I J C T A, 9(16), 2016, pp. 7697-7702
© International Science Press

Anti-Phishing Strategy Model for Detection of Phishing Website in E-Banking

Mohsin Fida* and A. Arokiaraj Jovith**

ABSTRACT

Phishing is deceptive attemptthat targets an individual or an organization, seeking unauthorized access to confidential data or personal credentials such as credit card information, passwords etc. by an individual that poses as a reputable entity or person. It has become a stern threat to companies that deal with E-transactions. If these threats cannot beceased, people cannot trust online transactions that include authenticationover credentials. In theproject, we have used an image-based authentication using Visual Cryptography (VC).The integrity of the secret image is maintained by dividing the secret image into two splits using VC,one is stored in server side database and other is given to the user such that the Secret Image can be recognized only when both the splits are concurrently available.The technique of both image processing and a cryptography is used in my project. Image processing is a technique to transform the secret image into digital form and carry out some operation on it, ina visual cryptography the Secret Image is splitting into splits and is kept in the server database, after login by the user, the Secret Image should get amatch with its content behind theimage. After both user and server side shares get matched, the user can login into the website very securely.

Index Terms: Phishing, Visual Cryptography, Secret Image, Shares, and Security.

1. INTRODUCTION

Online transactionsare becoming very common nowadays so are attacks against it.Among all the attacks, phishing is amajor security threat and anew approach is needed to safeguard our security system against these attacks. Thus, the security in these cases be very hard and should not be easily breached with implementation easiness. It is very difficult to tell whether a device connected tothe internet is secure and reliable or not.Phishing has become the major issue in E-banking.Phishing is an attempt of thieving personal confidential information such as credit card information, passwords etc. by an individual or a group to from unsuspecting victims for identity theft, financial gain, and other fraudulent activities.Phishing scams have been gettingcolossalpress coverage because such attacks have been rising in number and complexity. One definition of phishing is assumed as “it is anillegitimate activity that uses social engineering techniques.

Phishers attempt to deceitfullyobtain sensitive credentials, such as credit card details andpasswords, by posing as a reliable person or commercial in an E-communication”. The act of identity thieverywith this assimilatedsensitive information has also become simplerwith the usage of propertechnical skills and identity theft can be described as “anoffensein which the masqueradeobtains key pieces of information such as Social Security and driver’s license numbers and uses them to his or her personaladvantage”.Thus,thePhishing can be accomplished by social engineering or using some attacking tools. In the many cases, the phisher encourages the legitimate user to deliver him, his credentials or make the victim perform certain activities

* Student M.Tech–Information Security and Cyber Forensics, Department of Information Technology SRM University Chennai, India, *Email: mohsenfida@gmail.com*

** Assistant Professor (Sr.G) Department of Information Technology SRM University, Chennai, India, *Email: arokiarajjovith.a@ktr.srmuniv.ac.in*

which he is not supposed to do.The most effective and common phishing attackscan be donevia Email, where the phisher poses the sending authority.In my project, the websiteauthenticated andit proves that it is a legitimate website before the usersenter it credentials. we have used the concept of image processing and an enhanced visual cryptography. Image processing is a method to convert the secret image into digital form and perform some operation on it, in a visual cryptography the Secret Image is splitting into splits and is kept in the server database, after login by the user, the Secret Image should get a match with its content behind the image. After both user and server side shares get matched, the user can login into the website very securely.

II. RELATED WORKS

The phisher can make the crafted web pages and sent you malicious mail, whichclaims to come from legitimate sources or websites. Phishing web pages appear similar to the original one and are hard to identify unless we don't look at URL.Phisher embeds the link to a link in an email that redirects a user to an insecure website that requests sensitive information. An attacker can also install a Trojan through a crafted email attachment which will allow the attacker to trick a user and obtain sensitive information from him. The attacker can send you and email stating that your banking details need to be updated and trick a user into making him click on the embedded link. This link will take the user to the malicious website controlled by the attacker. The website will be areplica of the original website and a user may end up by entering all his sensitive details like account no, customer ID, secret word or password or other sensitive data.

