Password Generation Techniques for Accessing Cloud Services

Vaishnavi Deokar, Sayali Deshpande, Radhika Devkar

Abstract*— Cloud computing is emerging field because of its performance, high availability, least cost and many others. Besides this companies are binding there business from cloud computing because the fear of data leakage. Due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing.When organizations utilize cloud services, authenticating users in a trustworthy and manageable manner is a vital requirement. Organizations must address authentication related challenges such as credential management, strong authentication, delegated authentication, and managing trust across all types of cloud services. Users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. Thus depending on the file parameters(C-Confidentiality, I- Integrity, A- Availability), we use textual password for lower privilege files, CCP passwords(Cued Clickpoint) for medium privilege files and PCCP password(Persuasive cued Clickpoint) for high privilege files. In this paper we focus on the integrated evaluation of the Persuasive Cued-Click Points graphical password authentication system, including usability and security. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space.

***Keywords-* authentication, cued-click points, Graphical passwords, guessing attacks, persuasive technology.**

I. INTRODUCTION

Authentication in the computer world refers to the act of confirming the authenticity of the user's digital identity claim. It is a fundamental component in most computer security contexts and provides the basis for access control and user accountability. There are many things that are well known about passwords; such as that user can’t remember strong password and that the passwords they can remember are easy to guess. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to guess) is more tedious, avoids users from making such choices. In effect, this authentication schemes makes choosing a more secure password the path-of-least-resistance. Rather than increasing the burden on users, it is easier to follow the system’s suggestions for a secure password - a feature absent in most schemes.

While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication.

To overcome some of the shortcomings of the textual passwords, graphical authentication has been proposed as a user-friendly alternative to password generation and authentication. Current authentication methods are classified as biometric based, token based and knowledge based authentication as in figure1-

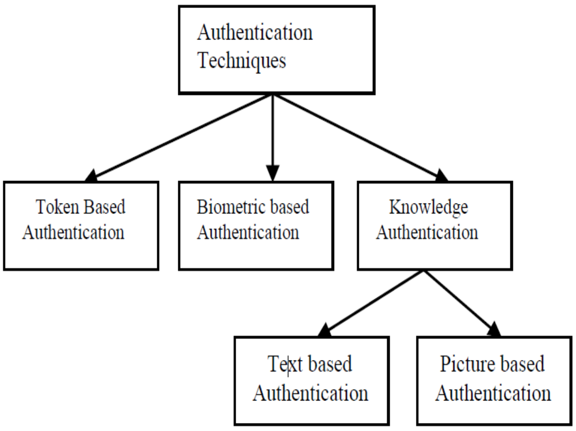

Authentication Techniques
Token Based Authentication
Biometric based Authentication
Knowledge Authentication
Text based Authentication
Picture based Authentication

Fig.1. Classification Of Authentication Technique

For uploading the data on cloud, the data is to be categorised on the basis of CIA (Confidentiality, Integrity, and Availability). The client who wants to send the data for storage needs to give the value of C (confidentiality), I (integrity), A (Availability). The value of C is based on level of secrecy at each junction of data processing and prevents unauthorized disclosure, value of I based on how much assurance of accuracy is provided, reliability of information and unauthorised modification is required, and value of A is based on how frequently it is accessible. With the help of proposed formula, the priority rating is calculated. Accordingly data having the higher rating is considered to be critical.

Manuscript received October 15, 2013

Vaishnavi Deokar, Computer Engineering, University Of Pune, Pune, India.

Sayali Deshpande, Computer Engineering, University Of Pune, Pune, India.

Radhika Devkar, Computer Engineering, University Of Pune, Pune, India.

II. BACKGROUND

The knowledge based authentication system includes the text password and graphical passwords. Typically text passwords are string of letters and digits, i.e. they are alphanumeric. Such passwords have the disadvantage of being hard to remember .Weak passwords are vulnerable to dictionary attacks and brute force attacks where as strong passwords are hard to remember. Hence we are using textual passwords for less confidential data. Though, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters [1][4]. For more confidential data we are using Cued-Click points (CCP) and Persuasive Cued-Click Points (PCCP) techniques.

