Implementation of Authentication using Graphical Password for cloud Computing

Asif Shaikh[1], Rabbana Pathan[2], Rasul Patel[3], Asst. Prof. Shaikh Rukaiya[4]

[1,2,3] Student, Dept. of Computer, AAEMF'S COE, Pune, Maharashtra, India
[4]Asst.Professor, Dept. of Computer, AAEMF'S COE, Pune, Maharashtra, India

Abstract - *Now a day's security to the information which is stored in system is very important. Authentication is the operation to supply guaranteed information security and the graphical password authentication method is an easy and convenient process to provide strong authentication. The major problem of user registration, mostly text and number based password, is well known. If the login user be used to choose a simple password which is frequently in his mind it becomes straightforward for attacker to guess. If the password is machine generated it is mostly complicated for user to keep in mind. User verify password using cued click points graphical password scheme contains usability, and memo ability security evaluations. This paper is on enhanced user graphical password authentication with a usability and memo ability, so that users select more difficult or more random to guess passwords. In click-based graphical passwords, image or video frames provide database to load the images, and then give authenticated access to all data in database. User authentication, graphical password scheme, cued recall, video frame as a password, usability, memorability, security.*

Key Words: **Graphical Password, Encryption, Cloud computing, data duplication, load Balancing, AES Algorithm, OTP.**

1. INTRODUCTION

Cloud computing system is the newer version of utility computing which has replaced its area at various data centers. Cloud computing customers have complete access to information technology capabilities and services which is provided through Internet. Cloud computing has brought tremendous change in operations of IT industries. It has benefited the IT industries with less infrastructure investment and maintenance.

Cloud computing is becoming popular as virtualization power, distributed computing with server cluster and increase in the availability of broadband internet assessing is increasing. The IT world is looking forward for the services provided by cloud computing thus boosting up the development of cloud computing.

With cost-effectiveness improvements in computational technology and large-scale networks, sharing data with others becomes correspondingly more convenient. Additionally, digital resources are more easily obtained via cloud computing and storage. Since cloud data sharing requires off-premises infrastructure that some organizations jointly held, remote storage are somehow threatening privacy of data owners. Therefore, enforcing the protection of personal.

Computer security is critical in almost any technology driven industry which Operates on computer systems. The main aim in security is to provide a cryptographic system that are computationally in feasible for attackers to gain access to the system. When designing a computer system, there are many aspects to be taken into consideration, among that one of the main factories security, which prove to be very important. For Example the problem of integer factorization is a technique Used in RSA. The discrete logarithm is used in Diffie-Hellman Key Exchange, Digital Signature Algorithm, Elliptic Curve Cryptography and soon. These primitives are based on hard AI problems.

1.1 RELATED WORK

The proposed cloud storage service involves three different entities-

- ➢ The Data Owner is an entity that has large amount of files which are to be outsourced i.e. to be stored on cloud.
- ➢ The cloud server (CSS) is managed and maintained by the cloud service provider (CSP).
- ➢ The external third party auditor (TPA) who audits the data.

1.2 Software Requirement

1. Operating system : Windows 7 or Above
2. GUI creation : XML, JavaScript
3. Database : MySQL
4. IDE : NetBeans IDE

For developing this system we will required and Netbeans IDE and implementation language will be Java. Above mention software source are easily available on internet.

1.3 Hardware Requirement

1. System : Pentium IV 2.4 GHz. Requires internet connection
2. Hard Disk : 80 GB.
3. Monitor : 15 VGA Color.
4. Mouse : Logitech.
5. Ram : 512 MB.

1.3 PROBLEM STATEMENT

To implement a system that providing security by using Login with Graphical Password, Login with OTP and scalability to the cloud servers by checking the integrity and deduplication of data.

2. MATHEMATICAL MODEL

S = { I, P, R, O }

Where,

I is set of Initial Input to the system.

I = {i1, i2, i3}

i1 = File given by the user.

i2 = Download request from User.

i3 = Download request from Owner.

P is set of procedure or function or processes or methods.

P = {p1, p2, p3, p4, p5, p6, p7, p8}

p1 = Registration and Authentication.

p2 = Uploading a file on cloud server.

p3 = Fragmentation of file received from user.

p4 = Replication of that file.

p5 = Download Request from user.

p6 = Download Request from Owner.

p7 = Collection and reassemble of fragments.

p8 = Downloading the original file. R is a set of rules or constraints. R= { r1}

r1 = File accessed from Replication when network is busy.

O is a set of outputs.

O = {o1 }

o1 = Downloading the original file.