Once the attacker retrieves all your details it can easily access your account.It includes methods such as defraud the customers through email and unsolicited mail, fitting of key loggers. E-mails are used for phishing, due to its easiness. However, there are techniques to detect phishing websites. Web of Trust is a browser extension, theuser can add it .it automatically tells a user if the website is legitimate or not.But it's not possible to validate each and every live website over theinternet. Most web browsers come up with theanti-phishing mechanism, but we are supposed to enable this service by default it is notconfigured. Web browsers like Google chrome and Firefox also provide phishing related detection mechanism, but we have todo some configuration to make it work. The URL's of phishing website can't have thesame URL as the legitimate website they are claiming to be.at the bottom of the Browsers the URL will be displayed .we can verify if it is the good or URL.The blacklist technique is also available in browsers, but the problem is it will detect only those phishing website which is available in blacklist database. The developer makes the database and adds the URLs.The user can update the blacklist database from the browser's website but it's very difficult to detect the new phishing pages if they are not in the database.

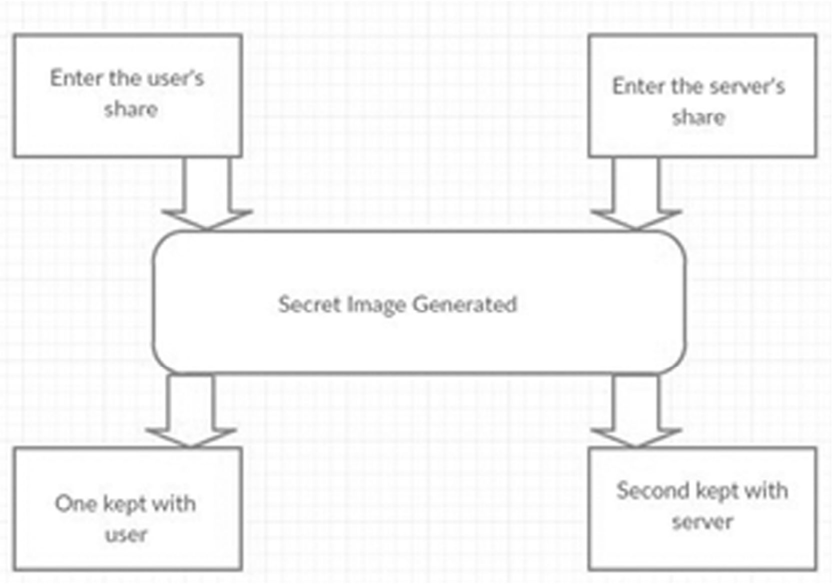
Domain Name System (DNS) blacklists preventspamming and is used by spam filters and spam firewalls. A DNS blacklist is consists of a database that has IP addresses of known spam sources. A spam filter uses this tool to checkwhether an e-mail is on a blacklist or not, if it is present in the list, it would block if the source is listed.

3. PROPOSED SYSTEM

The proposed system is consists of two phases: registration phase and login phase:

3.1. Registration

In this phase, the user will be registered with the bank. The user will enter his details like username, email, phone no, password.Along with all these details, the user has to enter the passphrase key. This secret key will be sent to the bank's server. The bank side server will generate the random key and will combine it with the user's secret key. Both the keys oncombination will form the secret image and this secret image will appear on user's screen. Then the secret image is encrypted using VC and using random pattern algorithm the secret image is divided into two splits one will be given to theuser and other will be kept at theserverside.



A . Registration Phase

Figure 1: Registration

The user has to download his split from the page and can use the split at the time of login [6].The user can later change the password or can generate anew secret image by entering the new passphrase key if required.

3.2. Login

In this phase, the user will enter his user id which will be sent to the server side. The server will receive his id and will send the split associated with that user id, then the user will have to produce its split. Both the splits are compared at server side and are superimposed together to form asecret image. This secret image will be sent to the user and the user then verifies the secret image. Once the secret image is verified by the user then theuser can type his password and get alogin to the legitimate website and can do online transaction securely [6].

