Design and Implementation of Anti Phishing Framework based on Visual Cryptography

[1]Senthil Kumar K
Asst. Prof/CSE
Muthyammal Engineering College,
Rasipuram, Tamilnadu.

[2]Deepnesh M
IV Year/CSE
Muthyammal Engineering College,
Rasipuram, Tamilnadu.

[3]Dinesh Kumar A
IV Year/CSE
Muthyammal Engineering College,
Rasipuram, Tamilnadu.

[4]Gothanda Sankar V
IV Year/CSE
Muthyammal Engineering College,
Rasipuram, Tamilnadu.

***Abstract*: Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. In this paper we have proposed a new approach named as "Design and implementation of Anti phishing framework based on visual cryptography" to solve the problem of phishing. Here an image based authentication using Visual Cryptography (vc) is used. The use of visual cryptography is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed 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 revealed to the user it can be used as the password..**

Keywords: Phishing, visual cryptography, image captcha, shares.

1. INTRODUCTION

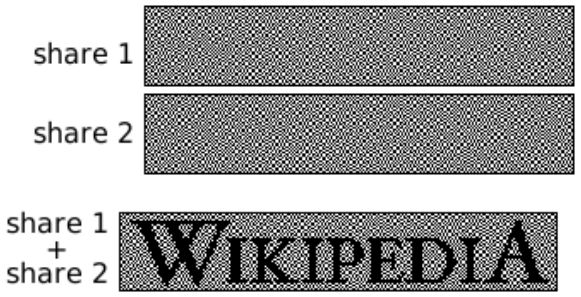
Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanisms should also be so effective. Thus the security in these cases be very high and should not be easily tractable with implementation easiness.

Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security.

Phishing is a form of online identity theft that aims to steal sensitive information such as online applications passwords and sensitive information from users.

Visual Cryptography:

One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.



VISUAL CRYPTOGRAPHY EXAMPLE

II. LITERATURE SURVEY

This paper introduces the idea of hierarchical visual cryptography. Authentication is the important issue over the internet. This paper describes a secured authentication mechanism with the help of visual cryptography. Visual cryptography simply divides secret information in to number of parts called shares. These shares are further transmitted over the network and at the receiving end secrets are revealed by superimposition. Many layers of visual cryptography exist in proposed system hence called hierarchical visual cryptography. Remote voting systems now a day's widely using visual cryptography for authentication purpose.

Now a days only few people go for voting because of their tight schedule. There are many reasons, few may be everyone has to go to voting center, we have to stand in a

long queue, many may be tired because of their tight schedule. So we have developed online voting system. But this system has some disadvantage. Phishing attackers directly get the passwords from the user and they enter into the relevant web sites with correct password. Consider an online polling system for corporate companies, polling is happening once in a year to elect the president or secretary or key directors of the company. At present system all the votes are has to assemble at one place on polling day and put their vote. In this approach we are making use of a new scheme which is known as Visual cryptography. In this scheme we are making use of visual information for security. Here we are dividing original image into two shares which are stored in separate database. Whenever these two shares are stacked with each other we get the original image. Once we get the original image it can be used as password. This system is very useful and safe for online remote voting. This system is web based application so that it can be accessed by any authorized person anywhere in the world through internet.

Phishing is a plague in cyberspace. Typically, phish detection methods either use human verified URL blacklists or exploit webpage features via machine learning techniques. However, the former is frail in terms of new phish, and the latter suffers from the scarcity of effective features and the high false positive rate (FP). To alleviate those problems, we propose a layered anti-phishing solution that aims at 1) exploiting the expressiveness of a rich set of features with machine learning to achieve a high true positive rate (TP) on novel phish, and 2) limiting the FP to a low level via filtering algorithms. Specifically, we proposed CANTINA+, the most comprehensive feature-based approach in the literature including eight novel features, which exploits the HTML Document Object Model (DOM), search engines and third party services with machine learning techniques to detect phish. Moreover, we designed two filters to help reduce FP and achieve runtime speedup. The first is a near-duplicate phish detector that uses hashing to catch highly similar phish. The second is a login form filter, which directly classifies webpages with no identified login form as legitimate. We extensively evaluated CANTINA+ with two methods on a diverse spectrum of corpora with 8118 phish and 4883 legitimate webpages. In the randomized evaluation, CANTINA+ achieved over 92% TP on unique testing phish and over 99% TP on near-duplicate testing phish, and about 0:4% FP with 10% training phish. In the time-based evaluation, CANTINA+ also achieved over 92% TP on unique testing phish, over 99% TP on near-duplicate testing phish, and about 1:4% FP under 20% training phish with a two-week sliding window. Capable of achieving 0:4% FP and over 92% TP, our CANTINA+ has been demonstrated to be a competitive anti-phishing solution.