III. PRIORTY RATINGS

```
Algorithm
1. Input: Data, protection ring, D[] array of n integer size.
Array C,I, A, S,R of n integer size.

2. Output: categorised data for corresponding ring.
3. For i 1 to n
3.1 C [i] = Value of Confidentiality.
3.2 I [i] = Value of Integrity.
3.3 A [i] =Value of Availability.
3.4 Calculate
S [i] = [(C[i] +I[i])/2]*(1/A[i])
4. For j 1 to 10
For k 1 to n
IF S [K] = = 1||2||3||4 then
R[k] =3 /* ring 3 allotted to D[k]th data.
IF S [K] = = 5||6||7 then
R[k] =2 /* ring 2 allotted to D[k]th data.
IF S [K] = = 8||9||10 then
R[k] =1 /* ring 1 allotted to D[k]th data
```

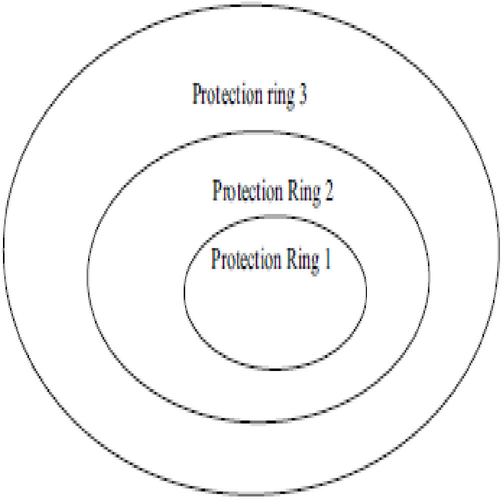


Fig.2. Ring Structure

In above algorithm the first job of the user is to categorise it on the basis of confidentiality, integrity and availability. Here D [] represents data, now the user have to give the value of C – confidentiality I – integrity and A –availability. After applying proposed formula the value of Cr criticality raring is calculated. Now allocation of data on the basis of Cr is done in protection ring. This suggests that internal protection ring is very critical and it require more security technique to ensure confidentiality.

IV. PROPOSED SYSTEM ARCHITECTURE

In this paper we are implementing CCP and PCCP along with textual password depending on file parameters of the respective file that user want to store on cloud. CCP was developed as an alternative click based graphical password scheme where users select one point per image for five images. The next image displayed to users is based on a deterministic function of the point which is currently selected. To address the issue of hotspots, PCCP was proposed.

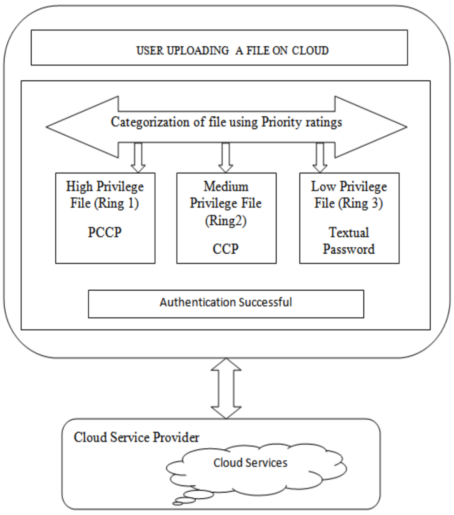

USER UPLOADING A FILE ON CLOUD
Categorization of file using Priority ratings
High Privilege File (Ring 1) PCCP
Medium Privilege File (Ring2) CCP
Low Privilege File (Ring 3) Textual Password
Authentication Successful
Cloud Service Provider
Cloud Services

Fig.3. Proposed System Architecture.

V. GRAPHICAL PASSWORDS

A. *Passpoints*

In the PassPoints graphical password scheme a password consists of a sequence of click points (say 5 to 8) that the user chooses in an image. The image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points.
Any pixel in the image is a candidate for a click point.

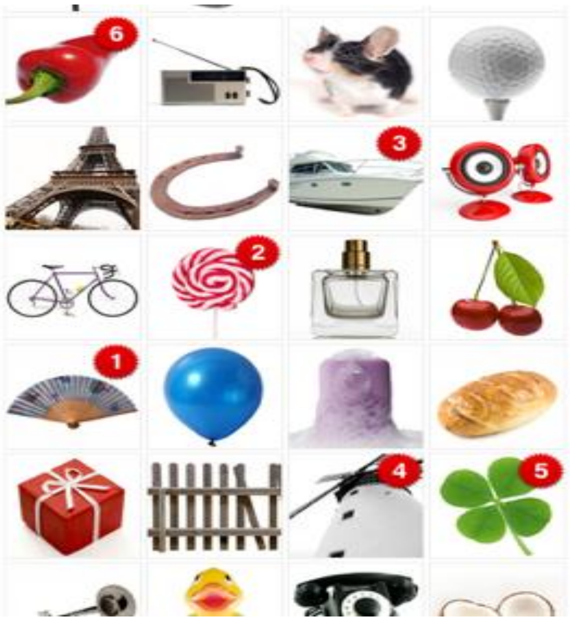


Fig.4 A screen shot of the PassPoints system

Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess PassPoints passwords.