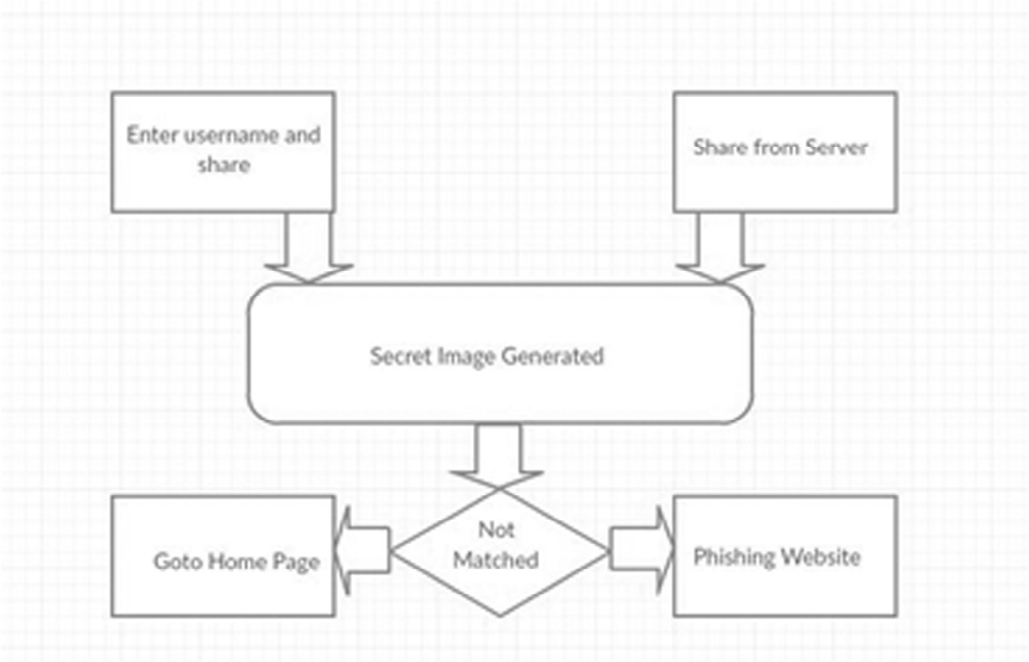


Figure 2: login phase

4. VISUAL CRYPTOGRAPHY TECHNIQUE

Visual cryptography is a scheme to hide the secret image using any number of shadow images called shares/splits. Here the secret image is the binary image means it either contains a black or white value. When the secret image is broken into two shares/split they alone don’t look like anything,but when they are overlaid thesecret image is revealed.

4.1. Random Pattern algorithm

Random pattern algorithm is an algorithm which used to encrypt a binary secret image into shares say X_1 and X_2. The input of this algorithm is expressed by A.

Where,

$$A = a\ w \times h \text{ image}$$

Algorithm:

```
**Algorithm 1** Generate a wxh random grid
**procedure** FIRST PASS
**for** ( i = 0 ; i < w ; i ++ )
**for** ( j = 0 ; j < h ; j ++ )
**if** ( A[i][j] == 0)
$X_2$ [i][j] = $X_1$ [i][j];
Else

$X_2$ [i][j] = $X_1$ [i][j];
Output ( $X_1$, $X_2$ )
```

We are purposing a new algorithm which is based on the above algorithm. Here if a secret image which is expressed by “K” (and is single greyleveled in nature) is processed and will result in a two greylevel encrypted image.We can express these two greylevel encrypted images as N_1 and N_2, where all the pixel in this image will be classified into two colors.When these two greylevel encrypted images N_1 and N_2 are superimposed,the single greylevelsecret image K will reveal .the two approaches that can encrypt each and every pixel on thesinglegreylevel secret image are:

1. *(2, k) visual cryptography scheme*-In this the single greylevel secret image will be encrypted and will result in n no of shares.When two shares are superimposed (any two shares) .the single greylevel secret image will be revealed.
2. *(2, 2) visual cryptography scheme*-In this the single greylevel secret image will be encrypted and will result in 2 shares .when these two shares are superimposed (any two shares). The single greylevel secret image will be revealed.

5. MECHANISM TO DETECT PHISHING

5.1. Website

In this methodology, the secret image will be split into two splits/shares, one with theuser and other with the bank side the server at the time of login, when user will type the user id.it will be verified by the bank side server and will provide the split/share associated with that user id.Once the secret image is generated by superimposition of two splits on user’s screen. Then the user will have to validate it and the user’s secret key(first half of secret image) will be hidden, only the server’s randomly generated key (the second half of secret image) will be visible, the user will have to enter the either the first two or last two digits of his