In this paper, we study the activeness of phishing black-lists. We used 191 fresh phish that were less than 30 minutes old to conduct two tests on eight anti-phishing toolbars. We found that 63% of the phishing campaigns in our dataset lasted less than two hours. Blacklists were ine_ective when protecting users initially, as most of them caught less than 20% of phish at hour zero. We also found that blacklists were updated at di_erent speeds, and varied in coverage, as 47% - 83% of phish appeared on blacklists 12 hours from the initial test. We found that two tools using heuristics to complement blacklists caught signi_cantly more phish initially than those using only blacklists. However, it took a long time for phish detected by heuristics to appear on blacklists. Finally, we tested the toolbars on a set of 13,458 legitimate URLs for false positives, and did not _nd any instance of mislabeling for either blacklists or heuristics. We present these _ndings and discuss ways in which anti-phishing tools can be improved.

The project titled “Remote Voting System for Corporate Using Visual Cryptography” aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place, even when key stakeholders of election process are not available at workplace. This is enabled by leveraging the features that are provided by visual cryptography that are implemented in Remote Voting System. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into his login by entering the correct password which is generated by merging the two shares.

III. SYSTEM ANALYSIS

A. Existing Work

The most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users The question is how to handle applications that require a high level of security. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. One definition of phishing is given as “it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication”. Another comprehensive definition of phishing, states that it is “the act of sending an email to a user falsely claiming to be an established legitimate enterprise into an attempt to scam the user into surrendering private information that will be used for identity theft”.

B. **Drawbacks**:

1. Not secure
2. Phishers can get personal confidential information such as passwords, credit card information

3. Fake websites which appear similar to original one

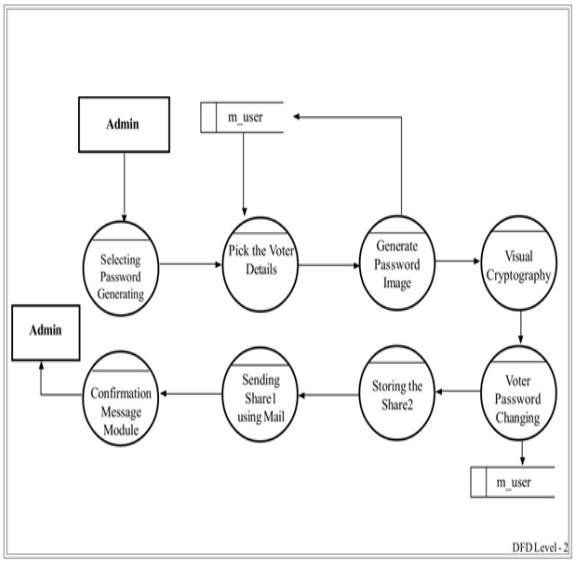
C. Proposed Work:

In this paper we have proposed a new approach named as "A Novel Anti-phishing framework based on visual cryptography "to solve the problem of phishing. Here an image based authentication using Visual Cryptography is implemented. The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares (known as sheets) that are stored in separate database servers(one with user and one with server) such that the original image captcha can be revealed 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 revealed to the user it can be used as the password. Using this website cross verifies its identity and proves that it is a genuine website before the end users.

D. Advantages:

1. Secure
2. Avoid fake websites
3. It is useful to prevent the attacks of phishing websites on financial web portal, banking portal,
4. Online shopping market.

IV. WORK FLOW



V. MODULE DESCRIPTION

A. Login modules.

In the Login phase first the user is prompted for the username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website, for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not.

B. Registration module.

In the registration phase, a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the shares is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data. After the registration, the user can change the key string when it is needed.

C. Image Generation module.

The user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website, for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not.

D. Captcha Creation Module.

The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the shares is kept with the user and the other share is kept in the server.

VI. CONCLUSION

The project" Design And Implementation Of Anti Phishing Framework Based On Visual Cryptography" is developed using c# as the Front End with MS-SQL Server 2000 as the Back End. ADO.Net is used in this project to link Dot Net and MS-SQL Server. Dot Net is a unified web platform that provides all the services necessarily required to build enterprise-class applications. Thus the project conforms to the requirement specification stated in the beginning.

VII. FUTURE ENHANCEMENT

This application is very useful in corporate organization to elect president, chairman, secretary and board of directors. With the help of this application, we can able to safeguard the password and polling from illegal activities. We tested this application and it shows successful result and it passes all the constraints specified in scope of the project.

VIII. REFERENCES

[1] Diffie, W., and Hellman, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp.
[2] Garret, Paul. Making, Breaking Codes: An Introduction to Cryptology. Upper Saddle River, NJ: Prentice-Hall, 2011
[3] Hoffstein, Jeffery, Pipher, Jill and Silverman, Joseph H. NTRU: A Public Key Crypto http://grouper.ieee.org/groups/1363/lattPK/submissions.html#NTRU1
[4] Kurose, James F., Ross, Keith W., Computer Networking: A top Down Approach Featuring the Internet. 2nd edition. Addison Wesley 2014.

REVIEW THROUGH WEB REFERENCE:

1. www.codenotes.com
2. www.dotnetspider.com
3. www.gotdotnet.com
4. msdn.microsoft.com
5. www.dotnet247.com
6. www.cs.columbia.edu
7. www.cdt.luth.se/~peppar/docs/lic/html/node66.html