Design Pair Based Algorithm for Selection of CAPTCHA to Get Better Security against Hard AI

Mayuri S. Ganjudde[1], Fazeel I.Z.Qureshi [2]

[1] *Miss.* Mayuri S. Ganjudde*, W.C.E.M, Nagpur, Maharashtra, India*
[2] *Prof. Fazeel I. Z. Qureshi, W.C.E.M, Nagpur, Maharashtra, India,*

ABSTRACT

In this paper, we present a new security primitivebased on hard AI problems, a novel family of graphical password system on CAPTCHA technology. It calls CAPTCHA as graphical passwords (CaRP). CaRP is both a CAPTCHA and a graphical password method. CaRP shows a number of security problems including online guessing attacks. A CaRP password can occur automatically, in onlineguessing attacks even if password is in search set. CaRP provide security,usability and appears to fit well some practical applicationsfor improving online security. Now, we proposed a pair based authentication scheme. At the time of registration we used an email id and password. But when we login the page, at that time the third term occur i.e. CAPTCHA. Now the CAPTCHA is generated using a pair based authentication scheme. CAPTCHA character are changes their location on new session.

Keywords:-CAPTCHA, Pair Based Algorithm, AES Algorithm

---

1. INTRODUCTION

A task in security is to create cryptographic primitives based on hard AI problems. that are computationally intractable. The discrete logarithm problem is to the Diffie-Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography .Using hard (AI) Artificial Intelligence problems for security ,is an exciting new paradigm. By using this paradigm, the most notable primitive invented is Captcha. which distinguishes human users from computers by presenting a challenge, beyondthe capability of computers. But it is easy for humans. Captchais astandard Internet security method to provide online security for email and other services from being abused by bots. This paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard AI problems and their wide applications. It ispossible to create any new security primitive based on hard AI problems? This challenging and interesting open problem. In this paper, we present a new security primitivebased on hard AI problems, a novel family of graphical password system on CAPTCHA technology. It calls CAPTCHA as graphical passwords (CaRP). CaRPis both a CAPTCHA and a graphical password method. CaRP shows a number of security problems including online guessing attacks. A CaRP password can occur automatically, in onlineguessing attacks even if password is in search set.CaRP provide security, usability and appears to fit well some practical applicationsfor improving online security. The online dictionary attacks are prevented by CaRPwhich have been for long time a major securitythreat for various online services. This threat is considered as a top cyber security risk .Online dictionary attacks is a more subtle problem thanit might appear.

2. LITERATURE REVIEW

R. Biddle and et.al [1]
 This paper implemented A Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme, CaRP addresses a number of security problems altogether, as online guessing attacks, relay attacks and many more. This offers security and usability and it appears to fit well with some practical applications for improving online security.
H. Tao,C. Adams and et. al [2]
This paper Inspired by an old Chinese game Go. They have designed a new graphical password scheme. Pass-Go, in which a user selects intersections on a grid as a way to input a password. While offering an extremely large full

password space (256 bits) their scheme provides acceptable usability, as empirically demonstrated by, to the best of our knowledge, the largest user study on graphical pass- words.

B. Pinks, T. Sander and et. al. [3]

The paper suggestsa novel authentication scheme that preserves the advantages of conventional password authentication. While simultaneously raising the costs of online dictionary attacks by orders of magnitude. The scheme is easy to implement and overcomes some of the difficulties of suggested methods of improving the security of user authentication schemes.

L. von Ahn, M. Blum and et. al [4]

This paper they introduce a new concept that is CAPTCHA. CAPTCHA has many applications in security. They provide many novel constructions ofCAPTCHA. Their approach introduces a newclass of hard problems that can be exploited for security purpose.

J. Yan, A. S. El Ahmad and et. al. [5]

This paper, they implemented security of a textbased CAPTCHA designed by Microsoft. And deployed for years at many of their online services. This scheme was designed to be segmentation-resistant. It has been well studied and tuned by its designers over the years. However, our simple attack has achieved a segmentation success rate of higher than 90% against this scheme. A CAPTCHA that is Carefully designed to be segmentation-resistant is vulnerable to novel but simple attacks. Their results show

that it is not a trivial task to design a CAPTCHA scheme that is both usable and robust.

G. Mori, J. Malik and et. al. [6]

This paper they implemented object recognition in clutter. They test their object recognition techniques on Gimpy and EZ Gimpy (Example of visual CAPTCHAs). A CAPTCHA is a program that can generate and grades tests that humans can pass but current computer can't pass. This CAPTCHA provide Good test sets since the clutter they contain is adversarial. It is designed to confused computer programs.

