IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105109

Graphical Password System Using Cued Points

Prasanna Lad[1], Shubham Thasal[2], Abhishek Shetty[3], Prof. Sanket Patil[4]

Student, Department of Computing, Vidyavardhini College of Engineering and Technology, Vasai, India[1]

Student, Department of Computing, Vidyavardhini College of Engineering and Technology, Vasai, India[2]

Student, Department of Computing, Vidyavardhini College of Engineering and Technology, Vasai, India[3]

Assistant Professor, Department of Computing, Vidyavardhini College of Engineering and Technology, Vasai, India[4]

Abstract: Usable security has interesting usable difficulties in light of the fact that the requirement for security regularly implies that standard human-computer communication approaches can't be effectively legitimately connected. A vital convenience objective for validation frameworks is to help clients in choosing better passwords. Clients frequently make paramount passwords that are simple for aggressors to figure, yet solid framework doled out passwords are troublesome for clients to recollect. So analysts of current days have gone for elective strategies wherein graphical picture are utilized as passwords. Graphical passwords basically use pictures or portrayal of pictures as passwords. A human mind is great in recalling pictures than printed character. There are different graphical password plans or graphical password programming in the market. Notwithstanding, next to no exploration has been done to break down the graphical password that is as yet juvenile. In this paper, Users click on a point for every picture for a grouping of pictures. So it becomes easy and interesting at for client. That is Cued Click Point algorithm. Client can login into any application or system by using our graphical password system.

Keywords: Cued Click Point (CCP), Tkinter, Authrntication, GUI.

I. INTRODUCTION

Cued Click Point is a click-based a graphical picture password system which is a successor of pass point strategy [1] [2]. There are numerous things that are "understand" about passwords, for example, that client can't recollect a solid password and that the passwords they can recall are anything but difficult to figure. A password verification framework ought to support solid and less unsurprising passwords while keeping up memorability and security [11]. This password confirmation framework permits client decision while affecting clients towards more grounded passwords.

The assignment of choosing feeble passwords (which are simple for assailants to figure) is increasingly monotonous, dodges clients from settling on such decisions. As a result, this confirmation plans makes picking a progressively secure password the easiest course of action. Instead of expanding the weight on clients, it is simpler to pursue the framework's proposals for a protected password - an element missing in many plans.

The customary alphanumeric passwords been utilized for verification have security and ease of use issues. The issue emerges on the grounds that passwords are relied upon to consent to two on a very basic level clashing prerequisites; the passwords ought to be secure and simple to recollect. Fulfilling these necessities is for all intents and purposes inconceivable for clients.

Research and experience have demonstrated that content based passwords are less human- accommodating. As per brain science thinks about, the human cerebrum is better at perceiving and reviewing pictures than content. Graphical password plot creates progressively secure passwords and thus keep clients from falling back on dangerous practices so as to adapt.

In Graphical based confirmation, Cued Click-Points utilizes a single click point on five unique pictures in grouping. The following picture showed depends on the area of the recently entered click-point, making a way through a picture set.

The Cued Click Point Authentication begins with the enrollment strategy, which incorporates both the enlistment stage and picture determination stage. The procedure stream begins from checking the client name and choosing a resilience level. When the client finishes all the client subtleties at that point continue to the following stage, which is choosing pictures and choosing click points on the five pictures. The client needs to choose a lattice square as his click point. This matrix square can be moved utilizing a revive catch. The client rehashes this procedure for 5 pictures. This procedure is called as CCP Creation. After finished with all these above methods, the client profile vector will be made which stores client subtleties, square arranges, click points, resistance esteem.

After this in the login strategy, the client first enters the special client name as same as entered amid enlistment. At that point pictures are shown ordinarily, without shading or the viewport, and rehash the succession of clicks in the right request. After finished with all these above systems, the client profile vector will be opened. The client profile made

amid the login stage is an impermanent vector which is utilized for approval. In the event that the client profile vector made amid the login stage and enlistment stage is same then client effectively signed in generally a mistake message will be shown.
The framework structured comprises of three modules [11], for example, client enlistment module, picture choice module and framework login module which are as appeared as follows:

