International Journal of Engineering Sciences & Emerging Technologies, June 2013.
ISSN: 2231 – 6604 Volume 5, Issue 2, pp: 104-118 ©IJESET

AN ENHANCED MULTILEVEL AUTHENTICATION SCHEME USING GRAPHICAL PASSWORDS

P.S.V Vachaspati[1], A. S. N. Chakravarthy[2], P. S. Avadhani[3]
[1]C S E Department, Bapatla Engineering College, Baptla, A.P., India
psvvachaspati@gmail.com
[2]C S E Department, JNTUK UCEV, Vizianagaram, A.P., India
asnchakravarthy@yahoo.com
[3]CS&SE Department, AU College of Engineering, Visakhapatnam, A.P, India
psavadhani@yahoo.com

ABSTRACT

With the advent of internet, various online attacks have been increased and among them the most popular attack is phishing. An enhanced multilevel authentication scheme using graphical passwords focuses on solving the problem of phishing using Visual Cryptography. Visual Cryptography is explored to preserve the privacy of image by decomposing it into two shares that are stored in separate database servers such that the original image can be revealed only when both are simultaneously available that is we are achieving mutual authentication by this. Using this approach one can cross verifies both the user and the website as of genuine or not. Once the user finds the legitimate, he logs into the website using his password.In this paper, we have proposed Multi-level Authentication using graphical passwords, which is a generalization to improve the security from online attacks . In this approach we could achieve mutual authentication in which both the user and the website are authenticated.

KEYWORDS: *Authentication, Captcha, Passwords, Phishing and Visual Cryptography.*

I. INTRODUCTION

Today's network environment is full of dangerous attackers, hackers, crackers, and spammers. Authentication, authorization and auditing are the most important issues of security on data communication. An authentication system must provide adequate security for its intended environment, otherwise it fails to meet its primary goal. A proposed system should at minimum be evaluated against common attacks to determine if it satisfies security requirements. We classify the types of attacks on knowledge-based authentication into two general categories: guessing and capture attacks. In successful guessing attacks, attackers are able to either exhaustively search through the entire theoretical password space, or predict higher probability passwords (i.e., create a dictionary of likely passwords) so as to obtain an acceptable success rate within a manageable number of guesses. Guessing attacks may be conducted online through the intended login interface, or online if some variable text (e.g., hashes) can be used to assess the correctness of guesses. Authentication systems with small theoretical password spaces or with identifiable patterns in user choice of passwords are especially vulnerable to guessing attacks.

Fake websites which appear very similar to the original ones are being hosted to achieve this. Phishing is an attempt by an individual or a group to get confidential information such as passwords and credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Authentication is the first line of defence against compromising confidentiality and integrity. The various authentication systems were introduced but even they are also suffering from shoulder surfing and screen dump attacks.

1.1 Security

Generally passwords are used to provide security to a user in a website. But, password capture attacks involve directly obtaining the password, or part thereof, by capturing login credentials when entered by the user, or by tricking the user into divulging their password. Shoulder surfing, phishing, and some kinds of malware are common forms of capture attacks. In shoulder surfing, credentials are captured by direct observation of the login process or through some external recording device such as a video camera. Phishing is a type of social engineering where users are tricked into entering their credentials at a fraudulent website recording user input.

Malware uses unauthorized software on client computers or servers to capture keyboard, mouse, or screen output, which is then parsed to and login credentials. As will be seen, early graphical password systems tended to focus on one particular strength, for example being resistant to shoulder surfing, but testing and analysis showed that they were vulnerable to one or more other types of attacks. Except in very specific environments, these would not provide adequate security. Often playing an important role related to security is the particular process of encoding or discretization used | transforming the user input into discrete units that can be identified by the system and used for comparison during password re-entry. As will be seen, some schemes require that the system retains knowledge of the exact secret (or portion thereof), either to display the correct set of images to the user or to verify password entries. In other cases, encoded or discretized passwords may be hashed, using a one-way cryptographic hash, to provide additional security in case the password level is compromised.

1.2 Phishing

Phishing is an act of attempting to acquire sensitive information of a person by masquerading as a trust worthy entity in electronic transaction. Phishing is typically carried out by e-mail spoofing or instant messaging. Phishing e-mails contain links to websites infected with malware

1.2.1 List of Phishing Techniques

There are three types of phishing attacks. They are listed below.

Spear phishing

Phishing attempts directed at specific individuals or companies have been termed as spear phishing.

Clone phishing

This is a type of phishing attack where a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient's address is taken and used to create an almost identical or cloned email. The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a re-send of the original or an updated version to the original.