3. LITERATURE SERVEY

A. User interface design affects security: Patterns in click-based graphical passwords[1]:

Design of the user interface for authentication systems influences users and may encourage either secure or insecure behavior. Using data from four different but closely related click-based graphical password studies, we display that user-selected passwords change considerably in their predictability. Our post-hoc investigation looks at click-point patterns within passwords and displays that Pass points passwords succeed distinct patterns. Our analysis displays that many patterns appear across a range of images, thus motivating attacks which are independent of specific background images. Conversely, Cued Click-Points (CCP) and Persuasive Cued Click-Points (PCCP) passwords are nearly indistinguishable from those of a randomly-generated simulated dataset. These results provide insight on modeling effective password spaces and on how user interface characteristics.

Advantages:

Choosing the password is very easy.

Drawbacks:

There are many chances to guess the password by watching at screen.

B. A graphical password based authentication based system for mobile devices[2]:

Authentication is one the most necessary security primitive. Password authentication is most widely used verification mechanism. Password provides security mechanism for verification and protection services against unwanted access to resource. To address these verification problems, a new alternative authentication method have been proposed by the use of picture as passwords. Graphical passwords have been created to try to make passwords more memorable and very easier for people to use and there, more secure. Using a graphical password system, user click on images rather than type alphanumeric characters. In this paper, we have purposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attacks on graphical passwords. This scheme is proposed for mobile devices which are more close and convenient to use than traditional desktop computer systems.

Advantages:

The advantage of the approach is increasing security by providing password of higher security.

Drawbacks:

This system is not reliable and robust.

This system is not user friendly.

C. A behavioral biometric challenge and response approach to user authentication on Smartphone's[3]:

With the raises popularity of tablets and in view of the information and data that can be stored on the tablet, it is important to ensure the security of the information and data that is stored on the tablet. User authentication is a very essential security measure for protecting the data stored on the tablet because these devices have very higher risk of theft. Also, an attacker may get hold of the device after initial authentication has been done. Hence, a continuous authentication technique can either complement entry-point based authentication methods by monitoring the user after a successful login, or, if the method satisfies particular accuracy requirements, it could even substitute entry-point based authentication. In this research a classification framework for continuous authentication of users based on their interaction with touch screen devices has been studied. The classification framework will be explored Further to test the feasibility of using it for authenticating tablets users. The touch screen size of tablet is large as compared to smart-phones, therefore, the usage pattern may vary over a tablet as compared to smart-phone. In that research a feature set will be extracted from raw touch screen data and classification framework will be applied to test if this touch screen biometric can be used for continuously authenticating tablet users.

Advantages:

By using this system authentication techniques should be verified extensively for usability and effectiveness.

Drawbacks:

This system is based on text and image only.

This system is not user friendly.

D. A Survey on Different Graphical Password Authentication Techniques[4]:

To impose security of information, passwords were introduced. Text occupying password is a popular authentication method used from ancient times. However text based passwords are prone to various intrusion such as guessing attacks, dictionary attacks, brute force attacks, social engineering attacks etc. So many graphical password schemes have been proposed so far as it enhances security and password usability. In that paper, they conduct a comprehensive survey of the existing different graphical password techniques. We can categorize these techniques into four: pure recall based, recognition based, cued recall based and hybrid approaches. Here we analyze the strengths and drawbacks of each method. This survey will be particularly useful for researchers who are interested in developing new graphical password algorithms as well as industry practitioners who are interested in deploying graphical password techniques.

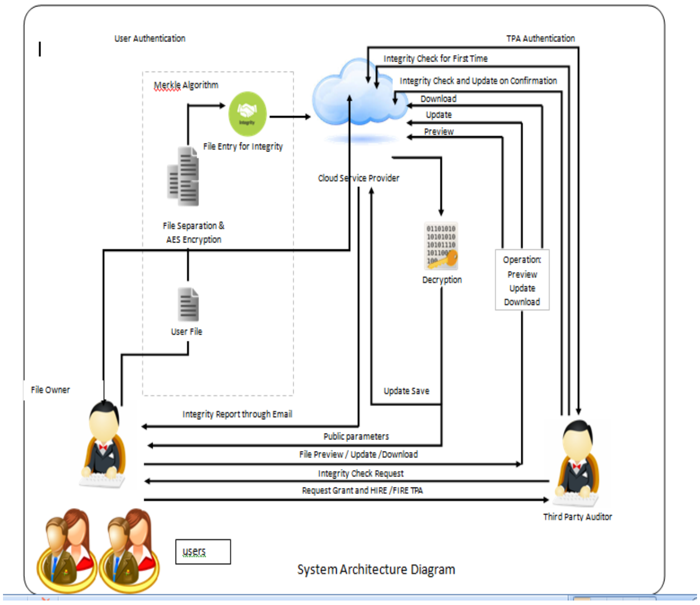
Advantages:

By using this system they survey on attack patterns and define common attacks in graphical password authentication methods.

Drawbacks:

This system is not secure, reliable and robust.

4. SYSTEM ARCHITECTURE



5. WORKING

5.1. USER REGISTER & LOGIN:

User registers with a name. email id, mobile number and password from the graphical password grid image.