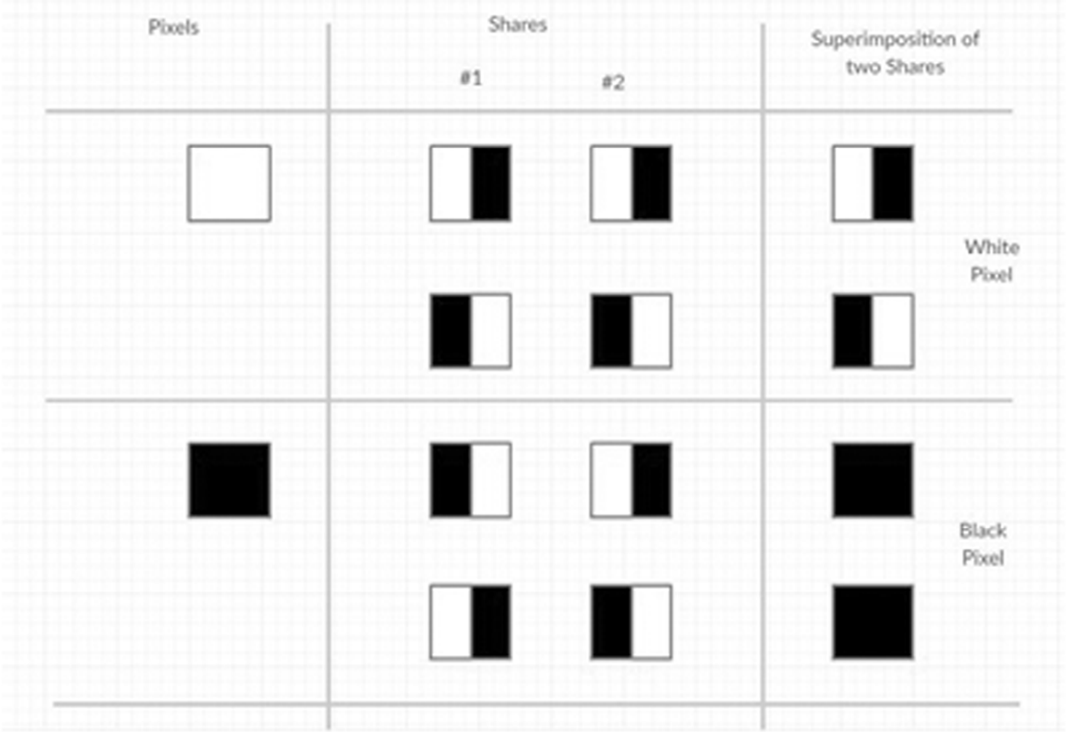


Figure 3: VCS scheme with 2 subpixel construction.

secret key to verify the secret images. Once the first two or last two digits are entered then the user can proceed with his password. The user can validate the website based on the secret image. The secret image must match with the image that was generated at the time of registration. If the images are same the website is legitimate if the secret images aren't same then it is a phishing website. If the website is a phishing website, the phisher will not be having the split/share associated with that user.

