Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

Securing Internet Banking with a Two - Shares Visual Cryptography Secret Image

Aparnaa. K. S.
Department of Computer Science and Engineering,
Paavai Engineering College,
Anna University,
Chennai, Tamil Nadu, India

Sathyasundaram. M.
Department of Computer Science,
Paavai Engineering College,
Anna University,
Chennai, Tamil Nadu, India

Santhi. P.
Department of Computer Science and Engineering,
Paavai Engineering College,
Anna University,
Chennai, Tamil Nadu, India

***Abstract*— Phishing is an illegal attempt to steal the sensitive personal information of any individual or organization without their consent. This information leakage in the internet banking will lead to a huge threat to the enormously increasing online bankers in day-to-day life. A new approach for phishing websites identification and securing Banking customers' personal data from phishing attackers is introduced. 'Original Personal Security Image' CAPTCHA is chosen individually by Client using their self preferred text and then create an image with overlapping Text over a dummy background. Later, splitting it into two shares and store those in separate databases like server and client level database created to serve as intermediary database that asks some questions about the security text provided by the client during the security image creation (which we call CAPTCHA as graphical password (CaRP). CaRP is both a CAPTCHA and a graphical password scheme) we make them as a security key for users. The original image is achieved only if client share CaRP1 is merged with server share CaRP2 i.e. CaRP1 + CaRP2.**

***Index terms*— Banking, Internet, Network security, Online, Phishing, Security.**

1. INTRODUCTION

Online banking has become an emerging trend at present date. As rapid as the online banking increases, the attacks over the online account also increases. One of such attacks is the Phishing attack. This attack is said to be the attempt by any individual or a group who are involved in illegal activity of stealing the personal confidential information of online users through some fake or look-a-like websites of an existing authorized website. It is a form of performing personal identity theft through internet that focuses to store the sensitive personal data. This data includes their online banking passwords and other account information of the users. So many reports were made over these phishing attacks. Such attacks have been noticed to be escalating in the number of attacks along with increasing online customers and sophistication. To provide improved security from leaking of confidential information we need to switch over to an even more reliable protection scheme to ensure safe networking of transactions. Online bank customers had always been the favorite targets of those who involve in phishing attacks, so that the account details of those customers can fetch them more money in just few seconds.

At present, many bank customers use online transactions frequently. So, the customer will have a set of username and password to access the bank account. These are very sensitive and a confidential information. When these fall into wrong hands of the phishing attackers, the information can be used by the attacker to access the bank account. This will lead to a huge loss to the customer. Unfortunately many people fall into the scams. This threatens the security system of online banking by spreading the fear among customers.

1.1. OVERVIEW

Now-a-days where online banking has been increasing rapidly, sadly, the Phishing scams are increasing in same pace. The most used two methods of attacking by them are

(i) Email phishing
(ii) Website phishing

'Email Phishing' involves the sending of a fake mail to the victim and requesting them to provide confidential information like an established organization. This can be avoided by just being aware of one fact that no legitimate bank will ask to give your account password in any emails that they send you. The process of creating a look-a-like fake website of an established organization and stealing the data from the user is referred as 'Website Phishing'. This can be avoided by verifying whether the website you are at is a secured website or not. But verifying every time is not always possible even to expert customer. So this made rise to develop some reliable techniques to overcome 'Website Phishing'.

Unlike email phishing the victims of website phishing can lead to huge number of victims because it is tough to detect if it is an authorized site or not by novice users. Even experts can become victims because of increased online purchases which is done mostly through pop-up window for payments.

1.2. EXISTING SYSTEM

The existing system makes use of a 'Security image' personally chosen by the client during the process of signing up. Then on each and every Log-IN process, first the Username or User Id is requested to be entered. The next step

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

takes to next webpage to get password. This prevents phishing by displaying their 'Security image' which is loaded from the database of the server. This will give the user the surety that it is not a fake website but an authorized site. This system uses two steps logging in process which makes any phishing personal to perform two attacks and only at second it is possible to get the actual information of both Username and Password from the client.

