International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)

ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014.

PASSWORD AUTHENTICATION IN CLOUD USING AUDIO AND IMAGES

S.Preethi[#1] and P.Sudhakar[*2]

[#]*M.E. Student, Dept of cse, Annamalai University, Chidambaram, India*

[*]*Assistant Professor, Dept of cse, Annamalai University, Chidambaram, India*

***Abstract* — From last decade, user authentication has been the most important topic in internet security. Current authentication systems suffer from many weaknesses.In cloud storage systems, data owners host their data on cloud servers and users can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. In large-scale cloud storage systems, the data may be updated dynamically, so existing remote integrity checking methods served for static archive data are no longer applicable to check the data integrity. In cloud storage system, however, it is inappropriate to let either side of cloud service providers or owners conduct such auditing, because none of them could be guaranteed to provide unbiased auditing result. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data is correctly stored in the cloud.**

***Index Terms* — Authentication, biometrics passwords, graphical passwords, multifactor, sound signature, textual passwords, 3-D password.**

I. INTRODUCTION

Cloud storage is an important service of cloud computing, which allows data owners (owners) to move data from their local computing systems to the cloud. More and more owners start to store the data in the cloud. However, the paradigm of data hosting service also introduces new security challenges. Data hosting owners would worry that the data could beget lost in the cloud storage. This is because data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take. Occasionally, cloud service providers might be dishonest.

They could discard the data which has not been accessed or rarely accessed to save the storage space and claim that the data are still correctly stored in the cloud. Therefore, owners need to be convinced that the data are correctly stored in the cloud. Also owners can check the data integrity based on two-party storage auditing protocols. There are several important requirements which have been proposed for third party auditing in cloud storage systems. The auditing protocol must have following properties:

A. Confidentiality

The auditing protocol should keep owner's data confidential against the auditor.

B. Dynamic Auditing

The auditing protocol should support the dynamic updates of the data in the cloud.

C. Batch Auditing

The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds.

Now-a-days, several remote integrity checking protocols were proposed to allow the auditor to check the data integrity on the remote server. However, due to the large number of data tags, the auditing protocols may incur a heavy storage overhead on the server. Recently, several remote integrity checking protocols were proposed to allow the auditor to check the data integrity on the remote server. Here proposed a dynamic auditing protocol that can support the dynamic operations of the data on the cloud servers, but this method may leak the data content to the auditor because it requires the server to send the linear combinations of data blocks to the auditor. The proposed method extended their dynamic auditing scheme to be privacy-preserving and support the batch auditing for multiple owners. The following features are satisfied in proposed system:

1) The new system provide passwords that are easy to remember and very difficult for another users to guess.
2) The new system provides passwords that are not easy to write down on paper.
3) The new system provides passwords that can be easily revoked or changed.

Cloud security is an evolving sub-domain of computer security, network security and information security. The security is the biggest problem for system, because the services of cloud computing is based on the sharing .Prevention of attacks such as authentication attacks, Distributed Denial of Services (DDOS) attacks and Cloud malware injection attacks and its solutions are used.

A. Click-based graphical password scheme

Enhanced Cued Click Points (ECCP) method. A password consists of sequence of some images in which user can select one click-point per image. User is asked to select a sound signature corresponding to each click point.

B. Collaborative PDP scheme

It takes as inputs a secret key sk, a file F and a set of cloud storage providers P = {Pk}, and returns the encrypted file.

The system intends to create a graphical password using a single/multiple images and associate a sound file. Password is generated by assigning click points in each image and associating sound file is used to provide another security layer. Provides the collaborative PDP scheme to construct audit system architecture.

II. Related Work

Luigi Catuogno and Clemente Galdi, et al proposed a graphical mechanism that handles authentication by means of a numerical PIN, that users have to type on the basis of a secret sequence of objects and a graphical challenge. The proposed scheme can be instantiated in a way to require low computation capabilities, making it also suitable for small devices with limited resources. This scheme is effective against "shoulder surfing" attacks. A simple graphical PIN authentication mechanism is used that is resilient against shoulder Surfing attacks. The presented scheme can be also used for low-cost device authentication, e.g., RFID tag-to-reader or reader-to-tag authentication [1].

