International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 3 – MARCH 2016.

AUTHENTICATION PROTOCOL FOR SECURITY BASED ON CAPTCHA AS COUNTERSIGN ON HARD AI PROBLEMS

Saranya. S[1] , Infantina A[1], Jabez J[2]

[1]*UG student, Department of Information Technology, Sathyabama University, Chennai, India.*
*[2]*Assistant Professor, Department of Information Technology, Sathyabama University, Chennai, India.*

***Abstract*--Phishing is an challenge by an entity or a set to steal personal secret information such as keys, credit card information etc from unwary victims for integrity stealing, financial grow and other fake behaviors. Visual cryptography is a individual type of covert sharing. In this paper we have suggested a new way for forged websites categorization to solve the problem of phony. Fake websites contain a mixture of cues within its content-parts as well as the browser-based protection pointers presented along with the website. Which we call Captcha as graphical passwords (CaRP).CaRP is both a Captcha and a graphical password scheme. The apply of images is discovered to conserve the privacy of image captcha by decaying the unique image captcha into two shares that are stored in part database servers such that the original image captcha can be exposed only when mutually are simultaneously obtainable; the entity sheet images do not admit the individuality of the original image captcha. Once the creative image captcha is disclosed to the user it can be exploited as the secret word. Some results have been offered to attempts. However, there is no distinct wonderful shot that can answer this danger drastically. because anti-phishing results plan to expect the website class rigorously and that exactly equals the data mining classification technique targets. In this learn, the creators discard light on the vital roles that differentiate fake sites from rightful ones and judge how high-quality rule-based data extraction method are in expecting duplicate websites and which classification technique is verified to be more consistent.**

I. INTRODUCTION

In these days Internet operations become very ordinary and there are different intrusions nearby behind this. In these kinds of diverse attacks, phishing find as a major protection risk and new modern ideas are happening with this in every moment so defensive mechanisms should also be so efficient.

In our work, the security also be increased and should not be easily identificable with performance easiness. Today, the majority claims are only as safe as their underlying scheme.

Since the plan and tools of middleware has recovered progressively, their recognition is a not easy problem.

Finally, it is nearly impractical to be confident whether a computer that is attached to the internet can be believed reliable and safe or not. False scams are also becoming a trouble for internet banking and e-commerce users.

One designation of phishing mean as "it is a illegal action using communal engineering techniques. Intruders attempt to deceptively acquire responsive information, like secret code and credit card number, by masquerading as a responsible person or industry in an electronic communication". The behavior of self stealing with this obtained information has also become simple with the need of machinery and identity thievery can be explain as "a offense in which the fraud obtains key parts of data such as common Security and license plate numbers and uses them for his or her own gain". Phishing assaults rely upon a mix of technical cheating and social engineering practices. Social media asgmail, social websites, IRC and immediate messaging services are popular. In all cases the phisher must impersonate a trusted source for the victim to believe. To time, the most victorious hits have been started by email – wherever the attacker impersonates the sending rights.

So here establishes a new way which can be utilized as a secure path beside phishing . As the name describes, in this paper website cross checks its own identity and shows that it is a legitimate website (to apply bank transaction, E-commerce and online booking system etc.) previous to the end users and make the mutually the surfaces of the system sheltered as well as an validated one. The theory of image processing and an progressed visual cryptography is utilized. Image processing is a system of development an input image and to obtain the output as either get better form of the similar image and/or features of the input image. Visual Cryptography (VC) is a plan of encoding a secret image to shares, such that loading a ample number of shares discloses the secret image.

II. PROBLEM FORMULATION

Phishing web pages are forged web pages that are generated by attacker to copy web pages of actual websites. Some classes of web pages have increasing visual matches to trick their fatalities. Some kind of web pages see accurately like the actual ones. It contains methods like traping users through some social media and spam messages, man in the middle attacks, setting up of input loggers and display catches. To offered physically powerful verification in a web application. To track safe progression while handling user instruction.

III. PROPOSED WORK

In this system launches a new method for finding if it is a creative site or copy. Our proposed work an image is showed by the user records and inserted into pixel by pixel. It indicates the shares of a white pixel and a black pixel. Take that the selection of shares for a white and black pixel is chance to determined. No share presents any hint about the unique pixel

because dissimilar pixels in the covert picture will be encoded using free arbitrary selections. It checks password and other private data from the phishing websites.To grant a strong validation in a web application.