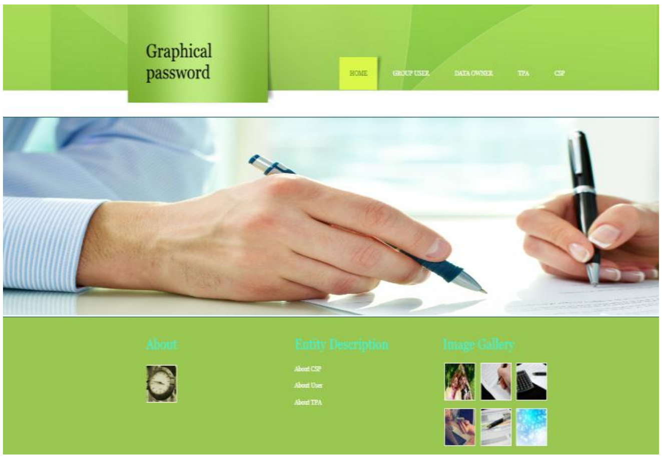
5.2 USER LOGIN

User have to login with the mobile number as a username and password as a grid based number provided by the login window. After entering the

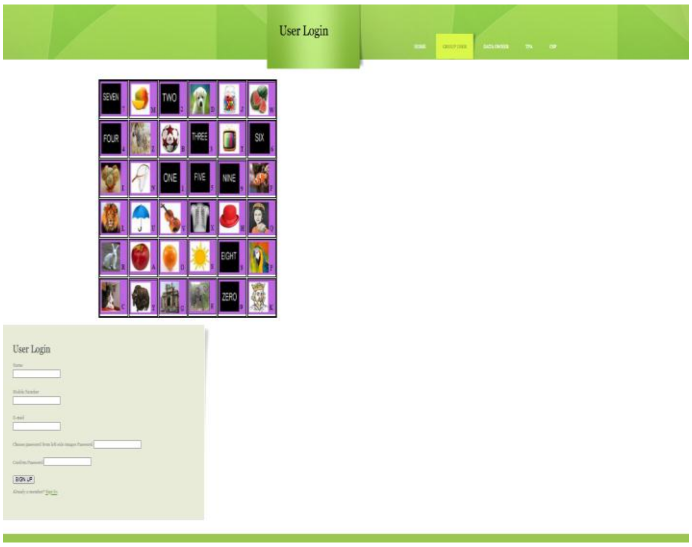
6. RESULTS

The results are as follows

6.1 HOMEPAGE



6.2 USER REGISTER



User Login

Name

Mobile Number

E-mail

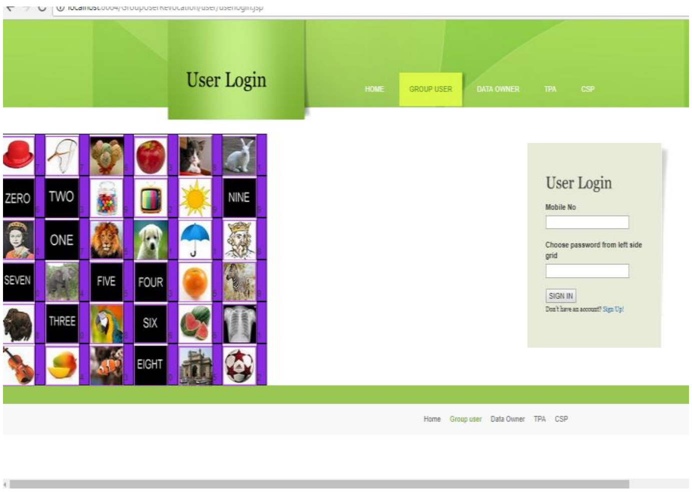
Choose password from left side images Password

