INTERNATIONAL ONLINE CONFERENCE ON ADVANCE RESEARCH & DEVELOPMENT IN ENGINEERING AND TECHNOLOGY

IO-CARDET 2016

E-ISSN NO:-2349-0721

Impact factor : 2.25

DESIGN PAIR BASED ALGORITHM FOR SELECTION OF CAPTCHA TO GET BETTER SECURITY AGAINST HARD AI

Mayuri Ganjudde[1],
[1]W.C.E.M, Nagpur
[1] ganjuddemayuri@gmail.com

Prof. Fazeel.I.Z.Qureshi[2]
[2] W.C.E.M, Nagpur
[2] fazeel.zama20@gmail.com

ABSTRACT:

In this paper, we present a new security primitive based 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. ACaRP password can occur automatically, in online guessing attacks even if password is in search set. CaRP provide security, usability and appears to fit well some practical applications for 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.

I. 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). 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 online guessing attacks even if password is in search set.

CaRP provide security, usability and appears to fit well some practical applications for improving online security. The online dictionary attacks are prevented by CaRP which have been for long time a major security threat for various online services. This threat is considered as a top cyber security risk .Online dictionary attacks is a more subtle problem than it might appear.

II. 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] Thepaper 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 text-based 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 algorithm at correctly 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 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.

III. EXISTING SYSTEM

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

I. 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.

II. 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.

III. 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.

IV. 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

V. 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

VI. AnimalGrid

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

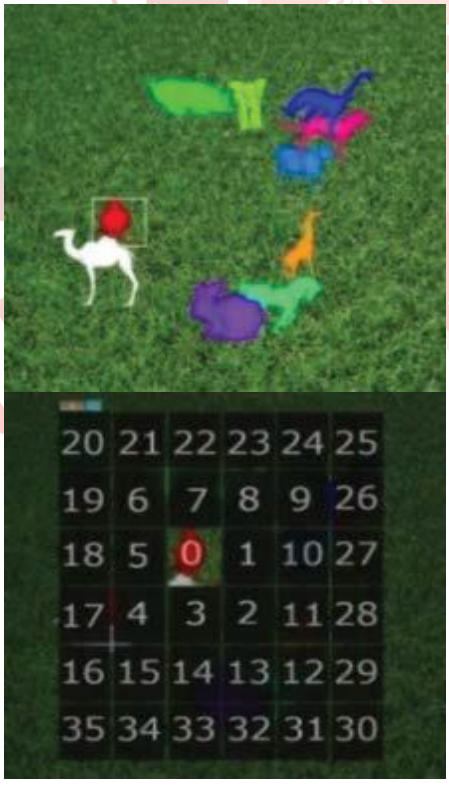

Fig C: ClickAnimal image

IV. PROPOSED TECHNIQUE

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

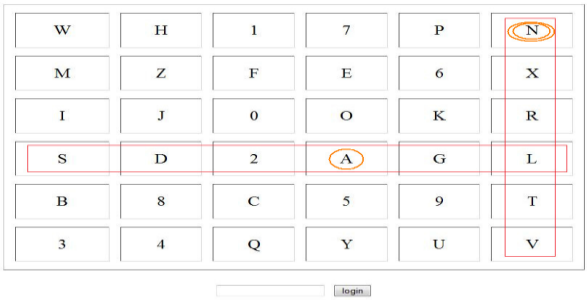

Fig: Intersection letter for Password

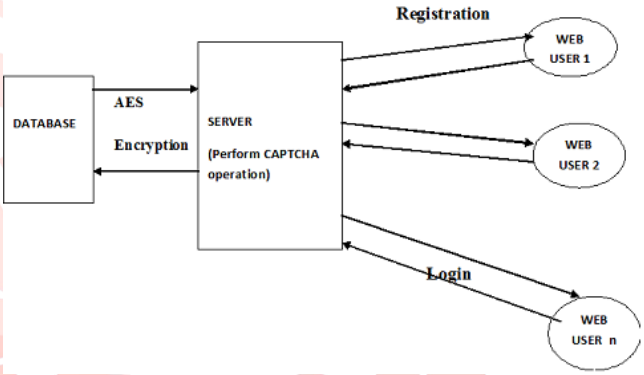

Fig: System Architecture of proposed technique

The above Figure shows the system architecture of proposed system. In this system architecture there are three main components i.e. Database, Server and Web User. Andalso three phase i.e. Constructing Database, Registration and Login Database can store the information of the User and the Image of CAPTCHAThe 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. Now, we create the first module i.e. Registration Phase. In this module we see the IDBBI Bank Registration page. In the registration time first we enter the email id and password. And then we enter the personal information like Name, Address, City, District, Pincod , State, Mobile number, And then lastly generate the CAPTCHA i.e. 6*6 matrics. In this CAPTCHA we see the combination of characters and numbers. The CAPTCHA can be change every time. The CAPTCHA can change the, Font Style, Color, Position, Character and Font Size. For example, as we see in the above figure... The CAPTCHA is "7JSV". Now if I want to select this CAPTCHA in the 6*6 matrics. First select the row element and then select the column element. For "7" we select the row element "Z" and column element "S", like wise remaining will be selected. The registration page can be see in the above figure

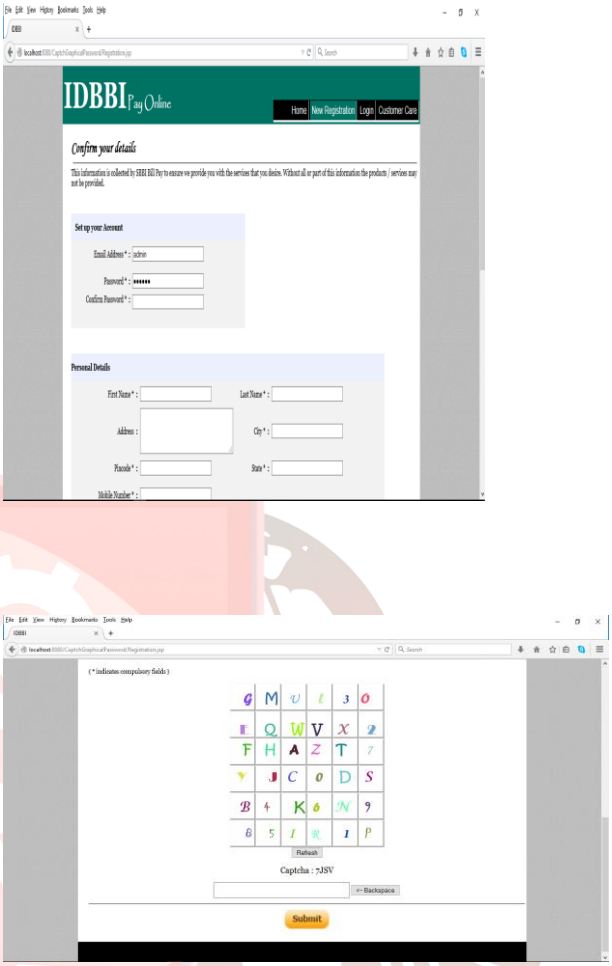

Fig. IDBBI Registration page

V. CONCLUSION

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 n by n matrics 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.

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] [27] 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.