Whaling

Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

1.2.3 How Phishing Works?

Phishing is generally carried out through e-mail spoofing. Here, attacker sends a mail to the person whose details he wants to track. In the mail attacker hides his true identity and generally he sends a link which appears similar to the genuine website like bank website etc.., Here, attacker adds some message to mislead the user. For eg: In the mail attacker may send a message saying "We are updating our database so we request you to click the following link and update your data in our site." Innocent users think it is true and they login to the site providing their credentials and thus falling prey for Phishing attack.

1.3 Authentication

All material Security has become an inseparable issue as information technology is ruling the world. As a result of the astonishingly rapid advancement of various kinds of Internet technologies, more information are transmitted to all parts of the world from everywhere through the net. Some of the objects transmitted online may be important secret images, and in such cases the senders have to take information security issues into consideration before they can trustingly enjoy the speed and convenience that nothing in this world but the Internet can offer.

Cryptography is the study of mathematically related techniques to achieve Information Security in terms of confidentiality, data security, entity authentication and data origin authentication. However, it is not the only means of providing information security.

Cryptography includes a set of techniques to achieve confidentiality (amongst others) when transmitting or storing data. Traditional cryptographic schemes require end users to employ complex operations for encryption as well as decryption. An alternative to encrypt messages is Visual Cryptography (VC), where the decryption is completely performed by the human visual system. Visual cryptography[1] is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms of traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. VC schemes hide the secret image into two or more images which are called shares. The secret image can be recovered simply by stacking the shares together without any complex computation involved. The shares are very safe because separately they reveal nothing about the secret image.

1.4 Graphical Passwords

Like text passwords, graphical passwords[2] are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches.

Graphical password technique is one of methods which may provide more secure and more efficiency system for authentication. A set of secure passwords needs to be long enough and random , but that will be a problem for human to remember. Everyone will forget their settings everyday if they didn't use again. The research results showed that, when users forget their password, they can only remember part of the correctness. Usable and easy memorization is the main research issues of graphical password authentication.

1.5 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.

Cryptography

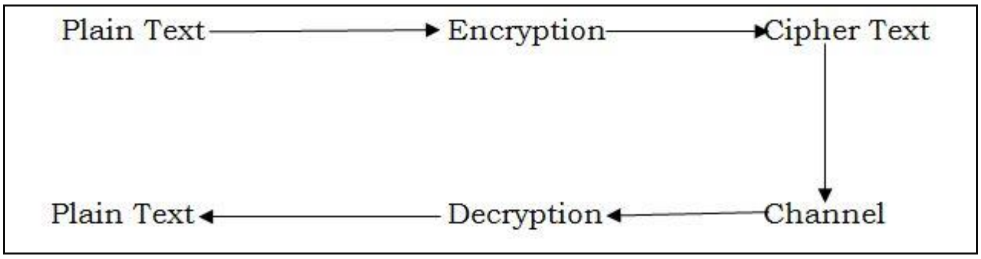


Figure 1 Sequence of Steps in Cryptography

Visual Cryptography is a secret-sharing method that encrypts a secret image into several shares but requires neither computer nor calculations to decrypt the secret image. Instead, the secret image is reconstructed visually: simply by overlaying the encrypted shares the secret image becomes clearly visible . A Visual Cryptography Scheme (VCS) [1] on a set P of n participants is a method of encoding a 'secret' image into n shares such that original image is obtained only by stacking specific combinations of the shares onto each other. It is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

- (2, 2)- Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid.
- (n, n) -Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed.
- (k, n) -Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed.[3]

In case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares.

VCS with random shares the traditional VCS or simply the VCS. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two conditions:

1) any qualified subset of shares can recover the secret image;

2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image.

Visual Cryptography

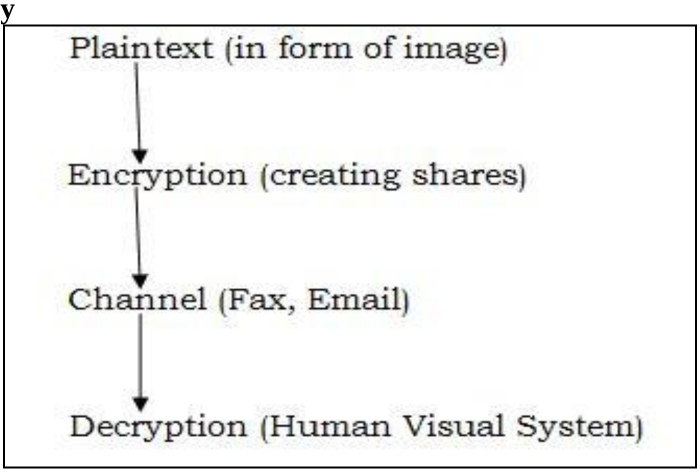

Plaintext (in form of image)
Encryption (creating shares)
Channel (Fax, Email)
Decryption (Human Visual System)