Sonia Chiasson, Robert Biddle, P.C. van Oorschots et al described that click-based graphical passwords, which involve clicking a set of user-selected points, have been proposed as a usable alternative to text passwords. Conducted two user studies: an initial lab study to revisit these usability claims, explore for the first time the impact on usability of a wide-range of images, and gather information about the points selected by users; and a large-scale field study to examine how click-based graphical passwords work in practice. No such prior field studies have been reported in the literature. It has found significant differences in the usability results of the two studies, providing empirical evidence that relying solely on lab studies for security interfaces can be problematic. Also it has presented a first look at whether interference from having multiple graphical passwords affects usability and whether more memorable passwords are necessarily weaker in terms of security. Two user studies has conducted : an initial lab study to revisit these usability claims, explore for the first time the impact on usability of a wide-range of images, and gather information about the points selected by users; and a large-scale field study to examine how click-based graphical passwords work in practice[2].

Daphna Weinshall and Scott Kirkpatrick has identified a wide range of human memory phenomena as potential certificates of identity. These "imprinting" behaviors are characterized by vast capacity for complex experiences, which can be recognized without apparent effort and yet cannot be transferred to others. They are suitable for use in near zero-knowledge protocols, which minimize the amount of secret information exposed to prying eyes while identifying an individual. Several examples of such phenomena is sketched and are applied them in secure certification protocols. Concluded result is that the innate human capability to capture effortlessly large amounts of everyday experience can be exploited to create a novel sort of computer-human interface. Rather than remembering a alphanumeric password, remembering images is more easy for the user[3].

M.Kameswara Rao and Sushma Yalamanchili et al proposed that Text password-based authentication is a popularly used authentication mechanism. Despite having greater security, text-passwords are characterized by selection of a weak and easy to remember passwords. Users also tend to write them down and share them with friends, family members and colleagues defeating the security provided by text-passwords. Graphical passwords offer an alternative to text passwords as the password space is typically higher, less prone to dictionary attacks and easier to remember visually. However, they suffer from shoulder-surfing attacks. In this paper, we propose two authentication schemes that support keyboard as well as graphical mouse-based input that map password characters to other regions of the password space. This shields the users password from being known to the adversary thus deflecting shoulder-surfing and spyware attacks. The schemes include both single and multi color input images consisting of printable characters. An analysis of security, usability, memorability and social Engineering aspects of the proposed schemes is presented [4].

Two authentication schemes that support keyboard as well as graphical mouse-based input that map password characters to other regions of the password space. The schemes include both single and multi color input images consisting of printable characters. Adrian Perris and Dawn Song that Current security systems suffer from the fact that they fail to account for human factors. This paper considers two human limitations: First, people are slow and unreliable when comparing meaningless strings; and second, people have difficulties in remembering strong passwords or PINs. The identified two applications where these human factors negatively affect security: Validation of root keys in public-key infrastructures, and user authentication. The approach is to improve the security of these systems is to use hash visualization, a technique which replaces meaningless strings with structured images. The requirements of such a system and propose the prototypical solution Random Art[5].

To apply hash visualization is to improve the real-world security of root key validation and user authentication.. To improve the security of these systems is to use hash visualization, a technique which replaces meaningless strings with structured images. The examine the requirements of such a system and propose the prototypical solution Random Art. To apply hash visualization is to improve the real-world security of root key validation and user authentication [6].

III. Outline of the Work

A. Portfolio and Authentication

User has to select a specific number of images from larger set of images presented by a server. Portfolio consists of 50 images. To authenticate the user, the system presents a challenge set, consisting of 50 images. The user has to select 3 images from the portfolio. The remaining 47 images are called decoy images. Server creates a challenge set, which consists of portfolio and decoy images. The user has to

identify all portfolio images, then only the user will be authenticated.

B. Sound Signature

Sound clips are used for Authentication. While the creation of password the user has to select one sound clip from the given audio clip by the system. The selected sound clip is stored in the System Database. During log in, the user has to select the same audio sound. The system checks that sound clip and pause time are same or not.