Users also tend to select their click-points in predictable patterns (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat[3].

B. *Cued-Click Points*

The Cued Click Points (CCP) scheme is a proposed alternative to PassPoints. Cued Click Points which was designed to reduce patterns and to reduce the usefulness of hotspots (areas of the image that have higher likelihood of being selected by users as password click-points as shown in fig.6) for attackers[2]. Instead of five click-points on one image, cued click points uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point. One best feature of Cued Click Point is that the message of authentication failure is displayed after the final click-point, to protect against incremental guessing attacks.

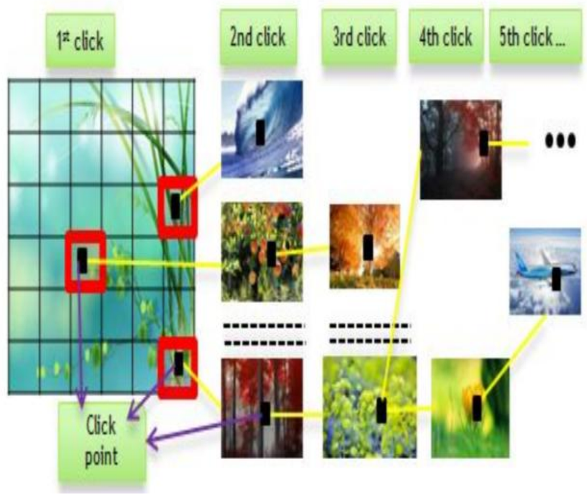


Fig. 5. CCP passwords can be regarded as a choice-dependent path of images.

But this technique has several disadvantages like false accept (the incorrect click point can be accepted by the system) and false reject (the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point.

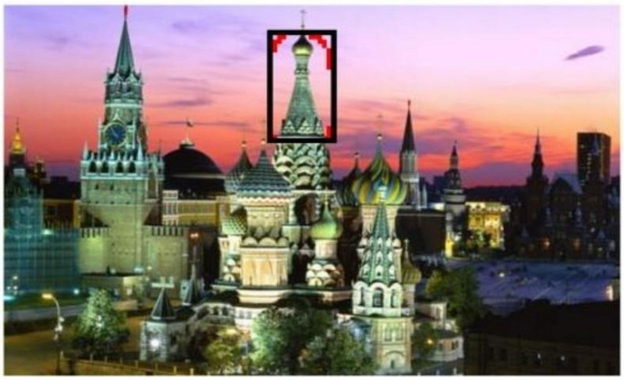
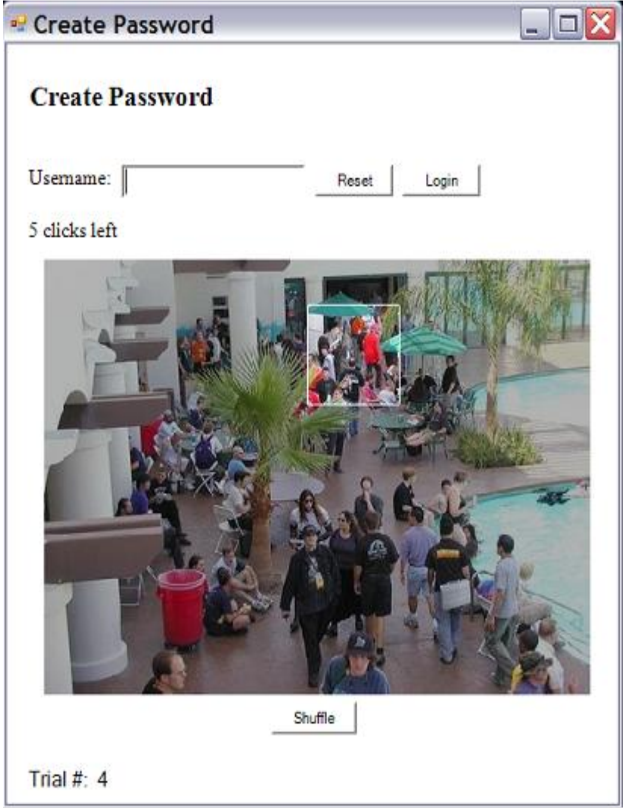


