of trails is directly proportional to the password size. If the password size increases number of trails increases and vice versa. Based on the above discussion, the use of chunks of images graphical password authentication provides better security for accessing cloud services. Screen shot for chunks of images graphical password authentication are given in Figure 3.
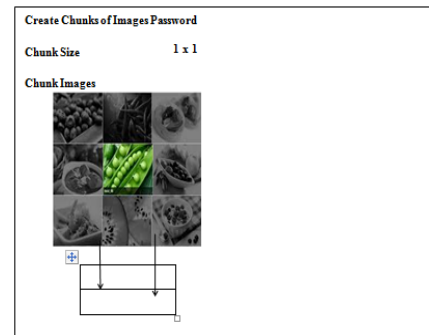

Fig. 3 Chunks of Images-Graphical Password Screen Shot

III. CONCLUSION AND FURTURE ENHANCEMENT

This graphical password provides better security to data and reduces the risk of breaking the cloud user's password from shoulder surfing, eves dropping, brute force attack. This chunk of images authentication made positive impact on the system's usability and provides a much more detailed account of how chunks of images can be useful and memorable in cloud user authentication. It also provides a supplementary dimension in network security. Further it can be improved by encrypting the chunks of images before sending to cloud provider for securing data and information.

TABLE I NUMBER OF TRAILS

Matrix (M(i,j) that represent password Size					No of	Pieces in each password				Number of attempts for each the 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

```java
import javax.imageio.ImageIO;
import java.awt.image.BufferedImage;
import java.io.*;
import java.awt.*;

public class ImageSplitTest {
    public static void main(String[] args) throws IOException {

        File file = new File("Seed.jpg"); // Seed.jpg working directory
        FileInputStream fis = new FileInputStream(file);
        BufferedImage image = ImageIO.read(fis); //reading the image file

        int rows = 3; //values for rows and cols variables
        int cols = 3;
        int chunks = rows * cols;

        int chunkWidth = image.getWidth() / cols; // determines the chunk width and height
        int chunkHeight = image.getHeight() / rows;
        int count = 0;
        BufferedImage imgs[] = new BufferedImage[chunks]; //Image array to hold image chunks
        for (int x = 0; x < rows; x++) {
            for (int y = 0; y < cols; y++) {
                //Initialize the image array with image chunks
                imgs[count] = new BufferedImage(chunkWidth, chunkHeight, image.getType());

                // draws the image chunk
                Graphics2D gr = imgs[count++].createGraphics();
                gr.drawImage(image, 0, 0, chunkWidth, chunkHeight, chunkWidth * y, chunkHeight * x, chunkWidth *
y + chunkWidth, chunkHeight * x + chunkHeight, null);
                gr.dispose();
            }
        }
        System.out.println("Splitting done");

        //writing mini images into image files
        for (int i = 0; i < imgs.length; i++) {
            ImageIO.write(imgs[i], "jpg", new File("img" + i + ".jpg"));
        }
        System.out.println("Mini images created");
    }
}
```

REFERENCES

[1] H.B. Anitha., Adithi Reddy, Irudaya Mary, and Vidya, "Graphical Password Based Authentication System", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol.*5*, pp. 169-171, 2016.

[2] Muna Kheder Al-Naamee, "Authentication Cloud Computing Using Chunks of Images", *Design for Scientific Renaissance,* Vol. 6, pp. 9-16, 2016.

[3] Phad Sunil, Malkar Ganesh, Dhaktode Mayur, Khalane Rakesh, and Prof. P.B.Vikhe, "Review on Graphical Password Authentication by using Cloud", *IJARIIE,* Vol. 2, pp. 186-189, 2016

[4] Ramandeep Kaur, and Amanpreet Kaur, "Multi Factor Graphical Password for Cloud Interface Authentication Security", *International Journal of Computer Applications*, Vol. 125, pp. 32-35, 2015

[5] Ramandeep Kaur, and Amanpreet Kaur, "Enhancing Authentication Schemes for Multi-level Graphical Password in Cloud Environment", *Foundation of Computer Science FCS,* Vol. 5, pp. 12-18, 2016.

[6]   R.B. Sangore., Gaurav Patil, Sagar Ramani, and Sunil Pasare, "Authentication Using Images and Pattern", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 3, pp. 8661-8667, 2014.

[7]   Sayli Chavan, Shardual Gaikwad, Prathama Parab, and Govind Wakure, "Graphical Password Authentication System", *International Journal of Computer Science and Mobile Computing,* Vol. 4, 324-329, 2015.

[8]   V. Sulochana., and Parimelazhagan, "A Puzzle based Authentication Scheme for Cloud Computing", *International Journal of Computer Trends and Technology*, Vol. 6, pp. 210-213, 2013.

[9]   V. Sulochana. And Parimelazhagan, "Implementing Graphical Password and Pattern lock Security Using MVC into the Cloud Computing", *International Journal of Computer Applications*, Vol. 79, pp. 7-10, 2013

[10]   Utkarsha Padhye, Pritesh Kansare, Ketan Chavan, Dhanashri Shinde, and Snehal Mangale, "Image based CAPTCHA as graphical password", Internal *Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, 6652-6659, 2016

[11]   Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, "A Graphical Password Based System for Small Mobile Devices", *International Journal of Computer Science Issues*, Vol. 8, pp. 145-154, 2011.

[12]   [Online] Available at: http://kalanir.blogspot.in/2010/02/how-to-split-image-into-chunks-java.html.