C. Data Store with Secret Key

Data storage in cloud is using protocol with storing data with secret key and public key. A secret and public keys is taken as input for the file F with the definition info of the update to be performed and the previous metadata Mc. The output is an "encoded" version of the file e(F). The client sends e(F), e(info), e(M) to the server. The output is the new version of the file F_i and the metadata M_i, along with the metadata to be sent to the client M.

D. Data Retrieval from Cloud

CPDP Protocol and its scheme is used to store the data in the cloud successfully. It can't be corrupted and hacked. The server also sends the requested file, along with verification method, secret and public keys, the latest client metadata Mc as input. The input is sent to the server .

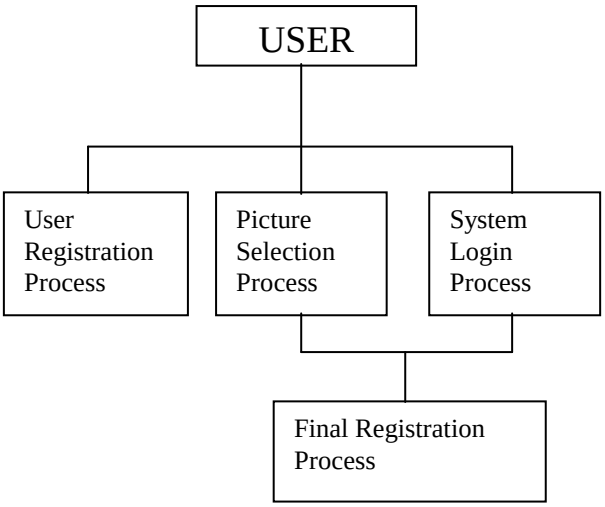

Fig.1 Graphical Authentication Working Process

IV. EXPERIMENTAL SETUP

In this proposed system, to provide the different audio and images for password authentication. This method gives high level security. Block diagram of the proposed technique is shown in Fig 2.

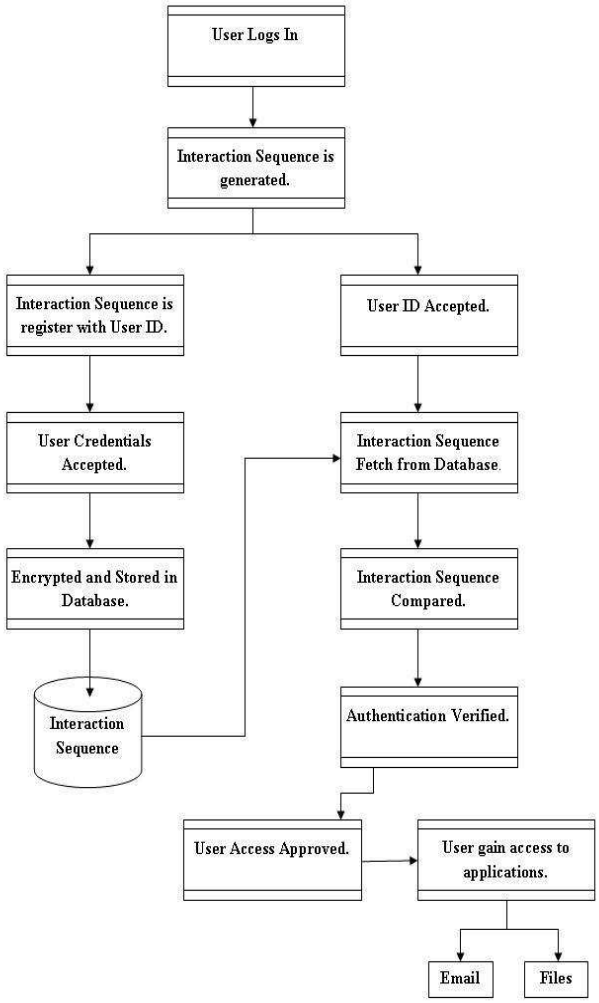

Fig 2 Block Diagram of proposed technique

The work of password Authentication involves two main phases.

Registration Phase

When new user registers, first enter the all details which give in registration form. Then select any one image from multiple images and also click the minimum 4 points at any sequence. Then represent the Thumb expression of user. Then select any one sound clip, play and pause that clip at particular time. This all interactions stored in database in encrypted format.