1.1.1. Demerits of Existing System

a) Limited Security Images

The existing system has certain limitation of the Security images in which the user has to choose one among those security images. The probability of guessing the security image or finding them is so easy using this limited pool of images.

b) Two attacks to get all the Information

The attacker first will attack the user to get the username. Simultaneously masquerade the user into Server and steal the security image by making an incomplete transaction and also displaying the user a temporary error. The user could be asked again to type same username and this time the stolen security image can be displayed and the victim falsely believes it as an authorized site. Then the attacker can receive the password from the user. This stolen username and password may be used even to perform unapproved transactions by the attacker.

c) Single step heuristic based technique

Heuristic is the precise word for self discovery or common level of sensing problem with some simple basic logics. The heuristic based Anti-Phishing technique used here makes the user to verify if the website they are entering their password is a secured website or a phishing site by seeing if the security image is true. But it does not verify from the server end if it is the actual client or an attacker who has stolen information from client through Phishing website and impersonates as the client. So, just a security image is not secured enough to stop this third party eaves dropping.

1.3. PROPOSED SYSTEM

The proposed system uses 'Visual Cryptography' image which is considerably better in reliability. In order to achieve comparatively higher reliability, we prepare a 'Security image' for each client using their own choice of word. Then that image is split up and used while submission of User Id and password which are made entered in separate web pages to perform the image verification. To help novice users who cannot identify secured http connection (https://), this image display will ensure them to know that this website is not fake and they are free from Phishing attacks. The user is first asked to provide Username; after displaying the first share of the security image stored in 'Intermediary database' the user is asked to answer any one question chosen randomly from the pool of questions about the 'Security image text' the user provided during signing up; after validating the answer with the security text values in 'Server database', the server discloses the complete 'Security image' superimposing first share received and second share that it has; looking at the complete image user is satisfied and sever also gets satisfied that there is no eaves dropping or impersonating. Finally the user enters the password.

1.3.1. Merits of Proposed System

a) Delimit the possible Security Images

The proposed system creates security images from a text chosen by the user. The text is embedded with some black and white image with lesser contrast and higher brightness such that text is visible to human eye. This technique delimits the limited security image concept of existing system.

b) Number of attacks to steal is impossible

The total number of attacks to completely impersonate someone is made undefined. It is because, the security text details are only known to the client. Even if the phishing attacker eaves drop he cannot answer all the questions that are asked randomly every time during Log-IN.

Additional to this, even if the attacker steals the security image, the image has both user provided text with server generated key. The attacker cannot identify the user text to answer the questions.

c) Multi-step heuristic based technique

The heuristics of verifying if the website is not a phishing site is increased by 'Visual cryptography' technique over the security image that is encoded by the user text within a image through 'Steganography'.

1.4. Architecture Diagram

The proposed technique to overcome Phishing implements Steganography and Visual cryptography of threshold (2, 2). This creates a security image to secure user data as depicted in the architecture diagram (Fig.1.1) shown below.