Figure 2 Visual Cryptography

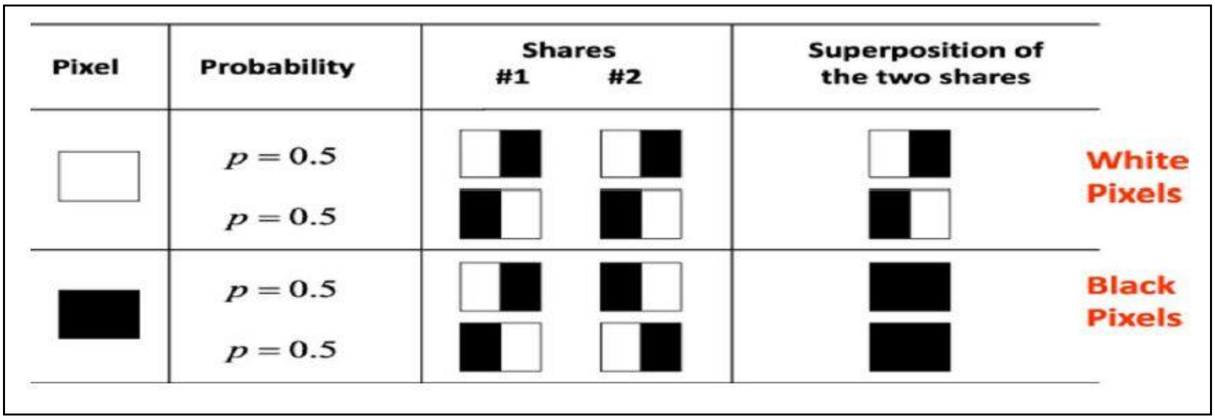


Figure 3 Shares of a White Pixel and a Black Pixel.

The choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices.

When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

The basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme that focuses on sharing secret images[4]. The idea of the visual cryptography model proposed in is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR. VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field. Many other applications of VCS, other than its original objective(i.e., sharing secret image), have been found, for example, authentication and identification, watermarking and transmitting passwords etc.,

Let us go through the practical example:

The figure shown below shows generation and dissolving that image Captcha into two shares using (2, 2) VCS. Image also shows reconstructed image Captcha from the shares. As we can see, Share1 and share2 are shares of Image Captcha and Reconstructed Image Captcha is also shown in the Figure

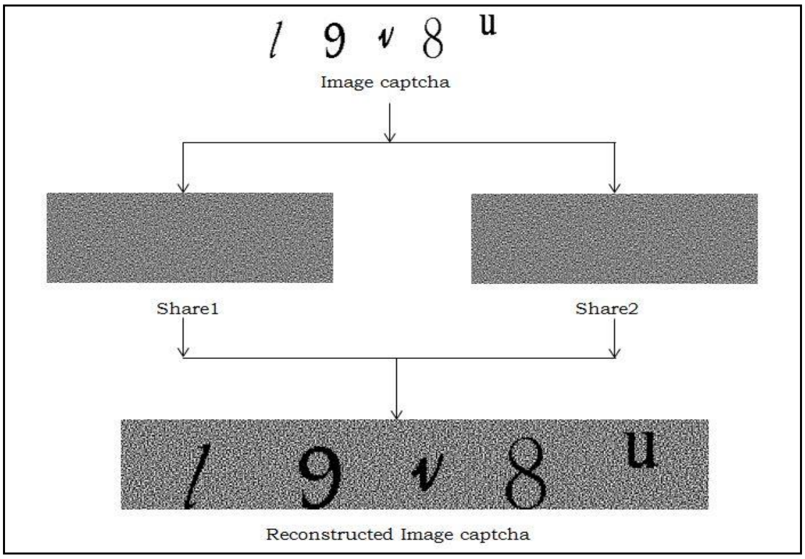


Figure 4 Shares Generation

In the next sections we'll discuss about Literature Survey, Implementation, Results, Conclusion and Future Scope.

II. LITERATURE SURVEY

Now-a-days there are many types of security that avoid online attacks . Still there are some limitations which are leading to violation of the security. This results in attacks in which the intruder can claim the user's confidential information.