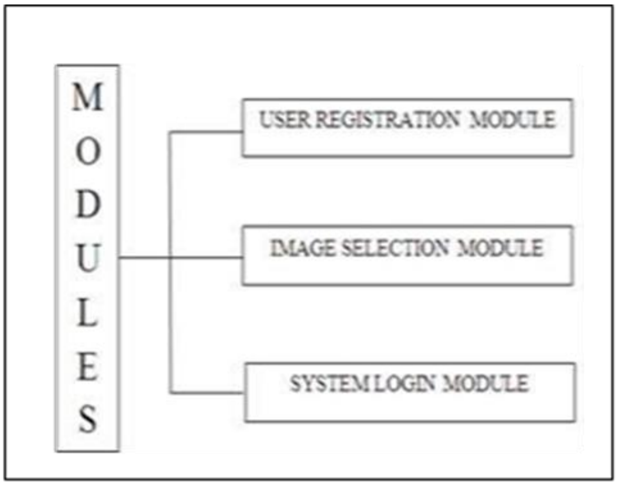


Fig.1. System Design Modules

II. Literature survey

Suvarna Pansambal (Shirke) and et al [12], abridges the idea of a graphical password framework. The essential idea of this framework is just the cooperation of the client with an arrangement of five pictures. The fundamental objective of this framework is to accomplish higher security and harder to figure by a programmer.
Sruthi P V [8] had been done work on graphical password verification. In the enrollment stage, the client enters all subtleties and chooses click point on pictures. On the off chance that all the click points are right, the framework will send an arbitrary powerful string/word to the client by email. At that point in the following page, a lot of pictures, each with the distinctive important word will be shown. Presently, the client will click on the picture with a similar string/word that he gotten by email. In the event that the chose picture is right, the login will be effective. The client can perform three fizzled endeavors after that login session will be terminated.
Tara H R and et al [10] basically center around click-based graphical passwords. Cued Click Points (CCP) was another graphical password conspire proposed, wherein client chooses a single click point on each picture instead of various click points on a solitary picture. Amid password creation, the client needs to choose the pictures, grouping of the pictures and a click point for each picture. This information is put away on a server which will confirm clients as they enter the graphical password. At the season of validation, the client needs to choose the right click point on every one of the pictures. Amid verification, the framework chooses the main picture to be shown. The client needs to enter click point on the picture as pictures are shown in a steady progression on the screen. Click point on each picture chooses the following picture.
Ansari Ahmed and et al [9] structured a click point-based method. Amid the enrollment stage, client needs to enter all subtleties. At that point the client has the opportunity to choose pictures which are put away on the customer machine or client can choose framework characterized pictures which are put away at the server side. The client can choose the method of trouble according to their benefit. The current framework just enables the client to enter the points with the assistance of the mouse paying little mind to that the client can be bear surfed by the aggressor or any unapproved client. In order to secure the honesty of the framework, they had presented BOGUS-POINTS and password fields. At the point when the client is approached to enter the points for verification he may enter n number of points on the pictures, in any succession. Be that as it may, the client must enter the right grouping.
Atish Nayak and Rajesh Bansode [11], centers around the fundamental assessment of the Persuasive Cued Click-Points graphical password framework which including ease of use and security assessment on three distinct dimensions. This paper utilized powerfully to impact client decision is utilized in click-based graphical passwords for urging clients to choose progressively irregular, and thus increasingly hard to figure, click-points. The methodology has demonstrated compelling at lessening the arrangement of hotspots and stays away from the shoulder surfing issue and furthermore give high-security achievement rodent, while as yet looking after ease of use.

DOI 10.17148/IJARCCE.2021.105109

Nikhil Bomanwar and Neha Singh [7], this paper quickly portrays the distinctive Graphical Authentication Schemes. Pass points, passwords comprise of a grouping of five click points on a given picture CCP comprises of password creation, wherein the client needs to choose the pictures, arrangement of the pictures and a click point for each picture. This information is put away on a server which will confirm clients as they enter the graphical password. This paper likewise conveys to see the Persuasive Technology which controls and urges clients to choose more grounded passwords, however not forces framework created passwords.
Uma D. Yadav and Prakash S. Mohod [6], centers around including more highlights in existing graphical password plans. The upgrades are realized by including the idea of modules wherein the main module manages setting the seed esteem or special and the later arrangements with offering resistance. To put it plainly, this paper involves upgrades in the current frameworks.

III. PROPOSED SYSTEM

These days keeping up security in any framework are the most difficult errand, in light of the fact that there are such a large number of approaches to break the current framework by means of password speculating calculation. The current framework experiences a ton of issues like printed passwords are difficult to recollect and furthermore there is plausibility of shoulder surfing.

Alongside that the biometrics utilized today are excessively expensive and difficult to keep up and pass point additionally experiences hotspot issue In a request to fulfill the inadequacies of the current content-based password frameworks and to make the framework progressively secure hacking we are building up another age of passwords that depend on pictures that can't be effectively anticipated.

