IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. I (Sep – Oct. 2014), PP 52-56
www.iosrjournals.org

Graphical Password Strength in Cloud Computing

Archana Bisen[#1], Nitesh Gupta[#2]
[#1] *MTECH (CSE), NIIST, Bhopal. Affiliated to RGPV, Bhopal, M.P, India*
[#2] *Asst. Professor (CSE) in NIIST, Bhopal. Affiliated to RGPV Bhopal, M.P, India*

Abstract: *In a Network we have various issues to work with our services & data (maintenances) & today Cloud computing provides convenient on-demand network access to a shared pool of configurable enumerate resources. The resources can be rapidly expand with great efficiency and minimal management atop. Cloud is an afraid computing platform from the view point of the cloud users, the system must design structure that not only assure sensitive information by enabling computations with encrypted data, but also assure users from envious behaviours by permissive the validation of the computation result along with an effective authentication mechanism to the user, from the past timing we have a multiple scheme to authorize any interface- here also in order to access a cloud we use textual password which is not much secure in terms of authentication because textual password might be easy to guess & lot of brute force attack has been already done on textual based attack in current world so that still here we are finding an efficient way where we can get a reliable authentication to original user, one of the way which we got is object password or graphical password to authenticate interface which we have described in existing system In this paper, we propose a technique for authenticating cloud which is advance authentication scheme in terms of graphical password at the same time we are going to propose this scheme for using in cloud & in cloud how we can verify the data integrity which we are storing. It is high-speed data verification scheme with minimal loss probability. The proposed system is highly efficient in order to authenticate in proper manner in order to maintain login security & after authentication again to verify our data integrity correctly.*

Keywords: *Enhanced Graphical password scheme, Cloud Computing, Data Integrity and Key Generation.*

I. Introduction

Organisations today are increasingly looking towards Cloud Computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and flexible assistance. The Cloud technology is a growing direction and is still undergoing lots of venture. Cloud promises vast cost prosperity, agility and gullibility to the trade. All business data and software are stored on servers at a remote location referred to as Data centres. Data centre environment allows venture to execute utilization faster, with easier manageability and less maintenance effort, and more rapidly scale resources (e.g. servers, storage, and networking) to meet fluctuating business needs. A data centre in cloud environment to catch information that end-users would more traditionally have stored on their system. This hike concerns regarding user isolation because users must keep secure their data. Cloud services should ensure data integrity and provide trust worthy authentication to the user isolation. Although deploy data into the cloud is economically attractive for the cost and complexity of long-term large-scale processing, it's flawed of offering strong pledge of data integrity. Cloud computing poses privacy concerns primarily, because the IAP consistently in time access the data. The Cloud IAP could unwittingly or deliberately alter or delete some information from the cloud slave. Hence, the system must have to assure the, data integrity. The current authentication scheme for the cloud using is textual password & basic image password which we have demonstrated in existing work, so in sequence to get an Intelligence login model we require a secure login process in order to access our cloud properly & secure we are using an effective graphical login process which is derived on basis of assuming the probable security issue in current graphical password authentication scheme.

II. Literature Review

Here we are mentioning the literature review the works which have already done in the field of image password-

- Persuasive cued click point 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.

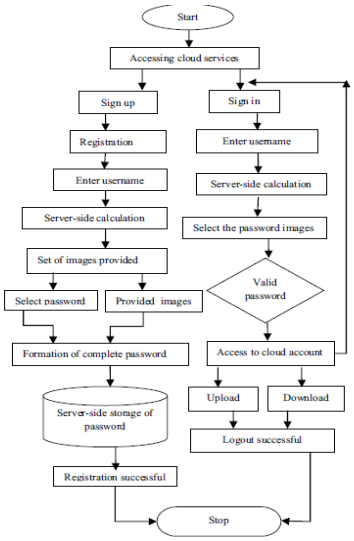
In this technique we are creating a password in particular hotpot area of an image, where we are selecting a particular portion to create a password, whereas in CCP we are going to create a password in whole image which give us less success rate in order to get into login process.
Still the problem into this scheme was to get good success rate while login into the system but effective in case of attack than textual password, so further enhancement moving to another graphical scheme.

- Taking the number of different images or set of images and selecting or more as a password, which is easy to remember and giving a good success rate than Previous demonstrated in fig-

Selecting one or multiple images from the given image dataset.

- Triangle scheme has been introduced to generate a triangle on to a large number of objects.
- Hybrid Textual scheme- Here user has to give rating to each sequence of colour or image so that here he/she need to remember while login.
- Calculation of the password from the combine effort of user & server – the password going to be four images –two from the user side & two from the server side.

Here based on four letter password & assign digit to each letter, sum of all digit is calculated & then two images has to be select by the user from the category of image subset which is the first digit of sum of digit which calculated automatically, & then server will give two images from server side and then combine all four images will treat as password.



Flow chart of last work done on image password authentication.

Till now the work up to this level has been done, which has been assumed to be worked with cloud. Here in our proposed system we are going to extend the available password scheme and going to show the authentication of cloud via our proposed scheme & also further we are going to check the authentication & then integrity verification about the data which we are storing into the cloud.

