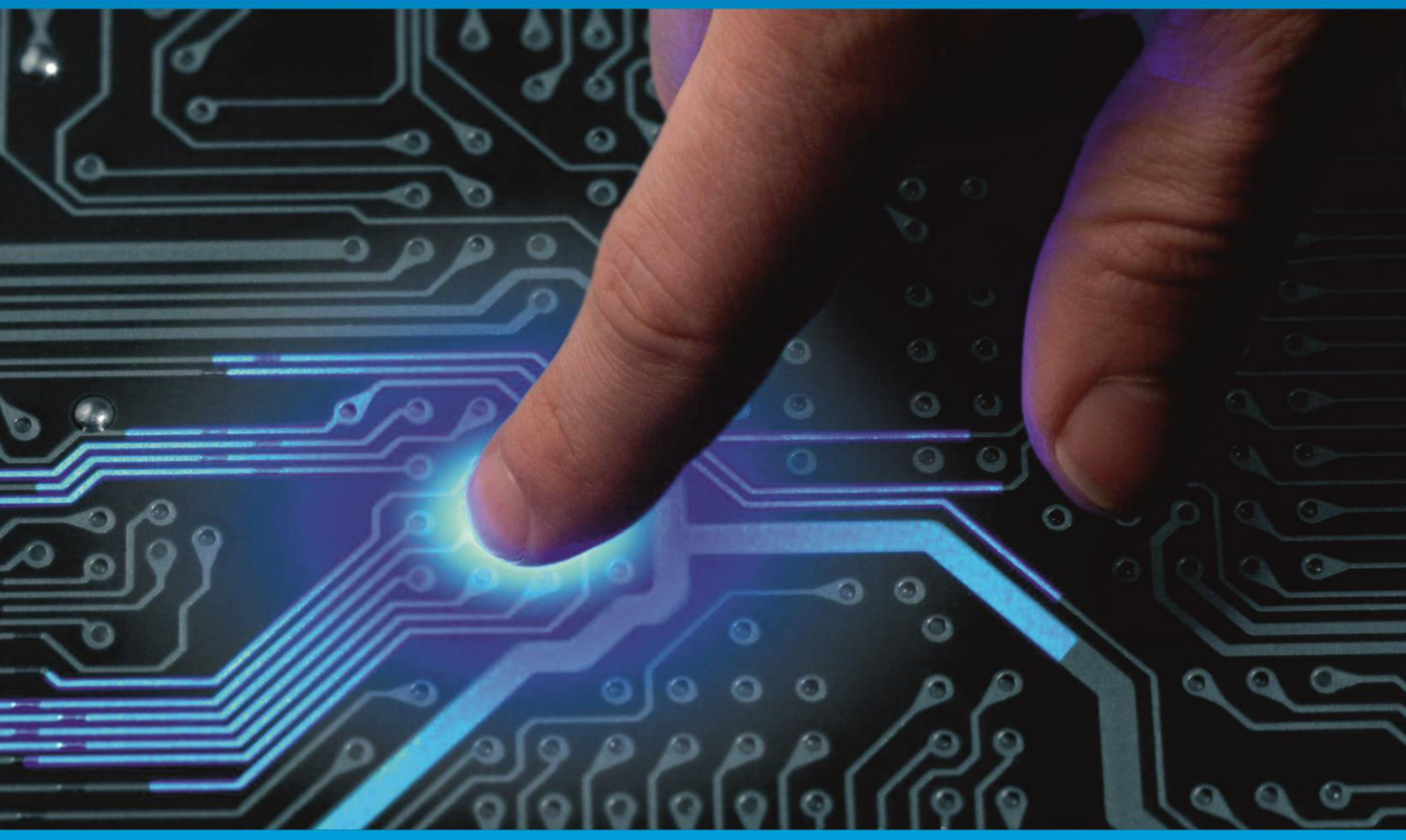
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905265 |

New Security Authentication with Graphical Passwords for Multi Images

B.Manjubashini, V.Gopi, A.Karthikeyan, A.Gokulraj, A.Eniyavan

Assistant Professor, Department of Computer Science and Engineering, Mahendra Institute of Technology Autonomous Namakkal, Tamilnadu, India

Department of Computer Science and Engineering, Mahendra Institute of Technology Autonomous Namakkal, Tamilnadu, India