A noteworthy objective of this examination is to find how to make information-based verification conspires that are essential, usable, and secure. In this paper, we are structuring the framework which utilizes the pixels of graphical pictures, which are treated as a password and dependent on that clients are verified.

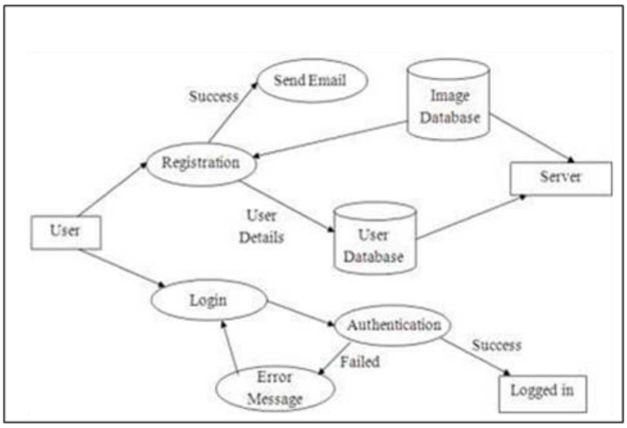


Fig. 2. Proposed System

Utilizing the CCP framework, we urge clients to choose increasingly secure passwords and to make it progressively hard to choose passwords. In particular, when clients made a password, the pictures were somewhat shaded with the exception of an arbitrarily situated viewport. The viewport is situated haphazardly as opposed to explicitly to maintain a strategic distance from known hotspots since such data could be utilized by aggressors to improve surmises and could likewise prompt the arrangement of new hotspots. The viewport's size was expected to offer an assortment of unmistakable points yet at the same time, spread just an acceptably little part of every conceivable point. The extent of the viewport relies upon the resilience esteem chosen by the client.

Clients were required to choose a click-point inside this featured viewport and couldn't click outside of this viewport. On the off chance that they were reluctant or unfit to choose a click-point in this district, they could press the "Revive" catch to arbitrarily reposition the viewport. While clients were permitted to rearrange as regularly as they needed, this altogether hindered the password creation process. The viewport and invigorate catch just showed up amid password creation. Amid password affirmation and login, the pictures were shown regularly, without shading or the viewport and clients were permitted to click anyplace. On the off chance that the client overlooked points, at that point new pictures showed dependent on the custom inquiry amid enrollment. What's more, clients again need to perform click point on the pictures

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105109

IV. IMPLEMENTATION

A. CUED CLICK POINT ALGORITHM

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point on each of c = 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging, as we discuss later. As shown in Figure, each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.

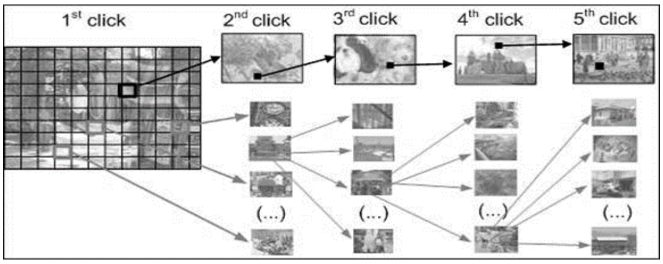


Fig.3. CCP passwords can be regarded as a choice-dependent path of images

Each of the 1200 next-images would have 1200 tolerance squares and thus require 1200 next-images of their own. The number of images would quickly become quite large. So we propose re-using the image set across stages. By reusing images, there is a slight chance that users see duplicate images. During the 5 stages in password creation, the image indices i1, ..., i5 for the images in the password sequence are each in the range 1 ≤ ij ≤ 1200. When computing the next-image index, if any is a repeat (i.e., the next ij is equal to ik for some k < j), then the next-image selection function f is deterministically perturbed to select a distinct image.

A user's initial image is selected by the system based on some user characteristic (as an argument to f above; we used username). The sequence is re-generated on-the-fly from the function each time a user enters the password. If a user enters an incorrect click-point, then the sequence of images from that point onwards will be incorrect and thus the login attempt will fail. For an attacker who does not know the correct sequence of images, this cue will not be helpful.

B. TKINTER

Python offers multiple options for developing GUI (Graphical User Interface). Out of all the GUI methods, tkinter is the most commonly used method. It is a standard Python interface to the Tk GUI toolkit shipped with Python. Python with tkinter is the fastest and easiest way to create the GUI applications. Creating a GUI using tkinter is an easy task. Importing tkinter is same as importing any other module in the Python code. Note that the name of the module in Python 2.x is 'Tkinter' and in Python 3.x it is 'tkinter'. i.e. Impot tkinter. There are two main methods used which the user needs to remember while creating the Python application with GUI.

