|  |  |  |
| --- | --- | --- |
| **Tech Saksham**  Final Project Report  **Track Name** |  |  |

**“Graphical Password Shuffling”**

**“** **Avanthi Institute of Engineering and Technology”**

|  |  |
| --- | --- |
| **ROLL NO** | **NAME** |
| 19Q61A05C2 | NEHA GUPTA |
| 19Q61A0568 | 1. SRI SOWMYA DEVI |
| 19Q61A0582 | MALLEPALLY MOUNIKA |

|  |  |
| --- | --- |
|  |  |
|  | Trainer Name: UMA MAHESHWARI |
|  | Master Trainer |

**ABSTRACT**

Graphical secret key will in general be an extremely encouraging and drifting elective system to conventional strategies like basic content secret word and alphanumeric passwords. It is the usability which pulls in individuals. Customary straightforward content passwords were too easy to even think about guarding the data and alphanumeric passwords had one tremendous inconvenience i.e., clients capacity to recollect these passwords. Beating these issues of old procedures, graphical secret keys woke up since it was a reality that individuals or clients will recollect the photos superior to the content or alphanumeric passwords. In this paper, a graphical secret key is created which is in a type of a 4X5 grid. The user has to select Pictures in pairwise fashion and shuffle them. The shuffle highlight of this graphical secret word will remain against different assaults.

**SYSTEM ANALYSIS**

# EXISTING SYSTEM

Graphical password schemes are often divided into three major categories supported the sort of activity required to recollect the password: recognition, recall, and cued recall. Recognition is that the only for human memory whereas pure recall is most difficult since the knowledge must be accessed from memory with no triggers. Cued recall falls somewhere between these two because it offers a cue which should establish context and trigger the stored memory. Among existing graphical passwords, CCP most closely resembles aspects of Pass faces, Story, and Pass Points. Conceptually, CCP could even be a mixture of the three; in terms of implementation, it is most almost like Pass Points. It also avoids the complex user training requirements found during sort of graphical password proposals, like that of Wein shall. Pass faces could even be a graphical password scheme based totally on recognizing human faces.

During password creation, users select kind of images from a much bigger set. To log in, users must identify one among their pre-selected images from among several decoys. Users must correctly answer kind of those challenges for every login. Proposed an alternate scheme, Story that used everyday

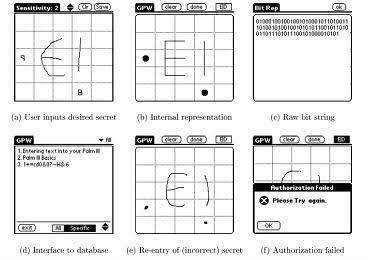
images rather than faces and required that users select their images within the proper order.

Users were encouraged to make a story as a memory aid. All Rights Reserved 396 in three separate in lab user studies to match text passwords to pass Points, test whether the selection of image impacted usability, and determine the minimum size of the tolerance square. the general conclusion was that Pass Points was a usable authentication scheme.

**RECOGNITION-BASED TECHNOLOGY**:

In recognition-based techniques, assessment is done by challenging the user to identify random images or images that the user had selected during the registration stage. Search metric systems are also known as Recognition based technology. It is generally requiring that users memorize a number of images during password creation, and then to log in, must identify their images among them. Humans have a unique ability to identify images previously seen, even those that have been viewed very briefly. Recognition based systems have been proposed using usability and security considerations and offer usability. In some of the graphical password schemes,

Knowledge of some details of the shared secret must be retained by the system, i.e., user-specific profile data example: in recognition schemes, the system already knows which image belongs to a user’s portfolio in order to display them. Sobrado and Birgit Scheme is one of the recognition- based systems that display a number of pass-objects (preselected by user) among with many other objects, the user should click inside the convex hull bounded by passobjects. In Pass, face scheme human faces are used as passwords. Dhamija and Perrig Scheme Pick several pictures out of many choices, identify them later in the authentication.



**RECALL-BASED TECHNOLOGY:**

In recall-based techniques, a user recalling the past represented activities. In the security process, the user will recall the password that has been created or selected during the time of registration. The user calls recallbased graphical password systems are referred to as a metric system that will be a secret drawing. The users typically draw their password either on a blank sheet or on a grid. The user can secure your password using various techniques in graphical authentication.

There are three different types of recall technique i.e.

1. Free recall.

2.Cued recall.

3.serial recall.

**FREE RECALL:**

The free call is basic recall technique where a person will study a list of items on each trail and

they start to recall the list in any of the order. In graphical password using the free recall technique, the user provides security to the system. The user creates a password during the time of registration in such a way that there will be a blank canvas and the user will draw a shape or an object as they required this is called free recall.