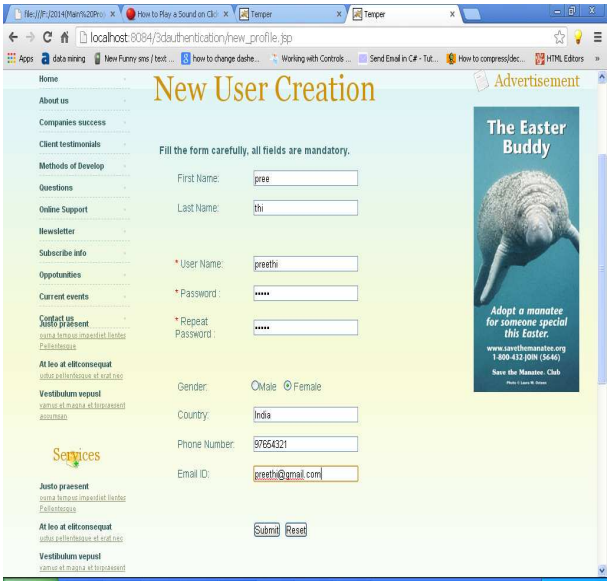

Fig 3 Registration form

Authentication Phase

Enter username and password. Select proper image and their sequence of click points. Recognize the Thumb expression of that user. Select proper sound clip and their pause time. All interactions fetch from database then compared one by one. Then access granted to authorized users for access applications.