Tk(screenName=None, baseName=None, className='Tk', useTk=1): To create a main window, tkinter offers a method 'Tk(screenName=None, baseName=None, className='Tk', useTk=1)'. To change the name of the window, you can change the className to the desired one. The basic code used to create the main window of the application is: m=tkinter.Tk() where m is the name of the main window object

mainloop(): There is a method known by the name mainloop() is used when your application is ready to run. mainloop() is an infinite loop used to run the application, wait for an event to occur and process the event as long as the window is not closed.

C. Python Library – PIL

PIL is the Python Imaging Library which provides the python interpreter with image editing capabilities. The Image module provides a class with the same name which is used to represent a PIL image. The module also provides a

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105109

number of factory functions, including functions to load images from files, and to create new images. PIL.Image.open() Opens and identifies the given image file.

D. Python Module - SHUTIL & OS

Shutil module in Python provides many functions of high-level operations on files and collections of files. It comes under Python’s standard utility modules. This module helps in automating process of copying and removal of files and directories.
shutil.copy() method in Python is used to copy the content of source file to destination file or directory. It also preserves the file’s permission mode but other metadata of the file like the file’s creation and modification times is not preserved.
Source must represent a file but destination can be a file or a directory. If the destination is a directory then the file will be copied into destination using the base filename from source. Also, destination must be writable. If destination is a file and already exists then it will be replaced with the source file otherwise a new file will be created.
The OS module in Python provides functions for interacting with the operating system. OS comes under Python’s standard utility modules. This module provides a portable way of using operating system-dependent functionality. The *os* and *os.path* modules include many functions to interact with the file system.

E. SQLITE

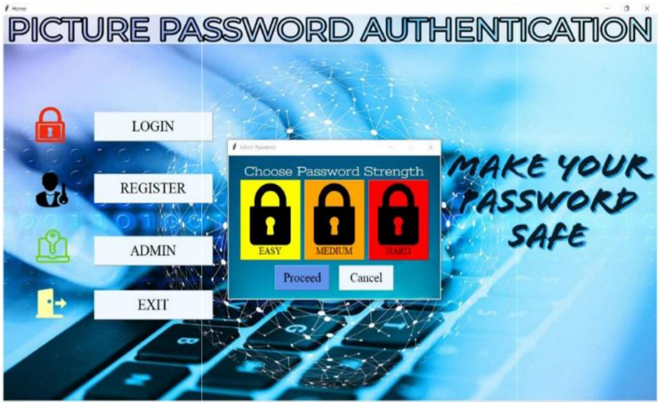
SQLite3 can be integrated with Python using sqlite3 module, which was written by Gerhard Haring.
To use sqlite3 module, you must first create a connection object that represents the database and then optionally you can create a cursor object, which will help you in executing all the SQL statements.

sqlite3.connect : This API opens a connection to the SQLite database file. You can use ":memory:" to open a database connection to a database that resides in RAM instead of on disk. If database is opened successfully, it returns a connection object.
When a database is accessed by multiple connections, and one of the processes modifies the database, the SQLite database is locked until that transaction is committed. The timeout parameter specifies how long the connection should wait for the lock to go away until raising an exception. The default for the timeout parameter is 5.0 (five seconds).

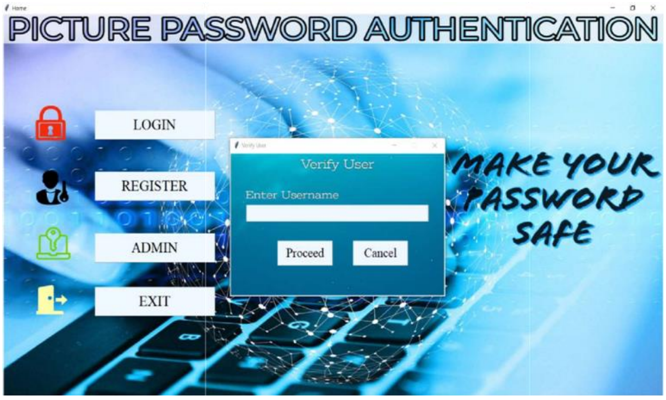
If the given database name does not exist then this call will create the database. You can specify filename with the required path as well if you want to create a database anywhere else except in the current directory.

cursor.execute : This routine executes an SQL statement. The SQL statement may be parameterized (i. e. placeholders instead of SQL literals). The sqlite3 module supports two kinds of placeholders: question marks and named placeholders (named style).

F. RESULT



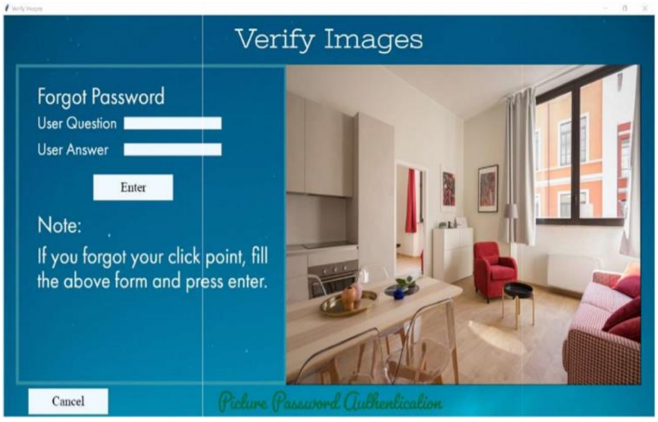
DOI 10.17148/IJARCCE.2021.105109



PICTURE PASSWORD AUTHENTICATION

Verify User

Enter Username



Verify Images

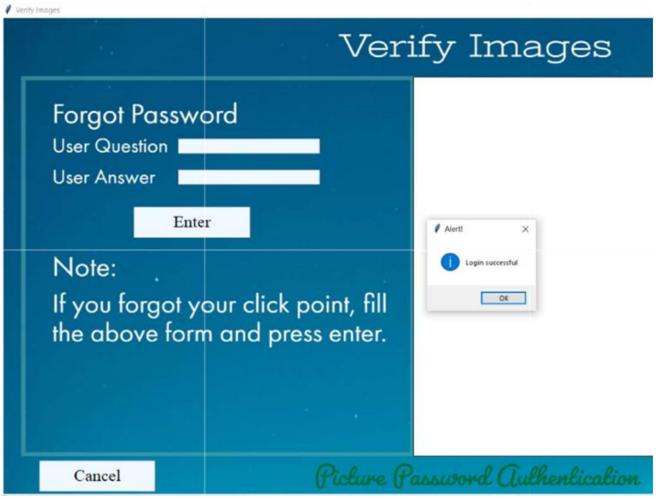
Forgot Password

User Question

User Answer

Note:

If you forgot your click point, fill the above form and press enter.



Verify Images

Forgot Password

User Question

User Answer

Note:

If you forgot your click point, fill the above form and press enter.

Alert!

Login successful

V. CONCLUSION

The proposed framework goes for giving less unsurprising passwords to clients as it focuses on the real preferred standpoint of human brain science of recalling designs instead of content. Additionally it disheartens the determination of known hotspots. Accordingly the adequate password space is expanded. This framework anticipates giving an advantageous UI to the clients along these lines giving adaptable utility. The discretization framework adds to the higher security than that given by other costly verification framework (for example biometrics) henceforth diminishing the viable expense.

CCP offers an exceptionally secure option in contrast to existing frameworks. CCP builds remaining burden for assailants by driving them to initially obtain picture sets for every client and after that direct hotspot examination on every one of these pictures.

DOI 10.17148/IJARCCE.2021.105109

REFERENCES

[1] S. Chiasson, A. Forget, O. Biddle, P.C. van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," published in IEEE transactions on dependable and secure computing, vol. 9, no. 2, pp.222-235, Apr. 2012.
[2] Vaibhav Moraskar, Sagar Jaikalyani, Mujib Saiyyed, Jaykumar Gurnani, Kalyani Pendke, "Cued Click Point techniques for graphical password authentication," International Journal Of Computer Science And Mobile Computing, Vol.3 Issue.1,
[3] Ian Jermyn, Alain Mayer, Fabin Monrose, Michael K. Reither, Aviel D. Rubin "The design and analysis of graphical passwords", Proceeding of The 8th UNISEX Security Symposium, 1999.
[4] Suo, Ying Zhu, G. Scott,Owen Xiaoyuan, "Graphical passwords: a survey", (Department of Computer Science Georgia State University).
[5] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, 2007.
[6] U. D. Yadav, P. S. Mohod "Adding Persuasive features in Graphical Password to increase the capacity of KBAM," Published in IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, vol.2, Mar.2013, pp.513- 517.
[7] Neha Singh, Nikhil Bomanwar "Improves Authentication Scheme Using Password Enables Persuasive Cued Click Points", Published in IEEE International Conference on Green Computing and Internet of Things (ICGCIoT),, vol. 00, Oct 2015, pp. 1394- 1398, 2015,
[8] Sruthi P V, "CRASH-Cued Recall Authentication Resistance to Shoulder Surfing attack", Published in IEEE International Conference on Green Engineering and Technologies(IC-GET 2015), Nov 2015.