ISSN 2395-1621

Secure Banking System using Anti Phishing Framework

[#1]Priyanka Sonkawade, [#2]Aditya Maharaj, [#3]Shubham Joshi, [#4]Smruti Vyavahare, [#5]Sarita Sapkal

[#123]Students, Department of computer engineering, MMCOE, Pune, India

[#4]Asst.Professor, Department of computer engineering, MMCOE, Pune, India

ABSTRACT

Nowadays the security of information is very important form the unauthenticated users. Unauthenticated users try to acquire the user's personal information. Phishing is one of the technique to capture the personal information like credit card details, passwords and other personal information. In our paper we have proposed a new approach named as "Secure Banking System using Anti phishing Framework" to solve the problem of phishing attack which is increase day by day. The term visual cryptography is used to store the privacy of image captcha by separating the original image captcha into two shares that stored in separate database servers such that the original image captcha can be formed only when both are simultaneously available the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is formed to the user it can be used as the password.

ARTICLE INFO

Article History

Received :16th April 2016

Received in revised form :

19th April 2016

Accepted : 21st April 2016

Published online :

25th April 2016

Keywords:- Phishing, Visual Cryptography, Cryptography, Steganography, Security, AES..

I. INTRODUCTION

In today's modern era, internet become very popular for various activities like communication, sending personal information through internet, bank transaction like online booking system, online shopping, online banking etc. is very common. So many attacks can hazards the information used while performing such type of activities. Phishing is one of illegal activity which performs using different social engineering techniques. Attackers try to acquire important and confidential information such as password, credit card details or other personal information. Phishing has become one of the very big issues in today's internet era. This attack will not hack any server or the website; it just creates duplicate copy of the website and tries to communicate with the user. The definition of phishing is "Act of stealing a person's information electronically."

Some of the Examples of Phishing Scams are:

- Many times the sites that closely similar look and feel of original sites.As these sites looks original sites, user logs in into those sites through which his/her sensitive information like bank details, name or other personal and confidential information. This information is stored at the phishers database.

- Sending the fake e- mail message to the bank user's is now very common, as if the database system of bank is trashed due to some technical reasons, so they request bank user for updation of the personal information.

- Sending e-mail message to the user's like you won the money prize and to deposit money they requested to send the personal information and bank account details.

- So to avoid phishing detection in banking we propose a new technique "Secure banking System using Anti-Phishing Framework". This framework detects the fake web sites as well as provides security with respect to phishing attacks. In this framework we identify phishing site as well as the authorized user.The proposed system has two phases. In the first phase, a new user registers itself. While making registration the web application chooses an image and then this image is converted into two share images. While authentication phase, both share of image is matched only if

the user is authorized. Because the share is only available with original user as well as original server.

II. VISUAL CRYPTOGRAPHY

Visual Cryptography is very well known technique in network security. Visual Cryptography is first proposed by the Moni Naor and Adi Shamir.Visual cryptography is a simple and very secure way to allow the secret sharing of images without any cryptographic computations.It is the technique to send and receive encrypted messages which cannot read by any user it only decrypted by the sender or the receiver. Encryption and decryption are done using various algorithms in such a way that no other user can read the message ,only the intended recipient can decrypt and read the message.Visual cryptography provides the security against sending and receiving of the information.

III.CRYPTOGRAPHY

Cryptography is nothing but the storing and transmitting the data in a particular form so that only authorized or intended sender and receiver can read it and process it.Cryptography has two techniques such as Encryption and Decryption.Conversion of the plain text into cipher text is nothing but Encryption. And conversion of the cipher text into plain text is nothing but the Decryption.

IV.STEGANOGRAPHY

The word Steganography comes from the two Greek words: steganos means covered and graphien means to write. Steganography is very old art to hide the information into another data using various techniques. The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. The advantage of steganography is the existence of the information into an image will not noticed at all. Steganography is of various media like Steganography in Text, Steganography in Audio and Steganography in Images.In our framework we use Steganography in images. The simple meaning of this is nothing but hiding the data or information into an image.Nowadays, using a combination of steganography and the other methods, information security has improved considerably.

V. RELATED WORK

Phishing web pages are forged web pages which is very similar to the original web pages. Most of these types of web pages have very high visual similarities to scam their victims. Many of these types of web pages look exactly similar the real web pages. Victims of these phishing web pages may expose their personal information like bank account details, password, credit card details, or any other important information to the phishing web page owners. It includes techniques such as tricking customers through email and spam messages, man in the middle attacks, installation of key loggers and screen captures.

Following are some techniques to identify the phishing web sites:

Emails are one of the most common and very easy techniques for phishing, due to its simplicity phishers can deliver crafted emails to millions of original email addresses very quickly and can fool the recipients utilising well known flaws in the SMTP.

DNS-based anti-phishing technique is one of the technique to detect the phishing. DNS- based anti-phishing technique mainly includes blacklists, heuristic detection, the page similarity assessment. But they do have some shortcomings.

Heuristic-based anti-phishing technique is another technique to identify the phishing websites. In this technique analyse the phishing site characteristics and generate a classifier using those characteristics. When user request for a particular web page then classifier determines whether the requested web page is phishing or not.
Disadvantage: Heuristic-based anti-phishing technique takes time to generate a classifier. This technique is easy for attackers to use technical means to avoid the heuristic characteristic detection

Blacklist is a DNS -based anti-phishing technique which is most commonly used by the browser to identify the phishing sites. In this technique one blacklist query interface is maintained. When user access any web page first it verified by the administrator whether it is in blacklist or not. If the requested web page is in blacklist then the requested web page is phishing web site. But this technique have many disadvantages. Phishing web sites is for short term. A website might be shut down before we found it as a phishing website.
Disadvantage: Blacklist-based technique cannot detect the websites that are not in the blacklist database. Because the life cycle of phishing websites is very short term and time taken for establishment of blacklist has so long, the accuracy of blacklist is islow.