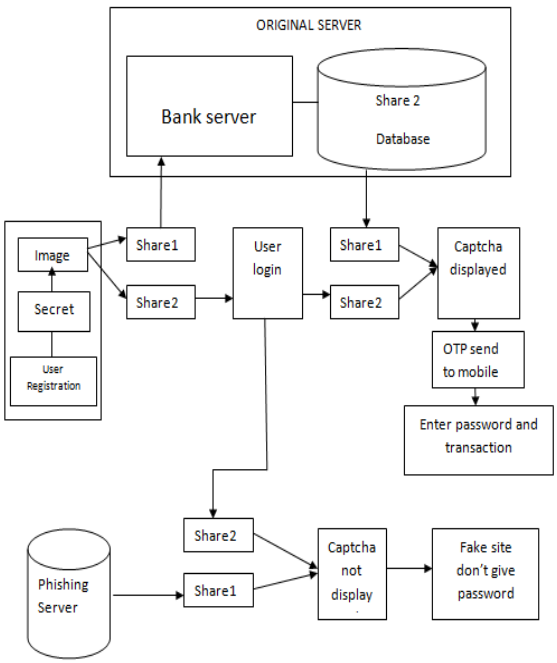


Fig.1.1 Architecture diagram

2. PROBLEM DESCRIPTION

1. PHISHING ATTACKS

The phishing is defined as "the unauthorized sneaking of others' sensitive information without their acknowledgment using some social engineering techniques. It is also said to be

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

unauthorized acquisition of sensitive information about a user by performing masquerade attack like a trustworthy unit through any communication system". When the account information is phished, it can lead to major mishaps when a huge amount of customers are being scammed.

This is said to be "an offense where the impostor will get to obtain the personal information like Social security data and use it without the consent of the user". Now-a-days, net banking has become popular. Same way the attacks made over this banking is also increasing in its count. Phishing is noted to be a challenge to the security of online users. Phishing allows different forms of information leakage where attackers develop new innovative ideas that are increasing the victims count. So, preventive mechanism should also be equally effective.

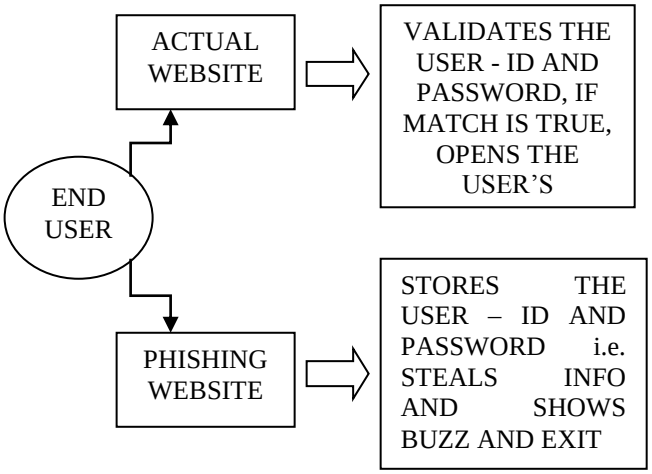


Fig.2.1. Activity comparison of Actual website with Phishing website

2.1. *TECHNIQUES TO OVERCOME PHISHING ATTACKS*

The proposed system introduces a new technique for detecting whether it is a original site or duplicate. In this system an image is formed by the user credentials and embedded into pixel by pixel. It denotes the pixel into shares. Each of the shares of pixel can be either a white pixel or a black pixel. The choice of that pixel value is made randomly (i.e. two choices are available for each pixel). Any individual share cannot disclose any clue about the original pixel. All the pixels of the secret image will be encrypted using multiple independent random choices. The value of the original pixel 'P' can be only determined when both the shares of the image are overlapped.

- Suppose 'P' is a black pixel, then it is made into two sub pixels with black color,
- Or else suppose 'P' is a white pixel, it is made into two sub pixels with one as black and the other as a white pixel.

The concept of Image Processing and a (2, 2) threshold Visual Cryptography Sharing (VCS) scheme is used. The technique of processing the input of image and then get the output as either a processed form of the same image and/or modified characteristics of the given image is known as Image Processing. Another interesting technique called Visual Cryptography (VC), is a process of securing a message by encrypting an image into 'n' shares of single image, where stacking the 'n' number or less of shares reveals the actual secret image. The number of shares created and the number of shares that may be needed to reveal the secret behind those shares are decided by the VCS scheme being implemented.

3. DEVELOPING METHODOLOGY

We are securing the internet banking customers from the attackers called 'Phishers or Phishing attackers' using two major techniques.