5.2. Architecture

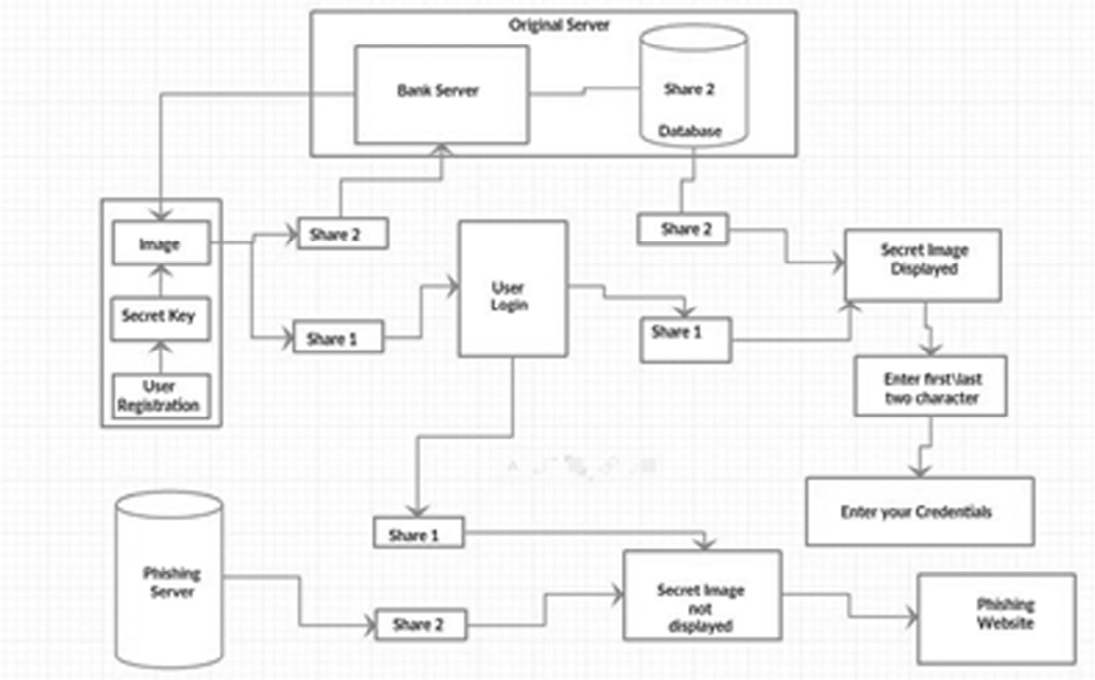


Figure 4: User log into website

6. FUTUREWORK

1. This technology cannot only use in thebanking sector but also used in defense sector to detect whether the website is legitimate or is phishing websites.
2. We can split the user's confidential information and store in different servers so that it provides more security.
3. If theuser forgets his/her password, so to create new password we use anew method such as aone-timepassword or they can also answer the one-time security question.
4. We use anew technique such as admin authentication.

7. CONCLUSION

Our methodology "Anti-phishing Strategy Model for detection of phishing websites is based on visual cryptography". The three levels of security are used to secure the user's information. Layer oneis used to authenticating the websites.it will inform the user whether thewebsite is secure one or is aphishingwebsite. In thesecond layer validation of the Secret,Image will be checked. Only human user acquire the website can read image Secret Image. In thethird layer of security, the phisher will be prevented from attacking the user and will not be able to get access to theunauthorizeddata user in theuseraccount. Therefore, it enhances the security mechanism

REFERENCES

[1] G. L. Haijun Zhang and T. W. S. Chow, "Textual and visual contentbased anti-phishing: A bayesian approach," *IEEE Trans.Neural Netw., vol. 22, no.* 10, pp., Oct. 2015.

[2] D. James and M. Phillip, "A novel anti-phishing framework based onvisual cryptography," *airccse.org//journel vol.3, no...1. pp.1264-3459,*2014.

[3] P. Cheng and C. Chen., "New antiphishing method with two types of passwords in openid system,*" in Proceedings of IEEEFifth International Conference on Genetic and Evolutionary Computing*, 2014.

[4] V. A. G. Thiyagarajan, P.; Venkatesan, "Anti-phishing technique usingautomated challenge response method,," *in Proceedings of IEEE- International Conference on Communications and Computational Intelligence*, 2014.

[5] C. Jackson and A. Barth, "Beware of finer-grained origins," 1*2th Information Security International Conference, Pisa, Italy.*, 2013.

[6] R. Youmaran and . A. Miri, "An improved visual cryptographyscheme for secret hiding," *in 23rd IEEE Biennial Symposium on Communications*, 2014.

[7] J. C. Haidong Xia, "Hardening web browsers against man-in-themiddleand eavesdropping attacks,*" WWW '05 Proceedings of the 14thinternational conference on World Wide WebPages 489-498 in ACM NewYork, NY, USA*, 2015.

[8] M. A. H. K. Dahal.;, "Modelling intelligent phishing detectionsystem for e-banking using fuzzy data mining,*" in Proceedings of IEEEConference on CyberWorlds*, 2015.

[9] J. Sunshine, S. Edelman and L. F. Cranor, "Crying wolf:An empirical study of ssl warning effectiveness," *in Proceedings of the18th USENIX Security Symposium*, 2013.

[10] M. Nourian. A.; Ishtiaq S., "Castle: A social framework for collaborativeantiphishing databases," *in Proceedings of IEEE- 5th InternationalConference on Collaborative Computing: Networking Applications, andWorksharing*, 2014.

[11] S. G. K. Nirmal, K.; Ewards, "Maximizing online security by providinga 3-factor authentication system to counter-attack' phishing," *IEEE International Conference on Emerging Trends in Robotics and Communication Technologies*, 2014.

[12] D. G. A. Dan Wendlandt and A. Perrig, "improving ssh-style hostauthentication with multi-path probing," *ATC'14 USENIX 2014 AnnualTechnical Conference Pages 321-334 USENIX Association Berkeley, CA,USA*, 2014.