INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REGION BASED GRAPHICAL PASSWORD AUTHENTICATION SCHEME FOR CLOUD COMPUTING

SULOCHANA V[1], PARIMELAZHAGAN R[2]

1. Research Scholar, Karpagam University, Coimbatore
2. Department Of Science & Humanities, Karpagam College of Engineering, Coimbatore

Accepted Date: 08/10/2014; Published Date: 01/11/2014

Abstract: This article presents region based authentication scheme, which is based on the tracking of mouse motions on the image called mouse gestures which is captured through corner detection method for selecting regions in the image by cloud user and validated by local server for accessing cloud services. This article includes graphical survey and details of proposed region based authentication scheme presented along with the architecture, algorithms and implementation.

Keywords: Mouse Gesture, Authentication, Cloud Computing Security

Corresponding Author: MS. SULOCHANA V.

Access Online On:

www.ijpret.com

How to Cite This Article:

Sulochana V, Parimelazhagan R; IJPRET, 2014; Volume 3 (3):46-53

PAPER-QR CODE

INTRODUCTION

Cloud computing is a new technology for complex systems with massive scale services sharing among numerous users. In this new style of computing dynamic scalable resources and virtualized resources can be provided as a service over the internet. Now-a-days, more data of individuals and companies are placed in the cloud and more concerns are given towards the safety and security. Authentication and authorization plays major role in cloud computing security. Cloud authentication is a process of determining whether particular individual or a device should be allowed to access a system or an application or merely an object running in a device of service providers. The conventional authentication mechanisms are based on knowledge, possession and biometrics [2]. The first authentication "textual password scheme" is vulnerable to attackers, and is difficult to remember. Graphical password is an alternative scheme to a text based password[5]. Psychology studies have revealed that the human brain recognizes and recall images than text[6]. Partha Pratim Ray added that graphical password uses pictures instead of textual password because humans can remember pictures more easily than a sequence of characters[7].

Vachaspati designed a novel scheme called **S3PA** which provides the login screen to the user every time the user logs in. Login image consists of a set of characters. Neural network is used for authentication[9]. Abuthaheer's authentication merges cued click points, text and token based verification and reduces the guessing attacks as well as encouraging users to select more random and difficult to guess passwords[1]. Harsh Kumar designed a method in which click points will based on user perception of click points not on the basis of traditional technique like tolerance square. A perceptual hash function will be used for comparing click points made at registration time and login time. The click point is compared ,based on the content of click points which provides more accuracy and security[3]. Sneha Vasant Thakare presents 3D security cloud computing using graphical password. The 3D security have a 3 protection ring in which file categorization done by R-CIA algorithm, divides the files into ring 1, ring 2, ring 3. 3D password is used for ring 1, graphical password with icons is used for ring 2, persuasive clued click point is used for ring 3. Depending on rings, multi level security system increases secure access of cloud services. 3D password is a time consuming process and needs large amount of memory space and so a multi level authentication is taken as a consideration[8].

Mauricio Orozco designed a graphical password system with the novelty of incorporating the sense of touch via haptic technologies. Using haptics, the system utilizes the physical attributes captured during human haptic computer interactions. Parameters such as pressure and velocity can be handled as hidden feature to increase the resiliency of the system[4]. Wazir Zada Khan

designed a new hybrid graphical password based on a system which is a combination of recognition and recall based technique resistant to shoulder surfing attack and many other attacks on graphical passwords. The system applied to smart mobile devices which is more handy and convenient to use than a traditional desktop computers[10]. We propose a region based graphical password authentication scheme, in which passpoints and cued click point are combined. The scheme presents a new technique for authentication which is based on the tracking of mouse motions on an image called mouse gestures which is captured through corner detection method for selecting regions in the image by the cloud user. A mouse gesture is an continuous, directed sequence of the mouse cursor movements with a clearly distinguished start and end point marked by pressing the mouse right button. Cloud users are allowed to select an image and gesture parameters are stored in the local server. To get authenticated, a cloud user must draw the correct gesture using a mouse and it is validated with a local server and it starts accessing the cloud services.

2. Design of Region Based Graphical Password Authentication Scheme:

This region based authentication password scheme happens between the cloud user accessing cloud services and local server, cloud service providers. The figure 1 shows cloud user selected gestures on an image. The figure 2 shows the overall working of the scheme. Initially the cloud user (1) connects with the local server and (2) acknowledgement is sent to the cloud user, after successful connection establishment. In this process if the cloud user is not registered, the user selects gestures (3) on image position, size and gesture parameters which are stored in a local server. If the cloud user is registered, new selected gestures is validated with the old saved gestures(4) in the local server. After a successful local server establish connection between the cloud user and service provider.

Figure 1.Cloud User Selected Gestures

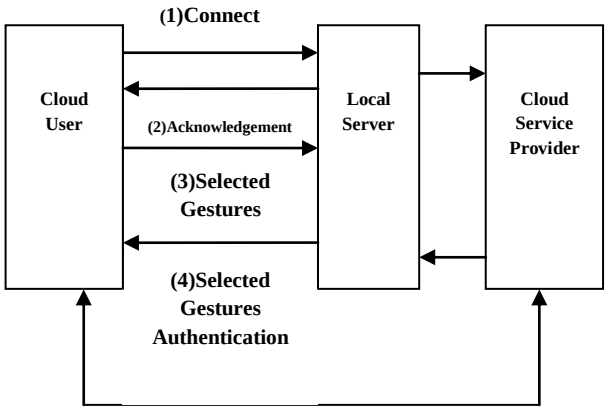

Figure 2. Region Based Graphical Password Authentication Scheme

The algorithm for "region based authentication scheme" are given below. Important notations used in the algorithms are Seq_No-Sequence Number, Img_No-Image Number.

