Graphical Image Based Password Authentication System

D.Sathish Kumar
Assistant Professor
Department of CSE
Sri Sairam Engineering College
Chennai, Tamilnadu, India

R.Rajkumar
UG student
Department of CSE
Sri Sairam Engineering College
Chennai, Tamilnadu, India

R.Kalpana
Project Associate
Cognizant Technology,
Chennai, Tamilnadu, India

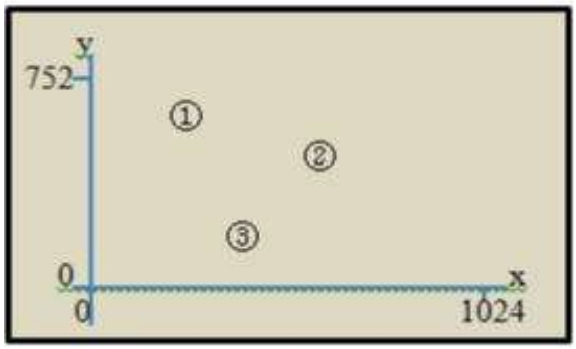
Abstract—Text based password authentication scheme is vulnerable to many attacks such as shoulder surfing attack and similar kind of attacks like dictionary attack, brute-force attack etc. Many graphic based password authentication schemes are in existence but they are also quite expensive in deployment and needs more response time at login phase. To solve the problem of text-based password authentication, graphical passwords using images have evolved. Graphical passwords process authentication by selecting the exact positions on the image shown on the screen. This ensures that the data is safe and has a reference selected from the image coordinates that the user selects. A scheme called Captcha based authentication protocol is used along Pass Positions method. Captcha based approach can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. Captcha offers a novel approach to tackle the well-known image hotspot problem in popular graphical password systems, such as Pass Positions, that often leads to weak password choices. This scheme is resistant to usability issues such that it does not overload human memory and provides extra security against unwanted attacks.

Keywords—Security, Password, Authentication, Data, Cloud computing, Captcha, Pass Points

I. INTRODUCTION

In today's information society, the importance of information protection is increased day by day. One of the things you need to protect your information is the security of information devices. The most commonly used scheme for the security of information devices, is the password. Password use numbers only, or use combinations of numbers and letters also. This authentication technique is called text-based authentication.

There is a problem with text-based authentication that is the numbers should be easy to remember, but others should be impossible to predict. However, In order to remember the password, the password should be short and meaningful. But short and meaningful password can be easily stolen. Moreover, users want to enter a password quickly and long passwords are hard to remember, so they often use the same password for different accounts. Therefore, when a password for one account is revealed, it becomes difficult to keep the security of other accounts. It is further improved by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given time frame. Captcha was also used with recognition-based graphical passwords to address spyware wherein a text Captcha is displayed below each image; a user locates her own pass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image as her password during authentication.



For example, if the Pass Positions is applied with an image size of 1024 x 752 (roughly the full screen), and three points are chosen (i.e. (150, 650), (530, 330), (370, 70)), as shown in Fig.1, then Pass Positions generates R-String (RD, LD) in the registration phase.

II. RELATED WORK

One of the major problems in the file sharing in a public cloud is that there may be some important and confidential data that can be beneficial to individuals and at the same time there is also a security concern that these files can be illegally accessed by unauthorized persons so there should be an intimation about the users accessing their data in a public cloud environment.

In common place text-based password schemes, users naturally decide passwords that are simple to remember, display patterns, and are thus in danger to brute-force dictionary attacks. This leads us to ask whether other types of passwords (e.g., graphical) are also vulnerable to dictionary attack because of users tending to choose memorable passwords. A method is recommended to forecast and model

a number of such classes for systems where passwords are formed exclusively from a user's memory. These classes define weak password subspaces appropriate for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall. These cognitive studies enables the user to define a set of password complexity factors (e.g., reflective symmetry and stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak the password subspaces they define might be, we use the "Draw-A-Secret" (DAS) graphical password scheme of Jermyn et al. as an example [1]

A Pass Points password is a sequence of points, chosen by a user in an image that is displayed on the screen. This model predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to evaluate automatically whether a given image is well suited for the Pass Points system, and to analyze possible dictionary attacks against the system. The predictions provided by this model are compared to results of experiments involving human users. At this stage, our model and the experiments are small and limited; but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research [2]

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses.

User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user's perspective user-friendliness is a key requirement. This paper suggests the use of a novel authentication scheme that preserves the advantages of conventional password authentication, while simultaneously raising the costs of online dictionary attacks by orders of magnitude [3].The proposed scheme is easy to implement and overcomes some of the difficulties of previously suggested methods of improving the security of user authentication schemes.

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. This paper, focuses the inadequacy of existing and proposed login protocols designed to address large-scale online dictionary attacks (e.g., from a botnet of hundreds of thousands of nodes). A concept called Password Guessing Resistant Protocol (PGRP) is used which is derived upon revisiting prior proposals designed to restrict such attacks [4].