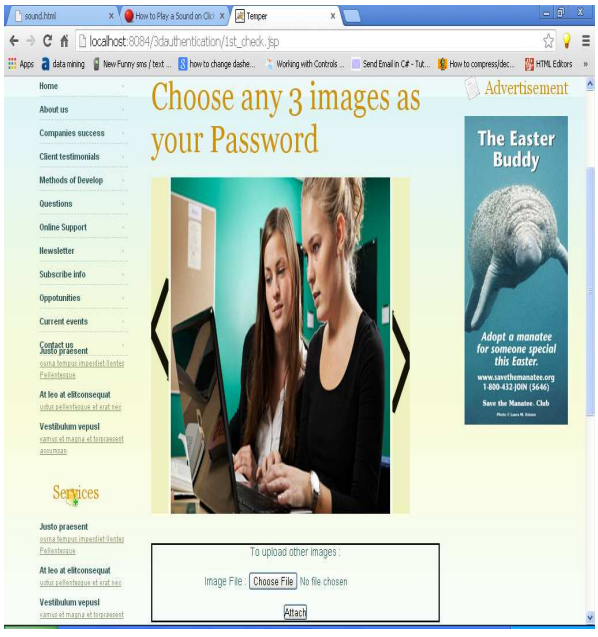

Fig 4 Setting graphical password

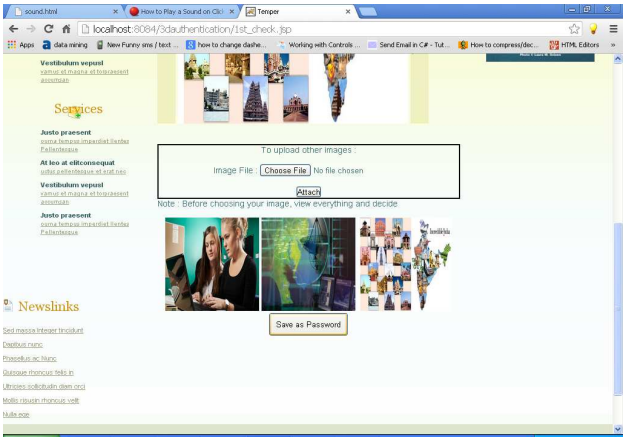

Fig 5 Saving images in server

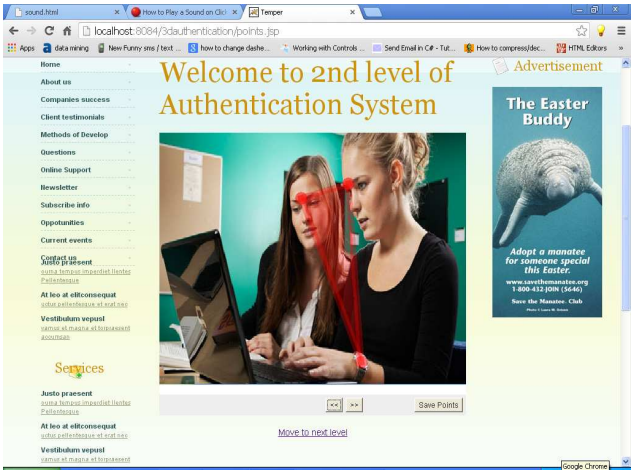

Fig 6 Choosing click points

Fig 7 Choosing audio

Fig 8 Creating secret key

Fig 9 Files stored in cloud

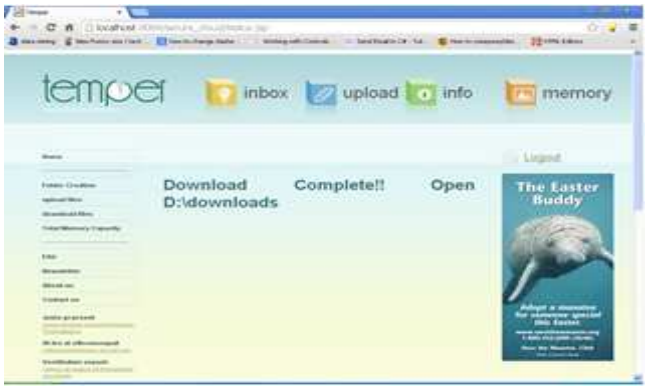

Fig 10 Downloading file from cloud

5. CONCLUSION

In this paper, Graphical authentication is an alternate solution to text based authentication. Graphical passwords have two aspects which are usability and security. Enhanced Cued Click-points method provides great security using hotspot technique

To achieve a secure and data privacy problem. Third-party Storage Auditing Service (TSAS) is a method to generate encrypted keys. The auditing protocol lets the server compute the proof as an intermediate value of the verification reduce the computing loads of the auditor by moving it to the cloud server.

REFERENCES

[1]. Eiji H., Nicolas C., "Use your illusion: secure authentication usable anywhere," Proceedings of the 4th. Symposium on Usable Privacy and Security (SOUPS). July 2008. Pittsburgh, PA USA. 35-45.

[2]. Roman W., Alexander D. L., "PassShapes - utilizing stroke based authentication to increase password memorability," Proceedings of the 5th Nordic conference on Human-Computer Interaction: Building Bridges. October 2008. Lund, Sweden. 383-392.

[3]. Saranga K., Dugald R. H. "Order and entropy in picture passwords," Proceedings of Graphics Interface. May 2008. Windsor, Ontario, Canada. 115-122.

[4]. Julie Thorpe, P.C. van Oorschot. "Towards secure design choices for implementing graphical passwords. Proceedings of the 20th annual computer security applications conference," December 2004 Ottawa, Ont., Canada: 50 – 60.

[5]. Xiaoyuan Suo, Ying Zhu and G. Scott. Owen. "Graphical passwords: a survey," Proceedings of the 21st Annual Computer Security Applications. 2005, 463-472.

[6]. Furkan T., A. Ant Ozok, and Stephen H. Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," Symposium on Usable Privacy and Security (SOUPS). July 2006, Pittsburgh, Pennsylvania, USA. 56-66.

[7]. Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu. "YAGP: Yet Another Graphical Password Strategy," 2008 Annual Computer Security Applications Conference. 2008, 121-129.

[8]. Ali Mohamed Eljetlawi, Norafida Ithnin. "Graphical password: comprehensive study of the usability features of the recognition base graphical password methods," Third 2008 International Conference on Convergence and Hybrid Information Technology. 1137-1143. 2008

First Author S.Preethi received the B. E degree in Computer Science and Engineering from Annamalai University, Annamalai nagar in the year 2012. She is doing her M.E degree in Computer Science and Engineering at Annamalai University.

Second Author P.Sudhakar ME, Ph.D., Assistant Professor, Department of Computer Science and Engineering, Annamalai University, Annamalai nagar.