2.1 Problem Formulation and Existing System

In the current scenario the main limitation in using the traditional password authentication method is that, a server must maintain a password table that stores each user's ID and password. If an intruder attacks the server system through attacks like phishing then he can access the entire information from the table. Even if the information is stored in the encrypted format the intruder can affect the system like modifying the user information by replacing correct information with wrong information in data base and thus leading to an attack where even the legitimate user is unable to login to his account etc.,. Such attack is known as Denial of Service (DoS) attack. At the same cost now a day's online transactions have become very common as well as the online attacks are also increased behind it. So security has become a very important part of human life. Recently authentication has become an important issue among many access control mechanisms. In prevailing systems a new approach such as mutual authentication is going to provide a solution to the online attacks like phishing. Mutual authentication is the one in which both the user as well as the server are authenticated.

2.2 Related Work

There have been many authentication methods that have been proposed by researchers for authentication. Some of the most prominent of them have been discussed here.

Initially there have been some techniques where user based mechanisms are used to authenticate server. Automated Challenge Response Method (ARM) [5] is one such authentication mechanisms where challenge generation module in server requests for response from Challenge-Response interface in client. Then Challenge-Response module calls get response application installed in client machine. Once this is done, user credentials are demanded from client and it is validated by server and thus transaction is made secure. This ensures two way authentication and also prevents man-in-middle attacks as response is obtained from executable which is called by browser and third man cannot interrupt at any cost.

There are also some Domain Name Service (DNS) based anti-phishing approaches[6] techniques which mainly include blacklists, heuristic detection, the page similarity assessment etc.., But, there are many disadvantages with these approaches.

Blacklist based technique is a DNS based anti-phishing approach commonly used by browsers. Some Work Groups provide an open blacklist query interface. Some of the most used browsers like Netscape Browser8.1, Google Safe Browsing (a feature in Google Toolbar for Firefox), Internet Explorer7 use blacklists to protect users when they are browsing through Internet. Blacklists are lists of URLs of some of the phishing sites.

There are many shortcomings in this approach. This technique has low false alarm probability, but it cannot detect the websites that are not in blacklists. Life cycle of phishing websites is too short for establishment of blacklists which makes this technique inaccurate.

Heuristic-based anti-phishing technique is a technique where a webpage is checked to find out whether the page has any of the phishing heuristics characters like host name, checking URL for common spoofing techniques and checking against previously seen images.

This method does not yield accurate results as even the attackers are aware of such techniques and they use some strategies so that they are not detected. So some *similarity assessment methods* have been proposed to detect phishing websites. For example, CATINA[7] is a content similarity based approach to detect phishing websites. Here, initially calculates the suspicious page's lexical signature using TF-IDF and then feeds this to search engine. Basing on the suspicious page's sort order in the search results the site is checked for its legitimacy.

There are many other similarity based assessment methods. Some of them are mentioned here.

Liu Wenyin and Anthony Y. Fu etc. [8] [9] proposed a page visual similarity assessment method to detect phishing websites, if a web page is similar to a financial organization's page, but it is not the organization's web page itself, it is considered a phishing site's page. JungMin Kang and DoHoon Lee [10] proposed the URL similarity assessment method, if an URL is similar to a bank's URL, but it is not the bank's URL, it is considered a phishing website's URL. There is low assess accuracy rate for the URL and content similarity assessment techniques. The speed of calculating the visual similarity between pages is too slow, so it is only used for phishing-spam detection generally.

Another scheme named A Three-Factor Authentication Scheme named *Phish-Secure* has been proposed to counter phishing[11].

As a first factor of authentication, an image similarity detection is done which helps in finding out which page the user tends to visit, then it is checked for Phishing. For this purpose a system captures the image of a webpage in a particular resolution in the required format. This image is termed as Visual image. If the attacker is going to create a Phishing site he is going to use the replica of the original webpage in order to fool the users. Now Phish-Secure gets the Visual image of the visited page and collects the mean RGB value of the image. This is termed as M_RGB. The database with Phish-Secure uses consists of details about the page which has to be authenticated. The actual mean RGB of various web pages is stored in the database which is denoted as AM_RGB. Phish-Secure will utilize this information and make a comparison to find out the similarity between the visited page and the page in the database. The similarity is obtained in means of percentage, if the percentage of similarity (PS) is greater than 99 % then Phish-Secure concludes which website the user is tending to visit. This is carried out by taking the corresponding URL in the database and checking is done in order to find whether the site is Phishing or not.