A. Our System And Assumptions

System components. The secure integrity verification cloud computing storage model on giving a solution to authenticate it, considered in this work consists of three main components

- Creating & implementing a new Graphical authentication scheme to the cloud
- a CSP who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files
- graphically giving access to authorized users — a set of owner's clients

Who have the right to access the remote data. Cloud computing data storage system model. The storage model used in this work can be adopted by many practical applications.

For example, in e-health applications, a trusted government organization can be considered as the data owner, and the physicians as the authorized users who have the right to access the patients' medical history stored on cloud servers.

The integrity of customers' data in the cloud may be at risk due to the following reasons. First, the CSP–

Whose goal is likely to make a profit and maintain a reputation – has an incentive to hide data loss (caused by incidents like hardware failure, management errors, malicious attacks) or reclaim storage by discarding data that has not been or is rarely accessed. Second, a dishonest CSP may store fewer copies than what has been agreed upon in the service contact with the data owner.

The authentication process is required to be considered at it best in order to get a proper authorization to proper user and give a best security level password scheme to compete its other competitor to provide best services.

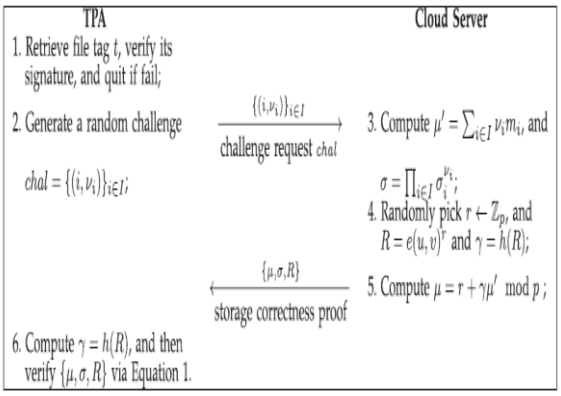
III. Research Finding/Objective

Here as we have described about our work – mainly our contribution will be for the cloud security solution in two ways-

- First most to authenticate in sequence to connect with the services of cloud account.
- Second once the user is connected security again user should be get assure about the security of data which kept into the cloud, so here we are providing a data verification technique to check data integrity.

Firstly, we get authentication via our effective password scheme & then verifying the data integrity with the procedure demonstrated in image.

The Privacy-Preserving Public Auditing Protocol



A. Problem Formulation
- Current password scheme (textual password) is sometime easy to memorized & sometime they face the problem of brute force attack or robot attack.
- Basic image password is hard to memorized sometime as it has to be chosen by the user and a set of images need to remember.
- Using over cloud is probably not been implement by any other CSP due to above reason.
- User not get ensured regarding the same data as uploaded to server- So as no proper checking mechanism has been given to detect it automatically on request by client to CSP.

B. Methodology/ Planning Of Work
- Enhanced Graphical password authentication module generation.
- B. Challenge Token Creation.
- C. Correctness Verification.

C. Software Tools:
- JDK 7.0
- NETBEANS IDE 7.1
- ORACLE/MYSQL.

D. Hardware Tools
- 2 GB RAM.
- 160 GB HARD DISK
- STANDARD MOUSE-KEYWORD

E. Work Plan

The proposed scheme consists of three procedures we are defining as given below-
- We are going to demonstrate efficient graphical password authentication scheme in sequence to authenticate the cloud.
- Generating an automated system to generate a key in order to calculate file verification factor (Fact).
- File verification at receiver end or request for data integrity verification.

Finally we are going to verify our level of security in terms of – method name & procedure, ease of use, Advantages & Disadvantages.

IV. Expected Outcomes

To Perform and provide a third party authentication in order to improve verification of data. Authentication Verifying the identity of a user, system or service. Authorization Privileges that a user or system or service has after being authenticated (e.g., access control), we need an efficient and good success rate in order to authenticate the server using enhanced graphical password authentication scheme.

V. Conclusion

Cloud Computing is gaining remarkable popularity in the recent years for its benefits in terms of resilience, scalability, accuracy and cost effectiveness. Although the entire obligation has one problem: Security.

In this paper, we studied the complication of data security in cloud data processing, which is essentially to appropriate cache. An effective and flexible appropriated scheme is proposed to ensure the login to cloud server are checking correctness of user data in the appropriate system. To perform high security and performance, we show that our scheme is highly efficient in recovering the singleton losses almost immediately and recovers from burst data losses.

References

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009, pp. 1–9.

[2] Cong Wang, Qian Wang, KuiRen, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011. Rampal Singh, IJECS Volume 2 Issue 3 March 2013 Page No. 825-830 Page 830

[3] A. Juels and J. Burton S. Kaliski, "PoRs: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

[4] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," Online at https://www.sun. Com/offers/details/sun transparency.xml, November 2009.

[5] M. Arrington, "Gmail disaster: Reports of mass email deletions," online at http: // www. techcrunch.com/2006/12/ 28/ gmail-disasterreports-of- mass-email-deletions/, December 2006.

[6] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.

[7] 7. T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, pp. 12–12, 2006.

[8] 8. B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.washingtonpost.com/securityfix/2009/01/ payment processor breach may b.html, Jan. 2009.

[9] 9. Amazon.com, "Amazon web services (aws)," Online at http:// aws.amazon.com/, 2009

[10] 10. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

[11] 11. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[12] Graphical password authentication – cloud securing scheme-2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies