Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 4- Issue 1, Paper 3, January 2021

CYBERING PRIVATE FOOTAGE VIDEO SECURING TOWARDS UNPREDICTABLE IMAGING PATTERNS

R.R.Prianka[1], K. Yuvalakshmi[2], S. Usha[3]
Assistant Professor[1] Department of Computer Science and Engineering
RMK College of Engineering and Technology, Pudhuvoyal, Chennai.
priankacse@rmkcet.ac.in, usha17cs105@rmkcet.ac.in, yuva17cs111@rmkcet.ac.in,

Abstract— *Securing the video footages of the high authenticated confidential places is very important at present in the market. Authentication is an obligatory factors of technological world concerned with security. Multifactor authentication becomes familiar due to two way authentication process which is proposed by google .In this research we will have the two step verification in the pc itself instead of depending on the external devices. Text based Password and Picturing Location based hotspot.In the existing methodology, an authentication by means of user security input in the form of text is utilized. This can be replaced with confusion picture matrix in which the user will be redirected to some other pictures which results in blocking of the user itself. The successive selection of the exact hot spots in the splitter image will enable the user to move to the next successful images. This hotspot will be another way prominent way of authentication.*

I. INTRODUCTION

In network security provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. Securing the private sectors video footages from unwanted access and creating a multiple layers with unpredictable patterns is the right chance of safeguarding the video footages.

The thought of captcha to interpret the licensed human is incorporated that prevail the human illation with the server by crypto logic ideas. Image hotspot technique concomitant with the notion of captcha styles the system in increased approach with security live. An ordered image hotspots has been designed by suggests that of graphical illustration or clued points on the image taken. On the thriving traversal of the five ordered hotspot pictures, the user get genuine to the server. The ordered traversal of hotspot image will been known by pattern matching situation so as to correlate the licensed user's click points within the hotspot.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 4- Issue 1, Paper 3, January 2021

To extend the multiple variety of hotspot level to avoid the vulnerability of the system. Conjointly the pattern matching technique wont to distinguishing the approved users supported our entered hotspot level. Video Footages of the Shopping Plaza. Instead of accessing DVR and improper UI, This research provides an optimized interactive Video UI to access the footages in a secure manner.

II METHODOLOGY

This system uses the concept of image patterning which provides high security. It makes user to select password in a more secured way. To select or to create password user is presented with a three image. When user selects a hotspot on a image, within the view port, out application will present the user with a new image based on the hotspot selected. When the user is done with selecting his choices, that information is mapped with the username and saved in a database. To login for username that is for textual password, they should use the correct sequence of click points. This system will be difficult for attackers where the sequence of image cannot be predicted easily. This method does not provide any alert messages, if the chosen hotspot is wrong, then he will be blocked directly by blocking his MAC and IP addresses. It will be known to them only during the final click point. So the chance of guessing the sequence is very low.

Hotspots are definite areas in the image that have a higher chance of being chosen by users as part of their passwords. If attacker is smart enough in guessing the hotspots in an image, then a dictionary of passwords containing combinations of these hotspots can be built. Providing security to the video footages is one of the most challenging job in the world of security system, so that unauthorized user is unable to view the footages without the permission. Taking in action all these things, we can design a software model which provide image based authentication as well as encryption using Fast Segmentation Algorithm.

The Design And Analysis Of Graphical Password in this paper provides a basic analysis of a cheating problem in the Analysis Of Graphical Password, and present the cheating method applied it to attack on the Analysis Of Graphical Password .Here is the list of points introduced in the paper : (a) each participant can't gain any useful information from his shares, (b) each pixel has the same number of black and white sub pixels in the secret share and in the verification share, (c) one's verification image will be recovered by stacking of his verification share and the secret share, (d) the secret image can be revealed by stacking all the secret shares. This paper didn't dealt with the performance of the system and it provides a mathematical approach with formulas. But the author didn't provide an exact statistics for the same. No clear inputs on the sub pixel division in the project.

Graphical passwords are an alternative to text passwords, whereby a user is asked to remember an image (or parts of an image) instead of a word.For generating Purely Automated attacks, we introduce a graph-based algorithm to efficiently create dictionaries based on heuristics such as click-order patterns .For simplicity some steps of the original window clustering algorithm is skipped at implementation, which ended up in four main steps: gradient computation, orientation binning, descriptor blocks and block normalization. In this project, there is no clear details on the security part.

This paper classifies the image retrieval into text based and content based, including the newly

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 4- Issue 1, Paper 3, January 2021

growing ontology based image retrieval system as one focus.Phishing—password theft via fake websites—is an extremely worrying, widespread phenomena. With billions of dollars lost and a large increase in the amount of attacks, it's clear that today's defenses aren't adequate. Zero truncation of the pixel value is an added advantage in this project.

A topic that has been the subject of active research as a replacement of alphanumerical passwords. The term ``hot spot password'' refers to many different graphical authentication methods, which can be broadly classified in three categories: 1) recall, 2) recognition, and 3) cued-recall passwords. A detailed comparison is taken for object recognition and mutual information for focus of attention mechanisms that is rapid localization based on a few classifiers. In this project, there are no clear details on the security part. They didn't specify the performance clearly in the system and lot of analysis were missed in this paper.

OBTAINABLE SYSTEM

Security plays a major role in the authentication process in high severity applications. Passwords are the type of secret code used in the process of authentication. In the existing system, a captcha and picture based authentication is designed to authenticate into the system. The concept of visual cryptography has been integrated with the captcha for individual user and got splitted equally in order to store in the server. The Server provide authentication to the requestor thereby verifying the captcha by merging the splitted shares to ensures the authorized human interpretations. The authentication by means of picture also been the part of the existing methodology that has a feature of picture spot clicking password.

III. PROJECTED SYSTEM

The drawback of the existing system is that only a specific number of pictures can be utilized to set as a password and there is no successive cued clicks. The vulnerability of cracking the password is high that leads to insecurity.

The projected system encompasses severe security outlook to design a secure authentication system.The concept of captcha to interpret the authorized human is incorporated that prevail the human inference with the server by cryptographic concepts.Image hotspot technique accompanying with the notion of captcha designs the system in enhanced way with security measure. Successive image hotspots have been designed by means of graphical representation or clued points on the image taken.On the thriving traversal of the 5 successive hotspot images, the user gets authenticated to the server.The successive traversal of hotspot image can been identified by pattern matching scenario in order to correlate the authorized user's click points in the hotspot. The drawback of the existing system is that only a specific number of pictures can be utilized to set as a password and there is no successive cued clicks. Hence the vulnerability of cracking the password is high that leads to insecurity.

IV. IMPLEMENTATION

In this module, the user is permitted to provide the basic authentication information like Username, Password, contact information.After providing the user information, the user is permitted to select the images and provide appropriate ranking to those images.Once the images were provided with ranking, appropriate image points were selected in the next module. In this module, we are providing an option of providing custom images for the user. Our system provides a strongest checks on the duplication of

ranking and multi selection of images without a boundary limit. In this module, the user is permitted to provide the basic authentication information like Username, Password, contact information. After providing the user information, the user is permitted to select the images and provide appropriate ranking to those images.Once the images were provided with ranking, appropriate image points were selected in the next module.In this module, we are providing an option of providing custom images for the user.Our system provides a strongest checks on the duplication of ranking and multi selection of images without a boundary limit.

In this module, the users were provided an option of selecting the hotspots in the hierarchy of the images.Once the hotspot is identified, the relevant point boundary of the hotspot is identified with the help of fast segmentation algorithm.Appropriate pixel values of box shaped were taken to avoid discrepancy in identifying the hotspot during authentication page.Once the first level of images were identified for the hotspot, the second level of images were placed for the hotspot. A similar algorithm is implemented to scale up the exact location of the hotspot.After that, based on the image ranking for the user, the hotspot on the next level of hierarchical images were identified. This process becomes a recursive process for the successive images. To make the fake users to deviate from the original image. Fake hotspots on the fake images were placed in a hierarchical manner.The hotspots will be placed with the help of segmentation algorithm. Appropriate pixel values of box shaped were taken to avoid discrepancy in identifying the hotspot during authentication page.The fake images with fake hotspot on the images will increase the complexity of the authentication scheme.The process will be followed as specified in the previous modules.