Under the brute-force attack the protocols are safe against eavesdropping, in that an observer who fully records any feasible series of successful interactions cannot practically compute the user's secret. Moreover, the protocols can be tuned to any desired level of security against random guessing, where security can be traded-off with authentication time. The proposed protocols have two drawbacks: First, training is required to familiarize the user with the secret set of pictures. Second, depending on the level of security required, entry time can be significantly longer than with alternative methods [5]. We describe user studies showing that people can use these protocols successfully, and quantify the time it takes for training and for successful authentication. We show evidence that the secret can be effortlessly maintained for a long time (up to a year) with relatively low loss.

III. PROPOSED SYSTEM

A new security primitive method is proposed based on hard AI problems, namely, a novel family of graphical password, which is called as graphical passwords. A graphical password addresses a number of security problems overall, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. The proposed method uses grid selection and passes point algorithms. This algorithm process on the image to get the pixel points and the points were used as a secret key for the file uploaded by the user. There are two approaches using in the system.

A. Pass Positions approach

Unlike most existing graphical password schemes, 'Pass Positions' is a graphical password scheme, which uses relative positions of the click points. If the user uses a thick pointer or a finger, and presses a region instead of a point (at a pixel level), then Pass Positions will find the center point of the region automatically, and use the center point as the click point.

B. Captcha approach

Completely Automated Public Turing test to tell Computers & Humans Apart. It is a program that is a challenge response to test to separate humans from computer programs. The CbPA protocol requires solving a Captcha challenge after inputting a valid pair of user ID and password. In Captcha approach, a new image is generated for every login attempt. This uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate a reference image. These schemes are clicked-based graphical passwords.

IV. SYSTEM ARCHITECTURE

The major modules of the system include (a) Registration section (b) File upload section (c) File request section (d) File download section. The Registration section involves a user or an organization to register in public cloud and select a captcha image as an additional security .After registration the user can have an option to upload files and at the time of uploading the user is prompted with an image to select its coordinates which is used as a reference to the files. File request can be issued by anyone who wants to view the file. The file request is sent to the owner. The downloading of the file is processed after receiving the coordinates from the owner.

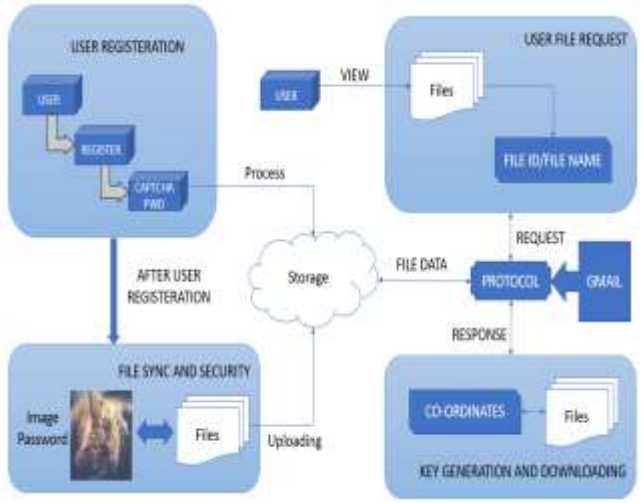


Figure 1: Proposed System Architecture

V. SYSTEM DESIGN

The authentication server AS stores a salt s and a hash value H(ρ,s) for each user ID . Upon receiving a login request, AS generates a CaRP image. The coordinates of the clicked points are recorded and sent to AS along with the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs.Then AS retrieves salt s of the account, calculates the hash value of ρ with the salt. Authentication succeeds only if the two hash values match

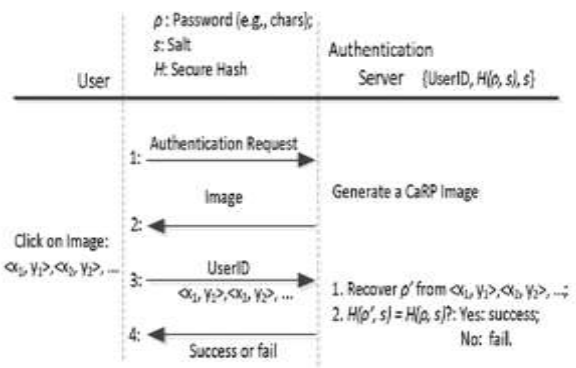


Figure 2: Flow Diagram

User Registration: In this module, Users are having authentication and security to access the cloud. For security, captcha technique is implemented to access the detail which is presented in the Image system. Each time Users have to enter, registered captcha text and password for accessing the account.

File Synchronization and Security: The user can start up the server after system is opened. Then the user can upload the file to the storage with the key to access it. The key process is done with Grid selection and Pass Point algorithm. By clicking particular point at the given image, the position of the image pixel is taken as X & Y Co-ordinates as key. These co-ordinates are assigned as X1, Y1 and by clicking on different position 2nd coordinates are assigned as X2, Y2. In this a password guess tested in an unsuccessful trial is determined than traditional approaches.

User File Request: The request process is done through protocol and key is send to an authorized user through mail. By this process key is shared and the file is view/downloaded by the other user with the key given by the data owner.

Key Generation and Downloading: The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password. To counter guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials, the password can always be found by a brute force attack.

VI. CONCLUSION

Thus this kind of approach to secure authentication using the captcha and pass positions methodology helps in protecting important data in a public cloud. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4, 2012.

[2] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.

[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005.