- Steganography and
- Visual Cryptography Sharing (VCS)

3.1. *STEGANOGRAPHY*

Steganography is the art of writing a hidden message where none apart from the actual receiver knows of the existence of the message. The 'Steganography' technique of Bit-Plane Complexity Segmentation (BPCS) is used. This scheme is said to be a lousy-image compression technique. The Kyushu Institute of Technology is the first to propose this scheme of BPCS Steganography. This allows us to embed a large amount of data in the images. We embed the Security text provided by the user into an image of Black and White random pixel combination of background.

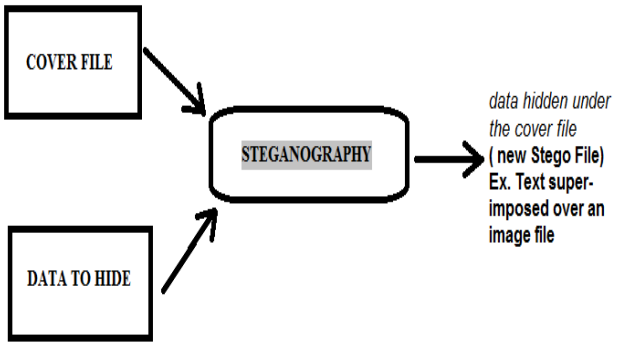


Fig.3.1 Steganography with Bit-Plane Complexity Segmentation on Text

3.2. *THE VISUAL CRYTOGRAPHY SHARING (VCS) SCHEME*

The method of encrypting a visual format of secretive and sensitive data into multiple shares, which on overlapping provides the actual visual data is called as Visual Cryptography sharing (VCS). Based on the number of shares to be created, following are some important types of threshold schemes.

- (2, 2) threshold VCS - It is a basic threshold scheme. The input is a secret message and it is encrypted into two different shares. To reveal the output into the secret image, both shares must be overlaid.
- (2, n) threshold VCS- This scheme splits the secret image into 'n' shares. Interestingly, at least two of those 'n' shares are superimposed, the secret can be revealed.
- (n, n) threshold VCS- The input is a secret message. Here it is encrypted into 'n' different shares, where the value of this 'n' may be any finite positive integer. To reveal the output into the secret image, all of the 'n' shares must be overlaid.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

- (k, n) threshold VCS- This scheme splits the secret image into 'n' shares. When any group of at least 'k' shares of the secret image are superimposed then the secret image will be revealed.

3.3. *(2,2) THRESHOLD VCS SCHEME*

In the case of any VCS scheme, the input must an image and they are made into multiple shares. In (2, 2) threshold VCS, image is made into two shares. Each pixel P in the original image is encrypted into two sub pixels (pairs) called shares. The choice of the shares for a pixel in the image is determined in a random manner (there exists two choices for any pixel and any one of the two can be applied). Neither of the shares provides any details about the input image pixel without overlapping because all pixels in the shares will be encrypted independent to each other using random choices.

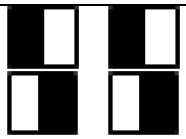
White Sub-pixel	I - Share II - Share	On superimposing
p=1/2 p=1/2		

Table.3.1. White based pixel sharing technique in proposed system using Visual Cryptography

If the two shares are overlapped or super - imposed, then the value of the initial input pixel P can be determined. If 'P' pixel is a black color pixel, then we get it as two black color sub pixels. If it is a white color pixel, then we get it as one black sub pixel and the other one as one white sub pixel.

The table 3.1 explains the white sharing into shares and the table 3.2 explains the black pixel sharing respectively. It shows two possible ways of splitting a pixel in a (2, 2) VCS.