The fake images redirect the user to the wrong path and end up with blocking the user.On successful finding of the hotspot. The steps move further with valid successive images and end up with the block unlock module. The users were provided with permissible number of access on the authentication page. If they couldn't access the content, in that case the user's IP Address and MAC address will be blocked by the system to prevent future access on the system. Once the user needs to access the data, a special request to the admin followed by the admin unlocking the system.

V. SYSTEM DESIGN

The software requirements specification is produced at the culmination of the analysis task. The function and performance allocated to software as part of system engineering are refined by a complete information description as functional representation of system behaviour and design constraints, appropriate validation criteria.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 4- Issue 1, Paper 3, January 2021

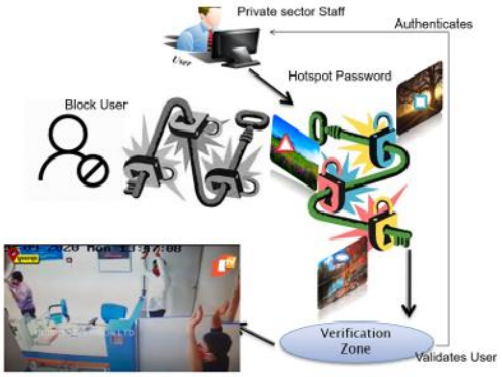

Figure :System Architecture

User enters the correct hotspot and directs to successive images if it is correct .Later it directs the user to the textual password verification .If the hotspots are not correct in the initial stage then the user will be blocked by blocking the IP and MAC address.

VI. RESULTS AND DISCUSSIONS

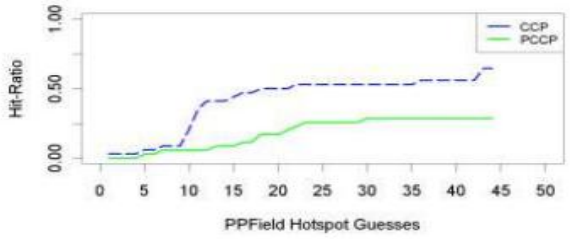

Figure: HotspotGuesses

Persuasive cued click points in which a password consists of five click-points, one on each of five images. During password creation, or during registration most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in figure. Users must select a click-point within the view port, and they cannot be able to click anywhere outside the viewport that is outside the view port clicking action does not work.

Viewport is nothing but a framed area. Within that random view port range there would be several tolerance squares per image or we can say tolerance area, tolerance area is nothing but the collection of all points closed to the clicked password point. If they are unable or unwilling to select a point in the current viewport, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the viewport moves to the specific location.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 4- Issue 1, Paper 3, January 2021

VII. CONCLUSION

We have generated CAPTCHA is splited into two by the thought of visual cryptography within the server for authentication functions and merged to verify the credibleness. Within the planned methodology, a Graphical Image secret has been designed that gives the users with associate degree choice to choose the hotspots within the hierarchy of the photographs. The sequential choice of the precise hot spots within the splited image can modify the user to maneuver to subsequent thriving pictures. These hotspots are the approach differently in a different way in our own way otherwise outstanding way of authentication.

VII. FUTURE WORK

In this project we are going to secured way authentication in web security vulnerabilities and identifying the attacks from hackers. It could be a valuable process to securing our website. In future it can be able to handle in a secured authentication while hot spot generates the fake clued click point to make more secured it can send alert messages to mobile phones and in email which has been blocked ip address and mac address as a text. So the user can identify the intruders.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4, 2020.
[2]Stobert, S. Chiasson, A. Forget,R. Biddle, and P. C. van Oorschot. Exploring usability effects of increasing security in click-based graphical password. In Annual Computer Security Applications Conference (ACSAC), 2010.
[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX SecuritySymp.*, 1999, pp. 1–15.
[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008.
[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphicapassword system," *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005
[6] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawngraphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.
[7] K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007, pp. 343–358.
[8] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proc. Symp. Usable PrivacySecurity*, 2007, pp. 20–28.
[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in *Proc. USENIX Security*, 2007,pp. 103–118.
[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," *IEEE Trans. Inf.Forensics Security*, vol. 5, no. 3, pp. 393–405, Sep. 2010