**CUED RECALL:**

The cued recall is the retrieval of memory using the help of cues. This technique contains

image that will be divided in the form of grids and the user will select the particular cue point that point will be represented using the pixel format this is called cued recall.

**SERIAL RECALL:**

The serial recall requires the user to remember the list of it's in a serial order only. This

technique contains an image in the form of grids or a plan canvas where the user need to will click a few points during the time of registration. The user needs to log in with the password by selecting the points in an exact sequence. This is called serial recall.

**3.1.3 CUED RECALL-BASED TECHNOLOGY**:

The recall may be a technique utilized in a graphical password as recovering the knowledge from the past. Graphical password is an alternate to text-based passwords that's mostly used and simply accessible to the users than the image password, but image password is more accurate than the text password. Several sorts of graphical passwords are proposed. Generally fixing of a text-based password should be strong i.e. the password contain particular rules supported the web site . If the user thinks to possess an easy password which will be easy for the attackers to predict the password. Our scheme makes choosing a safer password the “path-of-least resistance”.

In this password are created by positioning a “template” over a background image so the user fall with in the cut of the template. The user some times find it difficult for remembering the template and selected area of images in order that they will import the pictures as per the theme of the web site .

# 3.2 PROPOSED SYSTEM

The Graphical password helps the user to click on a particular point on the image. Picture password is represented in the form of grids. After inserting the image that image will be divided in the form of girds. The user needs to select the particular cue point for all the images in a sequence. The grid will be associated with the matrix value and that value will be stored into the database.

The authentication methods can be divided into three

1. Token-based authentication

2. Biometric-based

3. Knowledge-based authentication

**3.2.1 Token-based authentication:**

The token-based technology is the security technique for authentication that helps the users to login with the network or the server. It is the remote access servers that assign the user and gives the secret password. Eg: key cards, bank card and smart cards. The token-based also use the knowledge-based technique. We all use ATM cards where the card details and pin will vary from person to person. Biometric-based authentication: The biometric-based technique is a security process and manages physical and digital resources. Eg: Fingerprint, iris scan and facial recognition. Fingerprint security is used in many places

for different uses. There are many drawbacks as it is more expensive to buy and it will take more time to execute and identify the process. However, this method provides more security.

**3.2.2 Knowledge-based authentication:**

This technique is used for authenticating the system that included both text based.and picture-based passwords. The picture password has two techniques i.e.

**3.2.3 Recognition based and Recall based.**

Cued Click Points (CPP) is the proposed alternative to pass point. In CCP the user clicks one point on each image. Let us take if c=5 images each image will be given with a one-point on each image rather than different points on a single image. This shows us about the cued recall technique where the visual cues that should be a valid user and should click on the latest cue point. Clicking on one image then it moves to the next image with a sequence

of the path as they click. A wrong click leads an incorrect path which shows the authentication failure only in the final click. User can choose their images till a particular extent of the clicked point. If the resulting of images is not correct then they could create a new password with different images with different clicks.

**CHAPTER 1**

**INTRODUCTION**

Validation is the most crucial idea of security. Verification depicts a very significant job with regards to insurance of information. It is defined as a capacity where in, client needs to give a proof of his approval, set of certifications which thus ought to be actually like the current data put away in the framework, at that point the client will be approved or something else. Access control and responsibility of clients are the prime highlights of the verification. Authentication is the best way to confirm one’s character and qualifications to state whether the individual is approved to get to the assets and data. This personality of an individual can be anything including the advanced certificate to that site.

Text based passwords are not anchor enough for applications that authorize security by access control components. Validation dependent on text-based passwords has significant downsides. Text based passwords are exposed to phishing assaults and lexicon assaults. Text based secret key confirmation is not any more sufficiently secure to verify clients into the framework. Text based passwords stay universal, regardless of interminable analysis.

Verification is essentially classified into three unique sorts:

• Token Based Authentication is resolved based on what do you claim or what is in your ownership. For instance, school id of an understudy, permit to drive can go about as a character of the client. Models like ATM cards with PIN numbers. To make this strategy increasingly more grounded, it is utilized close by information based confirmation which is talked about underneath.

• Knowledge based systems are placed broadly being used. Involving both the dimensions i.e., text and picture based. Picture based dimension is additionally separated into two classes, review based: is client’s capacity to review and duplicate something which was at that point done while in enrolment; acknowledgment based: client will in general perceive similar pictures which he/she chose in the enlistment stage.