Fig.6.Hotspot

C. *Persuasive Cued-Click Points*

For creating Persuasive Cued Click Points persuasive feature is added to CCP. PCCP encourages users to select less predictable passwords. For password creation PCCP uses terms like viewport & shuffle. When users creating a password, the images are slightly shaded except for a viewport as shown in the fig. 7, to avoid known hotspots the viewport is positioned randomly. The most useful advantage of PCCP is attackers have to improve their guesses [6]. Users have to select a click-point within the highlighted viewport and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport .At the time of password creation users may shuffle as often as desired but it slows the process of password creation. Only at the time of password creation, the viewport & shuffle button appears. After the password creation process images displayed normally without the viewport & shuffle button. Then user has to select correct click on particular image. PCCP is a good technology but has security problems. Fig.7.shows the password creation process including viewport & shuffle button.
Our hypotheses are:

1. Users will be less likely to select click-points that fall into known hotspots.
2. The click-point distribution across users will be more randomly dispersed and will not form new hotspots.
3. The login success rates will be similar to those of the original CCP system.
4. Participants will feel that their passwords are more secure with PCCP than participants of the original CCP system.



5 clicks left

Trial #: 4

Fig.7. PCCP Create Password interface. The viewport highlights part of the image.

VI. CENTER DISCRETIZATION

Discretization of click-points allows for approximately correct click-points to be accepted by the system without storing exact click-point coordinates in the clear. Our second prototype implemented Centred Discretization, wherein an invisible discretization grid is overlaid onto the image, dividing the image into square tolerance areas, to determine whether a login click-point falls within the same tolerance area as the initial click-point[5]. For each click-point, the grid's position is set during password creation by placing it such that there is a uniform tolerance area centred around the original click-point, by calculating the appropriate (x, y) grid offset (Gx,Gy) (in pixels) from a (0,0) origin at the top-left corner of the image. On subsequent user login, the system uses the originally recorded offsets to position the grid and determine the acceptability of the each login click-point.

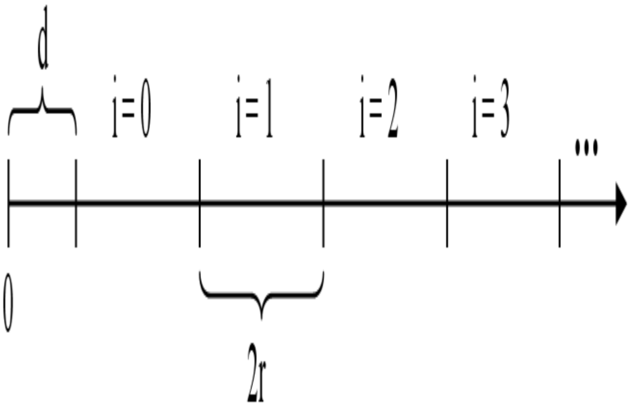


Fig.8. The continuous line L is divided into segments of length 2r.

Consider a 1-dimensional line, L, with a continuous set of data points. A particular point on this line is represented by a real number x. Our initial objective is to discretize this line into equal segments where x falls in the centre of the segment containing it. This ensures an even tolerance on both sides of x. A tolerance r is selected based on system or user preferences. Each segment is of length 2r as shown in Figure 8. To ensure that x is centred in its segment, segment 0 may need to be offset from the origin. This offset is represented by parameter d.

First assume that a 1-D password consists of a single click-point x. To store this password, we must discretize the point by calculating its offset d (where $0 \leq d < 2r$) and its corresponding segment identifier i (where $i \geq -1$, with $i = -1$ occurring if x is within r of the origin). Offset d is stored in the clear, while i is stored in protected form as its hash value h(i; d). The offset d is included in the hash to uniquely identify the segment. The system must also be aware of tolerance r that specifies the acceptable inaccuracy during password re-entry. The segment identifier i is computed by i = [(x - r)/2r], identifying the segment containing x. The offset d = (x - r) mod 2r determines the distance between the origin and the left boundary of segment 0. To verify if a re-entered click-point x' is acceptable, the system computes i' = [(x' - d)/2r]. This calculates which segment contains x' using the same offset as the original point. Note that x' is not necessarily centred within its segment; we are simply calculating which segment contains x' based on x's pre-determined segments. If x' is within tolerance r of x, then i' = i and hence h(i', d) equals the stored value of h(i, d) and system accepts the entry. If x' is outside of the accepted tolerance r, it falls in a different segment and i'≠ i, thus h(i', d) ≠ h(I, d) and the system rejects it.