ABSTRACT: In this era of digital world we are going towards digital transactions and we are getting depended on it that is why security is concerned for better authentication system or defend from various attacks. In the traditional authentication system, we have to create username and password, username as per availability and password as per your choice. It requires inputting your password through keyboard which may crack using brute force attack. We require a system that can protect from brute force attack and by having this issue CAPTCHA as graphical password has been introduced which can protect from various attacks. In graphical password we have to click on graphical objects either it may be alphabets or numbers. But now there are so many intelligent computer vision as well as image processing systems have been introduced which may break the security system of graphical password. Here we require an advanced graphical password which would be almost impossible to break. The proposed system develops a system that can enhance the level of graphical password and make secure from various attacks.

KEYWORDS : CAPTCHA, Authentication, Graphical Password, Image processing, Security.

I. INTRODUCTION

CAPTCHA (Completely Automated Public Turing Test to tell a Computers and Humans Apart) is a way to identify whether the user is bots or human. This is turing test which require to perform specially while performing transactions as well as while getting register. This technique has been used for authentication system also. CAPTCHA as a graphical password is represented on behalf of that. This technique turns the system more secure for inputting the sensitive information like username and password. In graphical CAPTCHA it requires to input your password from CAPTCHA by clicks. You will have to identify the alphabets or numbers and select your password from those distorted letters and after this you can only login by graphical CAPTCHA. Input box will not let you type through key board. As we know that distorted letters are supposed to not recognizable by robot and easily identified by human indeed, that is why this may provide best security in the field of authentication.

Fig1: CAPTCHA as a graphical password

Mostly, the security is provided by using the cryptographic primitives that are based on hard mathematical problems which are intractable. For example, the RSA public key cryptography depends on the integer factorization. The security

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905265 |

primitive that is developed using the hard AI problems is CAPTCHA. Captcha is used to distinguish the human and the computer bots. The need to develop the Captcha as a security primitive has risen when an organization conducted the online poll. The online poll ended as a fraud because some computer programs are used to vote in the poll. These Captchas are hard to break by computers and easy to humans. So, Captcha is a widely known internet security primitive which is used in many applications like email and other services to resist from bots.

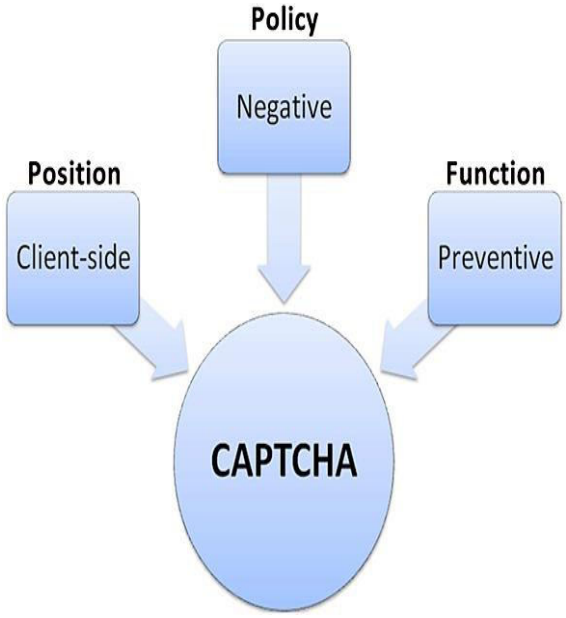


Fig2: Architecture

However, Captcha has achieved less when compared with the cryptographic primitives. In this paper, we are suggesting a new security approach which works based on hard math problems which is Captcha as gRaphical password (CaRP). It is a clickbased approach and user has to click on the sequence of the images which were selected while creating the password to get the access. The images in the Captcha are randomly ordered and a new CaRP image will be generated for every login attempt. There are two kinds of CaRP: one is text CaRP and the other is Image-recognition CaRP. The text CaRP is nothing but a sequence of characters as password which is entered by clicking the characters on the CaRP image in a right sequence. CaRP protects against online dictionary attacks and is a severe security risk for many online services. It also provides the security against the relay attacks which is bypassing the Captcha. It also provides security against the shouldersurfer attacks if the dual-view technology is combined with the CaRP. The CaRP can also work with touch screen devices which mitigate typing the passwords and also increase the operating cost of the spammer's.