G. Moy, N. Jones and et. al. [7]

In this paper implemented two distortion estimation techniques for object recognition that solve EZ-Gimpy and Gimpy-r (two of the visual CAPTCHAs) with high degrees of success. A CAPTCHA is a program that generates and grades tests that many humans can pass but current computer programs can't pass. They have developed a correlation algorithmthatcorrectly identifies the word in an EZ-Gimpy challenge image. And a direct distortion estimation algorithm that correctly identifies the four letters in a Gimpy-r challenge image.

J. Elson, J. R. Douceur and et. al. [8]

This paper implemented a CAPTCHA that asks users to identify cats out of sets of photographs of cats and dogs. Their image database is provided by novel. It is beneficial partnership with pet finder.com. This has a database of over 3 million of pets for home.Instead useof these 3 million of image, thy useAsirra displays an "Adopt me" link, promoting pet finders mission of finding homes for homeless animals.

R. Lin, S. Y. Huang and et. al. [9]

In this paper they implemented a two contributions. First one is the erosion-based CAPTCHA- breaking algorithm. It is easily attack the drawing CAPTCHA for mobile devices. Second one is the new CAPTCHA system used for mobile devices , it is called as CAPTCHA Zoo. It is based on parameterizes 2D projection of 3D models of natural animals on natural background. In second contribution they used a CAPTCHA breaking- breaking system.

Jermyn, A. Mayer and et . al. [10]

This paper implemented new graphical passwords that exploit features of graphical input displays for achieving more security than text-based passwords. In that, the graphical input devices enable user to decouple the position of inputs from the temporal number. In which those inputs occurs. And they displays this decoupling can be used to generate password spaces.In sequence to evaluate security of one of schemes.

3. PROPOSED TECHNIQUE
Existing System

Existing system consist of CaRP i.e. Captcha as Graphical Password. The CaRP is either Captcha or Graphical Password.

1. Graphical Password

   In this scheme, they used large number of graphical password scheme. It is classified into three main categories on the basis of their task involved in memory and entering password. They are recognition, recall, and cued recall.
2. Captcha

Captcha is based on the gap between humans and bots in solving some hard AI problmes. They are of two types of visual Captcha. They are text captcha and Image-recognition Captcha.

Captcha as Graphical Password (CaRP):

This type of CaRP is a Recognition-Based CaRP. In that the password is a series of visual based objects in alphabet. In this paper they Used the three main types of CaRP i.e. ClickText, ClickAnimals and AnimalGrid.

A. ClickText

In this Capcha their will only used the characters. ClickText is the recognition-based CaRP scheme, it builts on top of text Captcha. A ClickText image was generated from by underlying Captcha engine. If a Captcha image generated except that all alphabet character should appear in image.

Fig A: ClickText Image

B. ClickAnimal

In this Captcha scheme uses a 3D models of horse and dog for generation with number of texture, colors, lightning, poses, and arranges on to the clutterd background.

Fig B: Captcha with circled red horses

C. AnimalGrid

In this Captcha scheme has smaller alphabets, Smaller password space, than ClickText. It is based on grid-based graphical password.

Fig C: ClickAnimal image

Proposed Technique

In proposed technique, we used a Pair-Based Authentication Scheme onto the Captcha. The fig shows the intersection of letter for password.

Fig: Intersection letter for Password

In Pair-Based Authentication scheme , we used only for creating a matrix to arrange the characters, numbers and images. We proposed the new system for surety purposed used the Pair-based authentication scheme as well as Captcha . The CAPTCHA can be generated in the form of n*n matrix. In the matrix their well be the number of rows and number of columns.
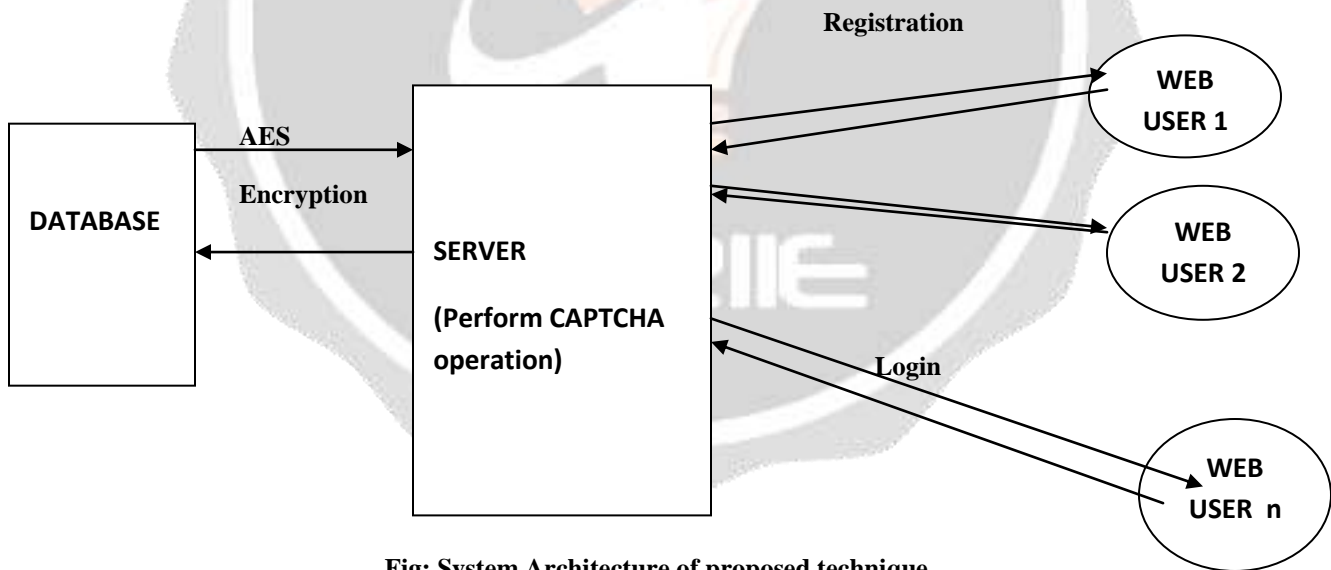