• Biometric Based Authentication reaches out to the information of recognizing the clients based on their standard of conduct. This technique deals with the establishment of what you are. Facial personality, eye scanner, voice recognition, fingerprints too are the examples of biometric verification.

Text based passwords were made for the clients to consider the usability factor. Utilization of pictures secret key appeared when it was reasoned that people are increasingly gifted in recollecting the pictures, pictures when contrasted with the series of characters. Greg Blender in 1996, defined the possibility of the graphical secret word and later, in light of this thought, numerous graphical secret key verification plans were made. Blender, thought of one such thought of graphical secret word where, client needs to pick couple of pictures and after that they need to choose similar locales while signing in, at that point the client will be validated.

Graphical password is a one of the processes to provide our security of digital device or important information. Alphanumeric password is an old traditional common authentication method. Practically this traditional method is too unsecure system. For example, attacker may easily guess user’s password, if user is not using a strong password. User may use same password for multiple device or site. These are all unsecure characteristics for normal user. And authentication is one of the important security points where user has active responsibility for their personal information security.

**CHAPTER 2**

**SERVICES AND TOOLS REQUIRED**

**HARDWARE REQUIREMENTS**

|  |  |
| --- | --- |
| • Processor | : Intel Pentium III |
| • RAM | : 64MB |
| • Hard Disk | : 10GB |
| • Monitor | : 15 VGA Colour |
| • Mouse | : Logitech or any other |
| • Keyboard | : Logitech or any other |

**SOFTWARE REQUIREMENTS**

* Language : Java

* Front End Tool : Java Swing

## • Operating System : Windows 2000 or XP or LINUX

**CHAPTER 3**

**PROJECT ARCHITECTURE**

**3.1 Architecture**

**USER FRONTEND BACKEND**

|  |  |  |
| --- | --- | --- |
|  | **HTML 5** | **NODEJS 14.0**  **Database** |

A diagram is the graphical presentation of a set of elements, most

often rendered as a connected graph of vertices (things) and arcs(relationships). We draw diagrams to visualize a system from different perspectives, so a diagram is a projection into a system. For all but the most trivial systems, a diagram represents an elided view of the elements that make up a system. In theory, a diagram may contain any combination of things and relationships.

In practice, however, a small number of common combinations arise, which are consistent with the five most useful views that comprise the architecture of a software-intensive system.

Design is done in various levels.

Structural design using **Data Flow Diagrams**

(OR)

Object oriented analysis and design using **UML**.

Database design using **E-R Diagram** and **Database tables**.

**CHAPTER 4**

**MODULES**

* User
* Admin

# MODULES DESCRIPTION

**USER:**

* + User has to register with necessary details along with details.
  + User can able to login with the username,password along with images whatever they are provided at registration.
  + Then the user can login with security images.
  + He/She can able to login with security then they can able to view their profile and view account balance.

# ADMIN:

* Admin can login with username and password.
* Admin can able activate users.
* Admin can able to view user details.

**SYSTEM TESTING**

**Introduction to Testing:**

Testing is a process, which reveals errors in the program. It is the major quality measure employed during software development. During software development. During testing, the program is executed with a set of test cases and the output of the program for the test cases is evaluated to determine if the program is performing as it is expected to perform.

**TESTING IN STRATEGIES**

In order to make sure that the system does not have errors, the different levels of testing strategies that are applied at differing phases of software development are

**TYPES OF TESTS**

# Unit testing

Unit Testing is done on individual modules as they are completed and become executable. It is confined only to the designer's requirements.

# Integration testing

Integration testing ensures that software and subsystems work together a whole. It tests the interface of all the modules to make sure that the modules behave properly when integrated together.

# 

# 

# System Test

Involves in-house testing of the entire system before delivery to the user. It's aim is to satisfy the user the system meets all requirements of the client's specifications.

# White Box Testing

In this the test cases are generated on the logic of each module by drawing flow graphs of that module and logical decisions are tested on all the cases. It has been uses to generate the test cases in the following cases:

* Guarantee that all independent paths have been Executed.
* Execute all logical decisions on their true and false Sides.
* Execute all loops at their boundaries and within their operational bounds
* Execute internal data structures to ensure their validity.

# Black Box Testing

In this strategy some test cases are generated as input conditions that fully execute all functional requirements for the program. This testing has been uses to find errors in the following categories:

* Incorrect or missing functions
* Interface errors
* Errors in data structure or external database access
* Performance errors
* Initialization and termination errors.

In this testing only the output is checked for correctness.

The logical flow of the data is not checked.

# Acceptance Testing

It is a per-delivery testing in which entire system is tested at client's site on real world data to find errors.