II. BACKGROUND AND RELATED WORK

A. Graphical Passwords Earlier multiple graphical password schemes were proposed and they were classified in to three groups according to the complexity involved in memorizing and entering passwords: recognition, recall and cued call. These categories will be illustrated here. Most of the psychological studies support that it is easy to remember the images than text for humans [6].

A recognition-based scheme need to be identified among decoys the visual objects pertaining to a Password portfolio. A complex scheme is passfaces where a user selects a portfolio of faces from a database in creating password. During authentication process, a panel of candidate faces were given to the user to select the face belonging to her portfolio. This procedure is repetitive for several rounds, every round with a different panel. A successful login need correct selection in each round. The set of images in a panel will be same between logins, but their locations were altered. It resembles passfaces but images in the portfolio are arranged in order, and a user should identify her portfolio images in the correct order. Cognitive Authentication need a user to generate a path through a panel of images as mentioned: Starting from the top-left image, scrolling down if the image is in her portfolio, or right otherwise. The user recognizes among decoys the row or column label that the path ends. This procedure is duplicated, each time with a different

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905265 |

panel. A successful login requires that the total probability that correct answers were not listed by chance exceeds a threshold within a given number of rounds.

A recall-based scheme needs a user to regenerate the similar interaction result without cueing. Draw-ASecret (DAS) was the first recall-based scheme proposed. A user pulls her password on a 2D grid. The system converts the sequence of grid cells adjacent to the drawing path as a user drawn password. Pass-Go improves DAS's usability by encoding the grid intersection points rather than the grid cells. BDAS adds background images to DAS to encourage users to create more complex passwords.

In a cued-recall scheme, an external cue is given to help memorize and enter a password. Pass Points is a extensively studied click-based cued-recall scheme where a user clicks a series of points anywhere on an image in creating a password, and re-clicks the same series during authentication. Among the three types, recognition is considered the easiest for human memory whereas recall is the hardest. Recognition is weakest in resisting guessing attacks

Captcha depends on the efficiency between humans and robots. There are two categories of visual Captcha (text Captcha) and Image-Recognition Captcha (IRC). The first category depends on recognition of character and the other depends on recognition of non-character objects. The security of text Captcha depends on the character segmentation difficulty which is more expensive and hard to implement [5]. It is easy to read the characters than the non-characters.
In principle, the visual Captcha schemes which are relying on recognizing two or more predefined types of objects can be converted to a CaRP Scheme. This requirement is satisfied by all the schemes of text Captcha and most IRCs. By adding more types of objects the IRCs that depend on recognizing a single predefined type of objects can also be converted to CaRP in general. To ensure both security and usability the conversion of a specific Captcha scheme to a CaRP scheme typically needs a case by case study. If the types are not predefined those are the IRCs which rely on identifying the objects.

Assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS) as other graphical passwords. The possible way to apply CaRP schemes in user authentication is as follows. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. By receiving a login request, AS will give a CaRP image and it records the locations of the objects in the image, also it sends the image to the user to click his password. The coordinates of the clicked points are recorded and they will be sent to AS along with the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects. To recover a password successfully, each user-clicked point must belong to a single object or a clickable-point of an object. Objects in a CaRP image may overlap slightly with neighboring objects to resist segmentation. Users should not click inside an overlapping region to avoid ambiguity in identifying the clicked object [1].

III. METHODS

RECOGNITION-BASED CARP In this section, we are going to see different schemes of recognition-based CaRP. There are two basic recognition-based schemes as explained in following sections and also some variations of these schemes. [A] Click Text It is very basic and simple CaRP recognition-based scheme and it is built on top of text captcha.In this scheme, one of the character should excluded which creates confusion e.g. letter 'O' and alphabet '0'. In this password is a sequence of alphanumeric characters like text captcha e.g. ρ="IN9DI8A".A Click Text image is generated by captcha engine same like a text captcha but all alphanumeric characters should appear on image. During generation of image, the location of all characters gets tracked to produce ground truth. In Click Text image, characters can be arranged randomly. Shows a Click Text image of 33 characters.