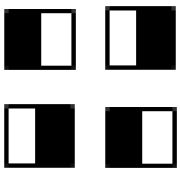
Black Sub-pixel	I - Share II - Share	On superimposing
p=1/2 p=1/2		

Table.3.2. Black based pixel sharing technique in proposed system Visual Cryptography

4. USER INTERFACE REQUIREMENTS

The modules that are to be implemented in the interface are enlisted as follows:

A. Registration With Secret Text
B. CAPTCHA Image Generation
C. Security Image Shares (VCS) Creation
D. Log-IN Phase

4.1 REGISTRATION WITH SECRET TEXT

In the registration phase, the user details like username or user-Id, password, email-Id, address, and 'a Security text' are requested from the user at the time of registration for the security of the user from Phishing attackers.

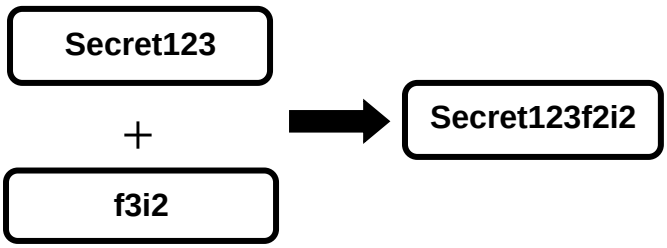


Fig.4.1. Security Text concatenated with Key String from Server

The key string can be a combination of some alphabets and numbers to provide increased security. This string is concatenated with some randomly generated unique 'Key string' in the server.

4.2 CAPTCHA IMAGE GENERATION

The security string or key string entered by the user during the registration process is taken as input. Then it gets converted into an image by using the java classes called 'Buffered Image' class and 'Graphics2D' class in this phase. The dimension of the image used is '260*60'.

Text is represented in black color and the background is represented in white color. The security text in image has a font value set by 'Font' class in java. Finally, image is generated. This will be written into the user key folder. The location is set to the server database.

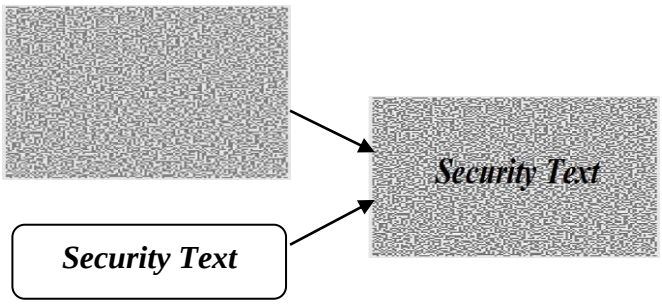


Fig.4.2. Security Image created with the Text ('Security text' + 'Key String')

4.3 SECURITY IMAGE SHARES (VCS) CREATION

The image CAPTCHA is divided into shares. Since we use (2, 2) VCS, we create two shares. One of the shares will be kept with the 'Intermediary' database. The other share is kept in another master database created by server to hold every details of the user including Secret security image, user Security Text, answers for security questions and original image created during CAPTCHA generation phase.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

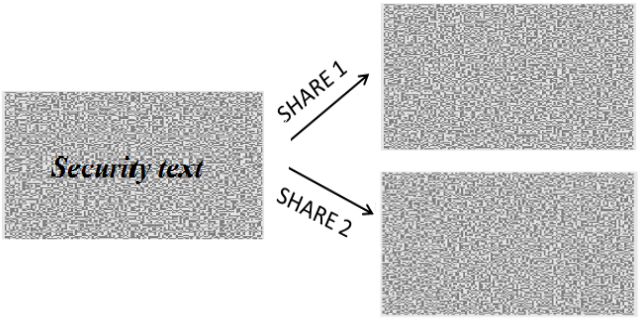


Fig.4.3. Creating two shares for the security image using Visual Cryptography

The share in the Intermediary database (i.e. share of the user) and the original image CAPTCHA is displayed to the user during later verification process that occurs at the login phase. The image CAPTCHA is stored in the server database of the confidential website as sensitive and confidential data.