Fig: System Architecture of proposed technique

The above Figure shows the system architecture of proposed system. In this system architecture there are three main component i.e. Database, Server and Web User. And also three phase i.e. Constructing Database, Registration and Login .

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.

3.1 Home Page:

This is the first module. This is the home page. We create a one bank home page, for example IDBBI Bank. In home page there is a two field i.e. "New Registration" and "Login". Whenever the new user wants to create new account in IDBBI Bank, at that he first creates the new Registration. And after that he used the login option. The above figure shows the Home Page.

Figure 3.1: Home Page

3.2 Registration Page:

In this module user create a new registration. User fills the entire mandatory field like, Name, Age, Email-ID, Password, Address, City, Mobile number, State. And after that user select the CAPTCHA. In this module the CAPTCHA is created with the help of pair based technique. In this CAPTCHA there are 6*6 metrics. The above figure shows the Registration Page.

Figure 3.2(a): Registration Page

Figure 3.2(b): Registration Page

The registration page shows the CAPTCHA image. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Fig 3.2(b) shows that 8 is the intersection symbol for the pair "WD". The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system. The grid size can be increased to include special characters in the password.

3.3 Login Page:

- **First Step: Basic CAPTCHA:** This is the first login level. In this CAPTCHA we used simple combination of character and number CAPTCHA. If the user enter the right password then going to user account, otherwise going to second login level. The above figure shows the first login or Basic CAPTCHA .

Figure 3.3(a): Basic CAPTCHA

- **Second Step: Character CAPTCHA:** This is the second login level. In this login level we used pair based technique for selection of CAPTCHA. In this CAPTCHA we used combination of character, number, and special symbol. Every time whenever the session will be restart then different CAPTCHA will be generated with the help of pseudorandom code generator. CAPTCHA changes its

location, text size, color, font, different character. If The user enter the right password then going to user account, otherwise going to third login level. The above figure shows the second step of login page.

Figure 3.3(b): Character CAPTCHA

The Second Login level CAPTCHA is same as the registration level CAPTCHA.

- **Third Step: Image CAPTCHA:**
    This is the third login level. In this CAPTCHA we used again pair based technique. In this CAPTCHA we used combination of images like animal, flower, nature, grass. In this CAPTCHA we only used animal and grass images. If The user enter the right password then going to user account, otherwise going to third login level. The above figure shows the third level of login.

    The above figure shows to select the "Dog". The user saw the dog images and then select all dog images one by one. In this CAPTCHA also we used the pair base technique. So that for one image of dog we select the its first row image and then column image. For Example, User selects the first row image as grass image and column image as horse image.

Figure 3.3(c): Image CAPTCHA

- **Final Step: Animal CAPTCHA:**
    This is the final or forth login level. In this level we used two layer of pair based technique for selection of CAPTCHA. In this CAPTCHA we only used animal and grass images. In first pair

based layer we used combination of animal and grass images. And after that we used thin layer of pair based technique. In this layer we label the 32 image using number and remaining four images unlabeled. If the user enter the right password then going to user account, otherwise going to third login level. The above figure shows the final step of login page.

Figure 3.3(d): Animal CAPTCHA

4. CONCLUSIONS

At the time of login we can see CAPTCHA having number, characters or images and we enter it by pressing button on keyboard. which is hack by hard Artificial Intelligence due to that security is not maintain to the user means password is not secured. So for that we implement new scheme in this paper that is 6*6 metrics by selecting row and column which having common element and that common element is nothing but our CAPTCHA. This technique can't hack by hacker so that our password will be secure using pair based CAPTCHA technique.

5. 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.