Since there is less number of similar animals as compared to number of available characters, the password space is less in Click Animal scheme. Therefore guessing attacks can easily break the password. And to make CaRP more secure, we need large password space also to resist attackers from guessing attacks. In order to increase the password range, it is necessary to combine it with some gridbased graphical passwords and select grid-size as per selected animal. As per DAS [5], we know that it is candidate but requires drawing on grid. To be uniform with Click Animal, we are going to change drawing with clicking. We are going to call it as Click-A-Secrete (CAS). In Animal Grid, we are going combine Click Animal with CAS to make Click Animal more efficient. Also we are going to design CaRP in such a way that the number of gridcells will as much larger than alphabet size. At a time of designing this scheme, we are going to design it in such a way that, the user has to select correct animal in order to get correct animal grid. If user selects wrong animal

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905265 |

then animal grid produced from it will also be wrong. If user is clicking on wrong grid correctly then also password will be wrong and authentication gets failed.

IV. RESULTS

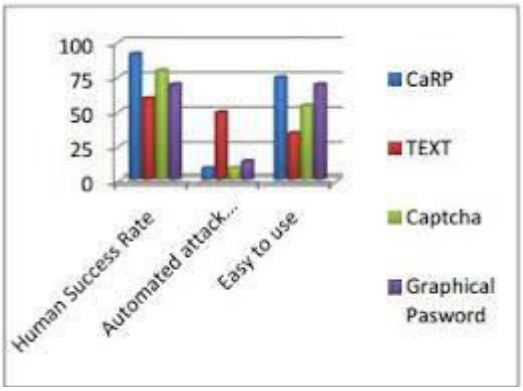


Fig3: Captcha

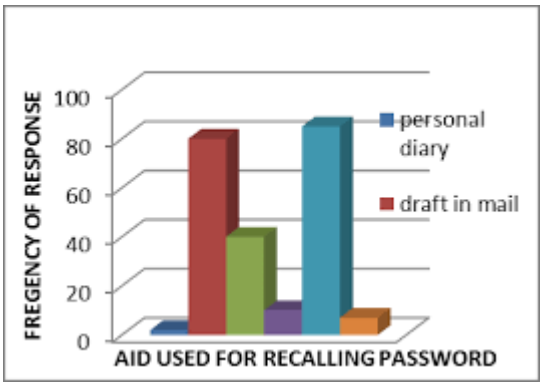


Fig4: Recall

The shares generated are combination of black & white pixels whose stacking results in original image which is also a black & white image. In the registration phase the most important part is the creation of shares from the image captcha where one share is kept with the user and other share can be kept with the server. For login, the user needs to enter a valid mail id in the given field. Then he has to browse his share and process. At the server side the user's share is combined with the share in the server and an image captcha is generated. The user has to enter the text from the image captcha in the required field in order to login into the website.

V. CONCLUSION

To overcome disadvantages of only text-based captcha, we introduced a new scheme known as CaRP which combines advantages of both captcha as well as graphical passwords. CaRP relies on unsolved hard AI problems. CaRP introduces CaRP image which is again a captcha challenge. It encounters various guessing attacks. This captcha challenge is used for every login attempt and also makes trials of guessing attacks computationally independent of each other. CaRP can also help to reduce the spam emails.

Database can stored the information of the User and the Image of CAPTCHA . The data can be encrypted using AES algorithm and stored in database. When the server wants the details of user or the database server send the details of user which is in the form of encrypted data. So that the data can't be access or hack by the hacker. Server can used to communicate between stored data and the web user. When the user wants to open his/her account on the internet, then the user first register his/her details and select the image for CAPTCHA. Stored images in database are in encrypted form. And when the user wants to login then she/he first enters his/her Email ID and Password. And then server shows the CAPTCHA structure with pair based scheme i.e in the form of n*n matrix.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905265 |

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, 2012.
[2] 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.
[3] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161– 170.
[4] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.
[5] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in Proc. ACM CCS, 2008, pp. 543–554.
[6] G. Mori and J. Malik, "Recognizing objects in adversarial clutter,"in Proc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognit., Jun. 2003, pp. 134–141.
[7] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in Proc. IEEE Comput. Soc.Conf. Comput. Vis. Pattern Recognit., Jul. 2004, pp. 23–28.
[8] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest-aligned manual image categorization," in Proc. ACM CCS, 2007, pp. 366–374.
[9] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K.Lee, "A new CAPTCHA interface design for mobile devices," in Proc. 12th Austral. User Inter.Conf., 2011, pp. 3–8.
[10] 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details