Confirm Password

SIGN UP

Already a member? Sign In

6.3 USER LOGIN



User Login

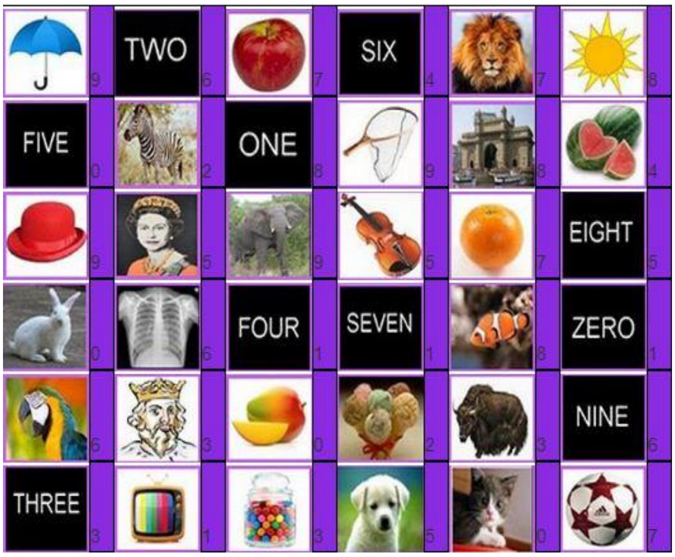
Mobile No

Choose password from left side grid

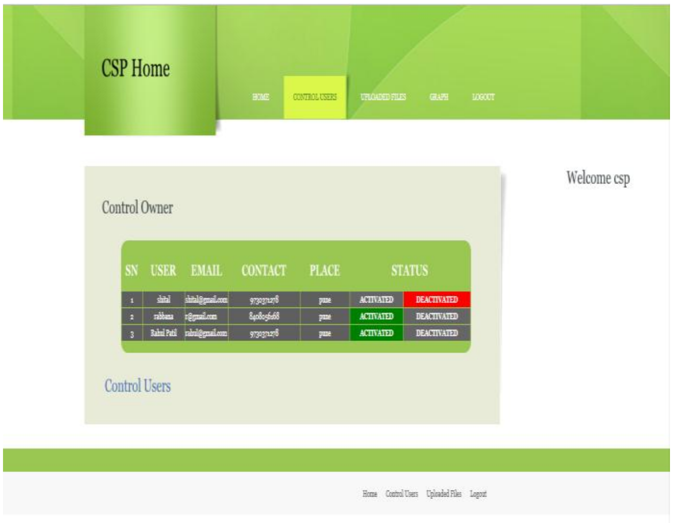
SIGN IN

Don't have an account? Sign Up!

6.3.1 GRAPHICAL PASSWORD



6.4 ACCOUNT ACCESS



Control Owner

SN	USER	EMAIL	CONTACT	PLACE	STATUS	
1	shital	shital@gmail.com	9730371278	pune	ACTIVATED	DEACTIVATED
2	rabbana	r@gmail.com	8408056168	pune	ACTIVATED	DEACTIVATED
3	Rahul Patil	rahul@gmail.com	9730371278	pune	ACTIVATED	DEACTIVATED

Control Users

6. FUTURE SCOPE:

Providing static time security is less secure than dynamic security mechanism. Our system is dynamically secure but in future we will need is more dynamic mechanism to secure our data. During graphical password processing speed is a biggest concern. So in future mechanism can be analyzed & faster scheme can be implemented with highly security.

7. CONCLUSION

The primitive of verifiable database with efficient updates is an important way to solve the problem of verifiable outsourcing of storage. We implemented a system with secure graphical password which allows authorization to user to secure datah user revocation are adopt to achieve the data integrity auditing of remote. Access control policies are to be established and client identities are to be checked. Datacenter platforms, infrastructure and client devices are to be secured by trusted computer policies. Enable secure migration from private cloud environment to public cloud providers.

REFERENCES

[1] Sonia Chiasson Alain Forget Robert Biddle P.C. van Oorscho - "User interface design affects security: Patterns in click-based graphical passwords", Copyright Springer-Verlag 2009. DOI 10.1007/s10207-009 -0080-7., January 2014.

[2] Er.Aman Kumar Er.Naveen Bilandi - "A graphical password based authentication based system for mobile devices", Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India, IJCSMC, Vol. 3, Issue. 4, April 2014, pg. 744–754.

[3] Burgbacher, U., Pratorius, M., Hinrichs, K.- ”A behavioral biometric challenge and response approach to user authentication on smartphones”, Systems, Man and Cybernetics (SMC), 2014 IEEE International Conference,pp.3328-3335, 5-8 Oct. 2014.

[4] Saranya Ramanan, Bindhu J S - “A Survey on Different Graphical Password Authentication Techniques”, PG scholar, Department of Computer Science, College of Engineering Perumon, Kerala, India Vol:2,Issue 12, December 2014.

[5] Gurav, S.M. Gawade, L.S., Rane, P.K., Khochare, N.R- ”Graphical Password Authentication: Cloud Securing Scheme”, Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference , pp.479 – 483, 9-11 Jan 2014.

[6] Ms. Shilpa Veerasekaran , Prof. Alka Khade , Prof. V.B Gaikwad- “Using Persuasive Technology in Click Based Graphical Passwords”,International Journal of Emerging Trends & Technology in Computer Science -Volume 3, Issue 2, pp.32-36, March – April 2014.

[7] Si Chen, Muyuan Li, Zhan Qin, Bingsheng Zhang- ” AcousAuth: An acoustic-based mobile application for user authentication”, Si Chen ; Dept. of Comput. Sci. & Eng., State Univ. of New York at Buffalo, Buffalo, NY, USA ; Muyuan Li ; Zhan Qin ; Bingsheng Zhang ,pp.215-216, April 27 2014-May 2 2014.