Step1: Assign Seq_No equal to 1.

Step2: Assign random number to the image and assign it be Img_No.

Step3: Display the image as input to cloud user with Img_No

Step4: Draw virtual grid over the image

Step5: Cloud user selects the region and calculate/compute the parameters.

Step6: Store the parameters with Seq_No, Img_No and cloud user ID in the local server

Step7: Increment the Seq_No

Step8: Exit

After the registration process "corner detection method" is used in the region authentication scheme. A corner is defined as the intersection of two edges, where an edge is defined by the points on the image and there is a sharp change in the intensity. This method is used for detection of cloud user selection region which represent the region in a numerical way stored in the local server in an efficient way and also reduces the network transmission of data. This method involves the figuring out which points are the corners and looking at the relationship

between the corners and also takes the proportions of each part of gesture. Cloud user gets access to the service providers by comparing the new and old saved parameters in the local server with some tolerance level. Important notations used in the algorithms are Seq_No-Sequence Number, Login_Stat-Login Status, Img_No-Image Number

Step1: Assign Seq_No equal to 1

Step2: Display the image as input to cloud user with Img_No

Step3: Draw virtual grid over the image

Step4: Cloud user selects the region and calculates/compute the new parameters

Step5: Fetch the old parameters from the local server with Seq_No, cloud user ID, Img_No

Step 6: Compare the new parameters with old save parameters in local server

Step 7: If the compared values/output are within tolerance level

→Increment the Seq_No

→Login_Stat equal to 1

→Successful Login

Else

→Increment the Seq_No

→Login_Stat equal to 0

→Login Failed

End

Step 4: Exit

The next level is implementation which can be done by using java with SQL JDBC database. Cloud user drags the image by using GUI toolkit and region is selected and size, position, gesture parameters are updated in the database. During authentication, newly entered gesture parameters are compared with the old saved in the database for accessing cloud services or unauthenticated. Table1 shows new data of cloud user. Table 2 shows old data stored in the database. The compared values between Table 1 and Table 2 shows that, only the first cloud

user get access to cloud services because coordinate tolerance and grid pixel tolerance are within the tolerance level. The grid pixel and coordinate tolerance values get changed for every login attempts. The low value of grid pixel and coordinate tolerance accept accurate login data while high value leads to the login errors.

To provide better security to the intended customer, it is a better option to use region based graphical password authentication for accessing cloud services. Region based authentication provides stronger security because it uniquely represents individual cloud user selected region on the image, no two different regions on the image will have the same corner value. So this scheme would be strong enough to withstand online attacks, where the system is able to detect and stop or throttle the attack after the fixed number of failed login attempts.

Table 1: New Data of Cloud User

Cloud user ID	Img_No	Seq_No	Top x	Top y	Bottom x	Bottom Y	Grid Pixel Count
1	011	1	59	3	73	30	71
2	022	2	80	15	115	59	135

Table 2: Old Data Stored in Database

Cloud user ID	Img_No	Seq_No	Top x	Top y	Bottom x	Bottom Y	Grid Pixel Count
1	011	1	59	6	73	31	74
2	022	2	86	18	118	60	121

For Successful Login
Coordinate Tolerance: 5, Grid Pixel Tolerance: 50

Table 1 & Table 2 Comparison

Cloud user ID	Img_No	Top x	Top y	Bottom x	Bottom Y	Grid Pixel Count	Result
1	011	0	3	0	1	3	Pass
2	022	6	3	3	1	14	Fail

CONCLUSION:

This region based authentication scheme is reliable, secure and robust. There is always a drastic improvement in future which provides a good, scalable, high authentication for cloud users which keeps malicious attackers away. It extends the challenge response paradigm to withstand various active and passive attacks. Our future works includes combining the graphical password and the color, texture information of gesture for authentication process.

REFERENCE:

1. Abuthaheer, Jeya Karthikka,Thiyagu (2014), Cued Click Points Graphical Images and Text Password along with Pixel Based OTP Authentication, International Journal of Computer Applications,Vol.87-No.2,pp.45-49.

2. Feng Zhang, Aron Kondoro, Sead Muftic (2012), Location Based Authentication and Authorization Using Smart Phones, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp.1285-1292.

3. Harsh Kumar, Sarohi and Farhat Ullah Khan (2013), Perception Based Cued Click Points, International Journal of Computer Applications, Vol.70-No.22, pp.29-33.

4. Mauricio Orozco, Behzad Malek, Mohamad Eid, Abdulmotaleb El Saddik (2009), Haptic Based Sensible Graphical Password, Proceedings of Virtual Concept.

5. Mohammad Hashemi,Norafida Ithnin,Rezvan Pakdel (2012),Asian Journal of Applied Sciences, Vol.5,Issue 1, pp.20-32.

6. Niranjana. G, Kunal Dawn (2012), Graphical Authentication Using Region Based Graphical Password, International Journal of Computer Science and Informatics, Vol.2,pp.6-11.

7. Partha Pratim Ray (2012) Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices, International Journal of Computer Trends and Technology,Vol.3, pp.235-241.

8. Sneha Vasant Thakare, Deipali. V. Gore (2013), 3D Security Cloud Computing Using Graphical Password, International Journal of Advanced Research in Computer and Communication Engineering, Vol 2, pp.945-949.

9. Vachaspati, Chakravarthy, Avadhani (2013), A Novel Soft Computing Authentication Scheme for Textual and Graphical Passwords, International Journal of Computer Applications, Vol.71-No.10, 42-54.

10. 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, Vol.8, No.2, pp.145-154.