IV. RANDOM PATTERN ALGORITHM

Random pattern algorithms to encoding a binary secret image. The input is a l1 × l2 image, indicated by I, and the outputs are two images P1 and P2. The algorithms is shown as below.

Algorithm 1:

create a l1 × l2 random grid P1// ℑ(P1) = ½
for(a = 0 ; a < l1 ; a ++)
for(b= 0 ; b < l2; b++)
if(I[a][b] == 0)
P2 [a][b] = P1 [a][b] ;
Else
P2 [a][b] = P1 [a][b] ;
output (P1 , P2)

The above algorithm, this process suggests a new procedure one gray-level secret image, indicated by J, and makes two gray-level enciphered images, mean by GR1 and GR2, that every dots are ordered into additional than two colors. User overlays those two enciphered images GR1
and GR2, the concealed coverts of the gray-level image J can be shown. Due to the limit of RGB value in gray-level, two schemes below are terminated to encipher all dots on the gray-level top secret image.

LINEARPROGRAMMING ALGORITHM:

Typical form is the common and the majority of instinctive form of defined a linear programming problem.
It has 2 following parts as ,

A linear method to be increased
f(x1,x2)=c1x1+c2x2

Problem constraints
e.g.
a11x1+a12x2≤b1
a21x1+a22x2≤b2
a31x1+a32x2≤b3

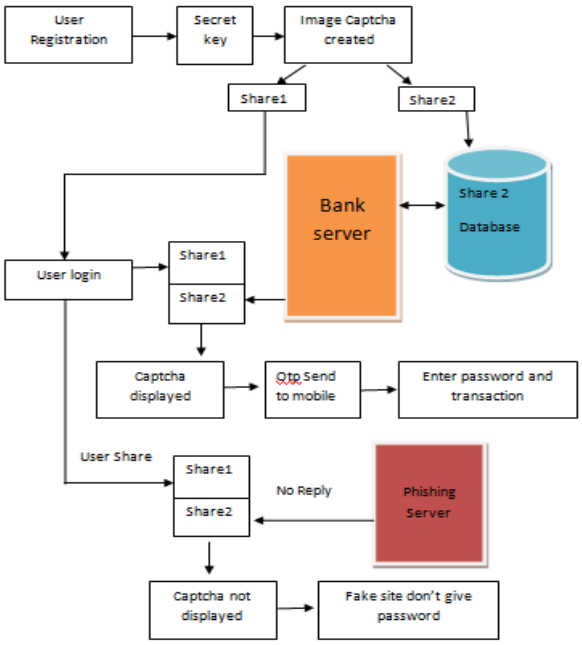


Fig 1. Architecture diagram

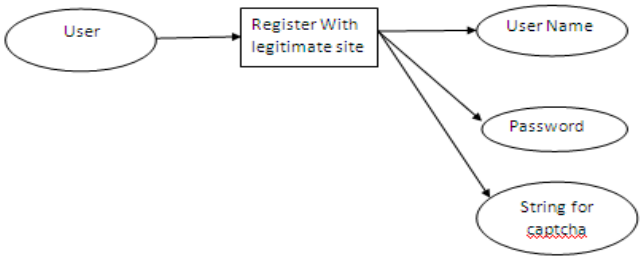


Fig 2 : level 0 –Registration process

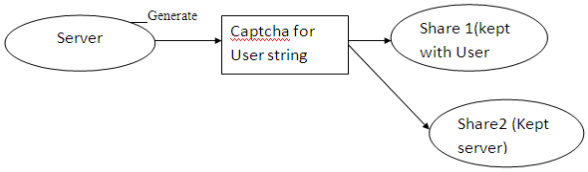


Fig 3: level 1 – Generating shares

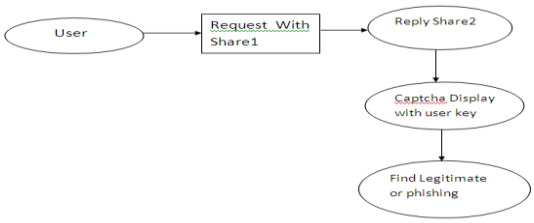


Fig 4: level 2 – Display captcha

V. IMPLEMENTATION

- Registration With Secrete Code

- Image captcha Generation
- Shares Creation(VCS)
- Login Phase

A. **Registration With Secrete Code:**

In the phase, the user details as user name, password, email-id, address, and a key string(password) is entered from the system at the point of registration for the safe website. The input string can be a mixture of alphabets and numbers to offer for more protected environment. This string joined with arbitrary produced string in the server.