4.4 LOG-IN PHASE

The login phase (Refer Fig.4.4) has three steps where the user must enter username, next a share of the CAPTCHA displayed and ask a secret question and then show complete CAPTCHA to get the password.

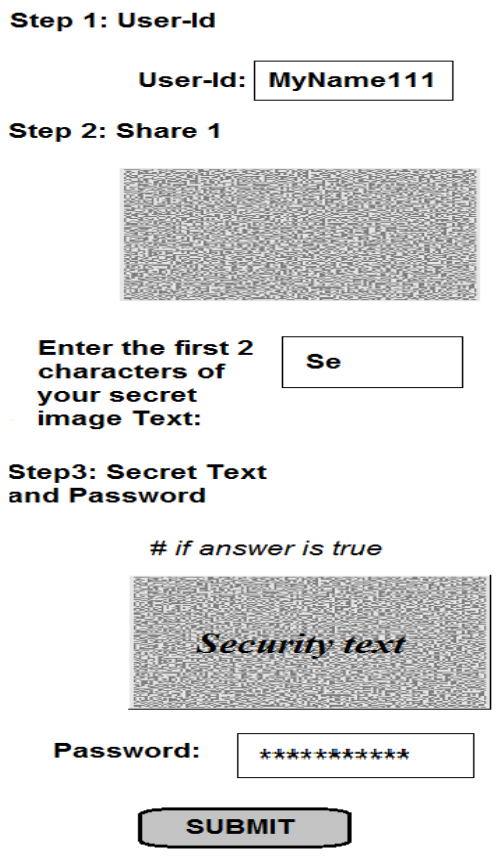


Fig.4.4. Steps involved in Log-IN process of the proposed system.

When the user logs into his online banking account, then first the user will be asked to enter only his User Name or User-Id. Then in the next webpage, the first share is displayed from the intermediary server and from a list of random questions about his secret key string, a question is asked. For example, "How many number of alphabets did you enter in your secret text?" If the answer is correct the first share will be sent to the server where the two shares namely the first share stored in Intermediate database and the second share (also known as server's share) in the database of the authorized bank, is superimposed over each other to produce the actual CAPTCHA image and that will get displayed in the next.

Here the end user gets to see through the human eyes and check whether the CAPTCHA image displayed in the Password page, is actually what the user has created at the time of registration. Finally, only after verifying the CAPTCHA is correct, the user must enter the account password. Finally, the user logs in into the website. Using the username of the user and also secret image CAPTCHA generated by stacking or superimposing both the shares, one can verify whether the website is authorized website or a phishing website and is it secured enough to enter the confidential data.

5. PERFORMANCE AND SIGNIFICANCE

The concept of Steganography and the (2, 2) threshold VCS is used. Then, the Intermediary database holds questions regarding the actual share value that is given as input by the User during Sign Up. For phishing attack identification and prevention, the proposed system uses a new methodology. It prevents the leakage of password and other confidential information to the network attack called Phishing by fake look-a-like websites.

Phishing web pages are forged web pages. It is created by malicious people to mimic the Web pages of authorized websites. This fake web page has the highest visual similarities to scam their victims. These victims of the 'Webpage – Phishing' may expose their sensitive information to the phishing web page owners.

Since this methodology is based on the image CAPTCHA validation scheme using 'Steganography' and 'Visual Cryptography', its reliability is at an improved level. The significances and limitations of this methodology are listed below.

5.1 *MERITS OF THE PROPOSED METHODOLOGY*

- It prevents password or any other types of confidential information from the phishing websites with 3 step logging in from other single and double steps logging in which are already in practice.
- The second step of viewing the share 1 and questioning any one of the question randomly chosen from pool of questions about Secret Image Text provided by User at Sign up time increases the reliability and security from the masquerading attacks or identity imposing attacks made by the phishing attackers.
- The third step of logging in which displays the user a superimposed image of share 1 and share 2 of the Secret image provides the user the assurance that it is not a phishing website and then the user can provide his/her sensitive data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

- This method provides improved security by not allowing the intruders to 'Log-IN' into the user's account. Even after the user knows the username of a particular user, he cannot masquerade because the intruder is not aware of the secret image or the whereabouts of the text.