CANTINA is nothing but Content-Based anti-phishing technique to detect phishing websites.
CANTINA examines the content of web pages to determine whether it is legitimate or not.
CANTINA is quite good to determine the phishing web sites.
Disadvantage: CANTINA is a very time consuming technique. It needs more time to calculate a pair of pages, so using this method to detect the phishing sites is not suitable.

VI.PROPOSED METHODOLOGY

Phishing is very common nowadays mainly in banking so that to avoid phishing detection and prevention is very important so that we are proposing a new methodology to

detect the phishing website. Our framework is based on the Anti-Phishing image captcha validation scheme using visual cryptography. It protets password and other confidential information from the phishing websites and provides the security.

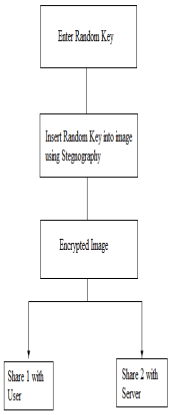
The proposed approach mainly divided into two phases:

A. REGISTRATION PHASE

In registration phase, a key string is asked from the user at the time of registration for the secure website. The key string may be a combination of alphabets and numbers to provide more secure environment. Using steganography generated key will be inserted into an image and this stegano image can be encrypted.

This encrypted image divide in to two shares, one share for user and second for the server side.

Figure 1:-Registration Phase.



B. LOGIN PHASE:

In login phase, the user side encrypted image is uploaded after that server side image and user side image concatenate and forms a encrypted image. This encrypted image can be decrypted and key is separated from this image. If the key matches at the time of registration phase and login phase then that site is trusted site.

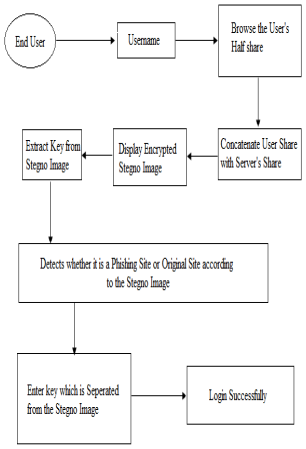


Figure 2:-Login Phase.

VII. IMPLEMENTATION & ANALYSIS

A. AES ALGORITHM:

1. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128-bits.
2. The key size can be 128,192 or 256-bits.
3. Private key is given to user when share1 is kept with user for secure sending of share1 from server to user.
4. At the time of transactions, user need to enter the key for authentication process.
5. After proper authentication, user is varied and goes for further process.

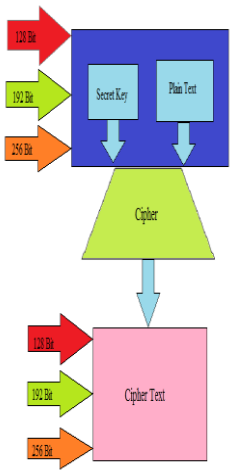


Figure 3:-AES Algorithm.

STEPS OF ENCRYPTION AND DECRYPTION-

Step 1: Get width and height of the image. Step 2: Horizontal block=image width/2. Step 3: Vertical block =image height/2.
Step 4: Number of block = horizontal block X vertical block.
Step 5: Encrypt all the pixels.

VIII. CONCLUSION

Now a days in banking field Phishing attack are very common because it can attack globally to stole the user`s confidential information. To detect the phishing website we proposed "Secure Banking System using Anti-Phishing Framework". This proposed system identifies the phishing websites and secure the bank user`s information from the attackers.

REFERENCES

1. International Journal of Advanced Research in Computer and Communication Engineering "An Anti-phishing Framework using Visual Cryptography", Vol. 4, Issue 2, February 2015.

2. International Journal for Research in applied Science and Engineering Technology, "detecting phishing websites based on visual cryptography, vol. 2 issue iv, April 2014.

3. IJCSMC "An Anti-phishing Framework with New Validation scheme using Visual Cryptography, vol. 3, issue. 2, February 2014, pg. 739.

4. International Journal of Research in Computer and Communication Technology, "The Secured Anti Phishing Approach using Image based Validation", vol .2, issue 9, September -2013.

5. International Journal of Computer Trends and Technology, "An Anti-Phishing Framework for Blocking Service Attacks Using Visual Cryptography, volume 4 Issue10 Oct2013.

6. Mounika Reddy.M, Madhura Vani.B,"A Novel Anti Phishing framework based on Visual Cryptography, International Journal of Advanced Research in Computer and Communication Engineering, Vol.2 Issue.9, September 2013.

7. Mary Ruby Star.A.L., T.Venu,"An Anti- Phishing Framework For Blocking Services Attacks Using Visual Cryptography, International Journal of Computer Trends and Technology, Volume.4 Issue.10,October 2013.

8.Divya James,Mintu Philip, A Novel Anti Phishing framework based on Visual Cryptography, in Journal on Cryptography,2012.

9. Nirmal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'", 2010.

10. Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method'", 2010

11. Sun Bin.; Wen Q iaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach, 2010.

12. Thiyagarajan, P., Venkatesan, V.P., Aghila, G.,"Anti-Phishing Technique using Automated Challenge Response Method'", 2010.