For example, assume x = 13 and r = 5:5. We compute i = [(x - r)=2r] = [(13 – 5.5)/11] = 0 and d = (x - r) mod 2r = (13 -5.5) mod 11 = 7.5. Offset d = 7.5 is stored in the clear along with protected h (i, d) = h(0, 7.5). If a user enters x' = 10 during login, the system calculates i' = [(x' - d)/2r] =[(10 – 7.5)/11] = 0. It then compares h (i', d) and h(i, d) and the click-point is accepted since they match. In practice, if a password consists of more than one clickpoint, all segment indices and their offsets are concatenated and hashed together as one. This stops attackers from matching individual points, and thus carrying out an efficient divide-and-conquer attack.

VII. SECURITY

A. Brute force search

The main defence against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords .Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password[6].

B. Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack[6]. More research is needed in this area. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

C. Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Pass face technique have shown that people often choose weak and predictable graphical passwords.

D. Spyware

Except for a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application Information, such as window position and size, as well as timing information.

E. Shoulder surfing

Most graphical passwords are vulnerable to shoulder-surfing attacks .With today's small cameras and camera phones, it is easy to video-capture a user's screen or key- board as they are logging in. Shoulder surfing can be avoided to some extend by making some manipulation on user interface side such as reducing the size of the mouse cursor or dimming the image[6].

F. Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming overall, we believe it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.

G. Capture Attacks

Malware is capture attack more attention must be given to this attack as it is hazardous to both text and graphical passwords since key logger, mouse logger, and Screen scraper malware could send captured data remotely or otherwise make it available to an attacker. The attacker‘s has to work hard because PCCP is not vulnerable to hotspot attack; attacker must also determine Sequence of images for attack.

VIII. FUTURE ENHANCEMENT

Cloud computing provides variety of internet based on demand services like software, hardware, server, infrastructure and data storage. To provide secured services to intended customer, we should have strong authentication password generation technique. By doing so, the probability of brute force attack for breaking the password can be reduced to a large extent. Our future work concentrates on the work for intruder detection technique.

IX. CONCLUSION

User authentication is a fundamental component in most computer security contexts. We proposed a simple graphical password authentication system which provides the more secure authentication than the text Password scheme.An important usability and security goal in authentication systems is to help users' select better passwords and thus increase the effective password space. We believe that users can be persuaded to select stronger passwords through better user interface design. As an example, we designed Persuasive Cued Click-Points (PCCP).

PCCP encourages and guides users in selecting more random click-based graphical passwords. A key feature in PCCP is that creating a secure password is the "path-of-least-resistance", making it likely to be more effective than schemes where behaving securely adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and avoiding known hotspots, thus increasing the effective password space, while still maintaining usability. Hence, we are using textual passwords for less confidential files and graphical passwords for highly confidential files.

ACKNOWLEDGMENT

Our sincere thanks to Prof. S.A.DARADE and Prof. G.S.NAWALE, Head Department of COMPUTER Engineering SITS, PUNE, for their constant encouragement.

REFERENCES

1. Chiasson, S., Biddle, R., and van Oorschot, P.C. A Second Look at the Usability of Click-Based Graphical Passwords. Symp. on Usable Privacy and Security (SOUPS) 2007.
2. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.

3. Dirik, A.E., Memon, N., and Birget, J.C. Modeling user choice in the PassPoints graphical password scheme. Symp. on Usable Privacy and Security (SOUPS) 2007.
4. D. Davis, F. Monrose, and M. Reiter, ―On user choice in graphical password schemes,‖ in 13th USENIX Security Symposium, 2004.
5. Birget, J.C., Hong, D., and Memon, N. Graphical Passwords Based on Robust Discretization. IEEE Transactions on Information Forensics and Security, vol. 1, no. 3, September 2006.
6. Chippy.T and R.Nagendran," Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points", International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012.

Miss. Vaishnavi Deokar, pursuing BE (Computer) in Sinhagad Institute Of Technology And Science.

Miss. Sayali Deshpande, pursuing BE (Computer) in Sinhagad Institute Of Technology And Science.

Miss. Radhika Devkar, pursuing BE (Computer) in Sinhagad Institute Of Technology And Science.