#### Test Approach :

**Testing can be done in two ways:**

* Bottom up approach
* Top down approach

**Bottom up Approach:**

Testing can be performed starting from smallest and lowest level modules and proceeding one at a time. For each module in bottom up testing a short program executes the module and provides the needed data so that the module is asked to perform the way it will when embedded with in the larger system. When bottom level modules are tested attention turns to those on the next level that use the lower level ones they are tested individually and then linked with the previously examined lower level modules.

**Top down approach:**

This type of testing starts from upper level modules. Since the detailed activities usually performed in the lower level routines are not provided stubs are written. A stub is a module shell called by upper level module and that when reached properly will return a message to the calling module indicating that proper interaction occurred. No attempt is made to verify the correctness of the lower level module.

**Validation:**

The system has been tested and implemented successfully and thus ensured that all the requirements as listed in the software requirements specification are completely fulfilled. In case of erroneous input corresponding error messages are displayed

**CONCLUSION**

Content passwords were depleted while ensuring the data and assets. Alphanumeric passwords was a cross breed technique, remained against all the different assaults for some time yet additionally got exposed to it's numerous inconveniences.Confirmation method created in this paper, utilizes both content and graphical secret key. Client gets the first secret word through his mail id which is alphanumeric in nature and client is offered freedom to change the secret word whenever he/she needs. Alphanumeric passwords may remain against speculating assaults for a while (if attacked).Adding graphical secret key to the validation gives on greater security level. Graphical secret key is in type of a framework 3x3, with shuffle include. Pictures chosen by client in the registration phase will be still shuffled at every login, which gives aggressor no preferred standpoint on overhang dropping. Created strategy gives two fold security check to the client to login. Hence, this verification is increasingly secure.

**REFERENCES**

1. A. Almulhem, “A graphical password authentication system,” in Internet Security (WorldCIS), 2011 World Congress on, pp. 223–225, IEEE, 2011.
2. X. Suo, Y. Zhu, and G. S. Owen, “Graphical passwords: A survey,” in Computer security applications conference, 21st annual, pp. 10–pp, IEEE, 2005.
3. O. Ayannuga Olanrewaju and F. Olusegun, “Graphic-text authentication of a window-based application,” International Journal of Computer Applications, vol. 21, no. 6, pp. 36–42, 2011.
4. A. F. Syukri, E. Okamoto, and M. Mambo, “A user identifification system using signature written with mouse,” in Australasian Conference on Information Security and Privacy, pp. 403–414, Springer, 1998.

[5]. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, “Design and evaluation of a shoulder-surfifing resistant graphical password scheme,” in Proceedings of the working

conference on Advanced visual interfaces, pp. 177–184, ACM, 2006.

[6]. M. G. Tuscano and A. Tulasyan, “Graphical password authentication using pass faces,” International Journal of Engineering Research and Applications, vol. 5, no. 3, pp. 60–64, 2015.

1. S. Man, D. Hong, and M. M. Matthews, “A shoulder-surfifing resistant graphical password scheme-wiw.,” in Security and Management, pp. 105–111, Citeseer, 2003.

[8]. M. Mihajlov, B. Jerman-Blazic, and M. Ilievski, “Recognition-based graphical authentication with singleobject images,” in Developments in E-systems Engineering

(DeSE), 2011, pp. 203–208, IEEE, 2011.

[9]. Y. Meng, “Designing click-draw based graphical password scheme for better authentication,” in Networking, Architecture and Storage (NAS), 2012 IEEE 7th International Conference on, pp. 39–48, IEEE, 2012.

[10].A. Bianchi, I. Oakley, and H. Kim, “Passbyop: bring your own picture for securing graphical passwords,” IEEE Transactions on HumanMachine Systems, vol. 46, no. 3, pp.

380–389, 2016.

[11].A. Bhand, V. Desale, S. Shirke, and S. P. Shirke, “Enhancement of password authentication system using graphical images,” in Information Processing (ICIP), 2015

International Conference on, pp. 217–219, IEEE, 2015.

1. A. Danish, L. Sharma, H. Varshney, and A. M. Khan,“Alignment based graphical password authentication system,” in Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on, pp. 2950–2954, IEEE, 2016.

[13].S. Agrawal, A. Z. Ansari, and M. S. Umar, “Multimedia graphical grid based text password authentication: For advanced users,” in Wireless and Optical Communications

Networks (WOCN), 2016 Thirteenth International Conference on, pp. 1–5, IEEE, 2016.

**CODE**

**https://github.com/nehagupta611/Graphical-Password-Shuffling**