6. CONCLUSION

Currently phishing attacks are so frequent. Phishing attack is a global threat. The attackers loot and illegally store the user's confidential information. The attackers may try to access those victim's accounts with their information. But in most cases, the victims are unaware of the attack that has stolen their information. The Phishing-Websites can be identified easily and optimally using the proposed project called as 'Securing Internet Banking with a two-shares Visual Cryptography Secret Image'.

The proposed methodology for internet banking secures the confidential information of 'Online Banking' users using this 3-steps security system with (2, 2) threshold VCS scheme that involves 2 shares of Security image. Final step is used to check whether the website is an authorized website or a phishing website by displaying a Secret Image CAPTCHA. Suppose the website the user is accessing is a Phishing website, that website can't be able to display the correct Security image CAPTCHA for that particular user because the CAPTCHA is generated by the stacking of two shares (one with the Intermediary database and the other with the actual Server database of the website). Here the server merges both the shares of the image and checks that output matches with the actual CAPTCHA of the user.

The individual user can verify if it is their CAPTCHA and if it is correct then he/she can ensure that the site is not a Phishing website. So, using this type of CAPTCHA image based security technique, Phishing attacker can't crack the sensitive account information of the users. Finally as a third layer of security it prevents masquerade attacks, such that, even after capturing confidential account details as such username and password of the user's account because along with 'Steganography' with Visual Cryptography technique, the user who wants to Log-IN must answer a randomly chosen question about the Secret image. So, the attacker can't mishandle the stolen information. The proposed methodology is significantly useful in the growing fields of Online-Banking portal, financial web portal, Online-Shopping market, where the attacks of phishing websites may create a big chaos.

7. REFERENCES

[1] R.Biddle, S.Chiasson and P.C.Van Oorschot, "Graphical pass - words: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.

[2] "Cognitive Authentication Schemes safe against Spyware" IEEE publication under security and privacy 2006 by Weinshall, D., Hebrew University of Jerusalem.

[3] R. Dharnija and A. Perrig., "Deja vu: A user study using images for authentication". In Proc. 9th USENIX Security Symposium, 2000.

[4] S.Wiedenbeck, J.Waters, J.C.Birget, A.Brodskiy, and N.Memon, "Pass Points: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[5] "Steganography using Genetic Algorithm along with Visual Cryptography for Wireless Network Application" by G.Prema and S.Natarajan.

[6] Dirik, N.Memon, and J.C.Birget, "Modeling user choice in the pass points graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.

[7] J.Thorpe and P.C.Van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007, pp. 103-118.

[8] P.C.Van Oorschot and J.Thorpe, "Exploiting predictability in click based graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.

[9] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Authentication in an Internet Banking Environment" October 12, 2005, the FFIEC agencies.

[10] Alok Bansal, Yogeshwari Phatak and Raj Kishore Sharma, "Quality Management Practices for Global Excellence", Prestige Institute of Management and Research Indore, 2015, page number 253.

[11] P.C.Van Oorschot and S.Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.

[12] Ch.Ratna Babu, M.Sridhar and Dr. B.Raveendra Babu, "Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security".

Aparnaa.K.S. is a student of Master of Engineering, Computer Science and Engineering, Paavai College of Engineering in Paavai Engineering College and has previously presented a paper about the security of Internet banking in the Rukmini Devi Institute of Technology, New Delhi in January, 2016.

Sathyasundaram.M. is an assistant professor in department of Computer Science and Engineering, Paavai Engineering College. He has completed his Master of Engineering.

Santhi.P. is an associate professor in department of Computer Science and Engineering, Paavai Engineering College. She has completed her Doctor of Philosophy.