B. **Image captcha Generation:**

A input string is translated into image using java classes BufferedImage and Graphics2D. The image measurement is 160*30. Passage color is black and the backround color is white. Passage font is set by Font class in java. After image appear it will be write down into the userkey folder in the server using ImageIO class.

C. **Shares Creation(VCS):**

The image captcha is splits into two shares after that one of the share is kept on the users hand and the other share is kept on the server. The user's share and the actual image captcha is sent to the user for afterward authentication during login phase. The image captcha is also saved in the actual database of any private website as covert data.

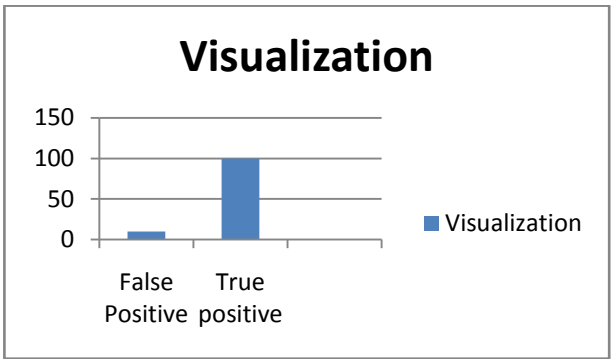
D. **Login Phase:**

User entering his/her secret information as userid and his/her share which is kept with him to login. This share is pass through the server where the user's share and share which is stored in the server of the sites for all user, is heaped mutually to create the image captcha. The image captcha is presented to the user. Here the final user can test whether the showed image captcha equals with the captcha generated for registration. The final user is wants to enter the text presented in the image captcha and this can provide the reason of key and utilize this, the user can login into the site. Here the username and image captcha created by loading two shares one can prove whether the website is true/secure website or a fake website.

VI. EXPERIMENTS AND RESULTS

The tests are complete using a variety of captcha images. The suggested method usedto identify fake intrusion is achieved on each time the experiment is take out.

It is clear that the claim reveals 100% true positives. Consequently it can be ended that false attack is not achievable in the function. The Normal effects of 50 testings are there. The parallel axis signifies the group of results while the perpendicular axis signifies the % of achievement of the trials. The general outcomes expose that the intended system for perceiving and stopping phishing intrusions is very efficient and can be employed in the factual worldrelevances.



VII. CONCLUSION

Presently intruders attacks are so general since it can physical assault overall and capture and store private information for users. This data is utilized by the invaders which are not directly occupies in the false process. Fake websites as well as users can be simply recognized our framework. The proposed tactics conserves top secret instruction of users. Check whether the site is a good/safe website or a forgery website. If the website is not a real website (website that is a forgery one just parallel to safe website but not the safe website), then in that situation, the fake website can't show the image captcha for that particular user. According to the reality that the image captcha is created by the heaping of two shares, one share is on the user's hand and the other share on server of the website.

REFERENCES

[1] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, pp. 2021–2040, Dec 2003.
[2] "Playstation Network Hack," http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony, 2011.
[3] "RockYou hack compromises 32 million passwords," http://www.scmagazine.com/rockyou-hack-compromises-32-millionpasswords/article/159676/, 2009.
[4] "#OpWorldCup: Anonymous Hacks Brazilian Government, Police, Court, Globo TV and Cemig Telecom," http://hackread.com/anonymoushackers-brazil-worldcup-hacks/, 2014.
[5] "Software Company Tom Sawyer Hacked, 61,000 Vendors Accounts Leaked," http://www.databreaches.net/software-company-tomsawyer- hacked-61000-vendors-accounts-leaked/, 2013.
[6] "Hacker Defaces Microsoft U.K. Web Page," http://rcpmag.com/articles/2007/06/29/hacker-defaces-microsoft-uk-web-page.aspx, 2007.
[7] "Hackers Leak Data Allegedly Stolen from Chinese Chamber of Commerce Website," http://news.softpedia.com/news/Hackers-Leak-Data-Allegedly-Stolen-from-Chinese-Chamber-of-Commerce-Website- 396936.shtml, 2013.
[8] "LinkedIn Hack," http://en.wikipedia.org/wiki/2012_LinkedIn_hack.
[9] "SQL Injection," https://www.owasp.org/index.php/SQL_Injection.
[10] "sqlmap - Automatic SQL injection tool," http://sqlmap.org/.