As a second factor of authentication Phish-Secure grabs the destination IP in Layer 3 which gives information about to which IP address the user is getting connected, this is referred as C_IP. If an attacker's web server IP address has already been found guilty the particular IP is blacklisted. Phish-Secure check this Blacklist with the C_IP and will warn the user. On the other hand if the C_IP is not found in Blacklist, further verification is done in the following step.

Here in this step Phish-Secure grabs the actual list of IP address of the provider which he tends to connect. This is because any provider may have multiple servers for the purpose of load balancing and the user may be connected to his location accordingly.

In order to avoid any confusion Phish-Secure gets the list of IP address which is referred to as actual IP and is checked with the C_IP (i.e.) the IP address to which the user is getting connected. If these two IP address are same Phish-Secure identifies the particular site as genuine and returns a message as authenticated. On the other hand if there is a mismatch in the above verification Phish-Secure identifies the site as Phishing and warns the user. In addition to this the C_IP is added to the black list so that in future if the attacker uses the same web server and tries to attack, Phish-Secure detects the site as Phishing in the second step.

There are many short comings in this method too. Most prominent of them being Time. This technique is very time consuming as it takes lot of time to calculate a pair of pages. So this method is not suitable for using on client terminal. Moreover, accuracy rate for this method depends on many factors such as the text, images and similarity measurement technique.

Another offline phishing detection system LARX (Large-Scale-Anti-phishing by Retrospective data-eXploration) [12] to detect phishing attack has been proposed. It uses traffic archiving in a vantage point to collect network trace data. Then, LARX uses cloud computing technology to analyze the experimental data similar to “divide and conquer” scheme. A physical server is also used for comparison. All of LARX’s phishing filtering operations are based on cloud computing platform and they work in parallel. LARX can be effectively scaled up to analyze a large volume of network trace data for phishing attack detection.

To meet the user traffic as users manage more accounts, OpenID was proposed. OpenID provides single sign-on (SSO) service, that is, we can enjoy service of multiple sites by signing in only once. But this is vulnerable to phishing attack, So many methods have been proposed to overcome this drawback. Some of them are mentioned here.

“New Anti-Phishing Method with Two Types of Passwords in OpenID System”[13], is one such method. In this method, two types of passwords have been put forward for anti-phishing for OpenID users. In this method only one fixed passwords and many temporary (session) passwords are used. Fixed passwords are bound to a PC or any electronic device which user owns or which he frequently uses. Temporary passwords are used when user logs in different systems, for this user is sent temporary passwords to his mobile or mailbox. This method effectively avoids phishing.

Detecting and identifying any phishing website in real-time, particularly for e-banking, is really a complex and dynamic problem involving many factors and criteria. Because of the subjective considerations and the ambiguities involved in the detection, Fuzzy Data Mining (DM) Techniques can be an effective tool in assessing and identifying phishing websites for e-banking since it offers a more natural way of dealing with quality factors rather than exact values. "Modelling Intelligent Phishing Detection System for e-Banking using Fuzzy Data Mining" [14], a novel approach to overcome the 'fuzziness' in the e-banking phishing website assessment propose an intelligent resilient and effective model for detecting e-banking phishing websites. The proposed model is based on Fuzzy logic (FL) combined with Data Mining algorithms to characterize the e-banking phishing website factors and to investigate its techniques by classifying there phishing types and defining six e-banking phishing website attack criteria's with a layer structure. The proposed e-banking phishing website model showed the significant importance of the phishing website two criteria's (URL & Domain Identity) and (Security & Encryption) in the final phishing detection rate result, taking into consideration its characteristic association and relationship with each other as showed from the fuzzy data mining classification and association rule algorithms. Our phishing model also showed the insignificant trivial influence of the (Page Style & Content) criteria along with (Social Human Factor) criteria in the phishing detection final rate result.

Haijun Zhang, Gang Liu, Tommy W. S. Chow [15] proposed a textual and visual content based anti-phishing mechanism using Bayesian approach. This framework synthesizes multiple cues, i.e., textual content and visual content, from the given web page and automatically reports a phishing web page by using a text classifier, an image classifier, and a data fusion process of the classifiers. A Bayesian model is proposed to estimate the threshold, which is required in classifiers to determine the class of web page. It also develop a Bayesian approach to integrate the classification results from the textual and visual contents. The main contributions of this paper are threefold. First, it proposes a text classifier using the naïve Bayes rule for phishing detection. Second, it propose a Bayesian approach to estimate the threshold for either the text classifier or the image classifier such that classifiers enable to label a given web page as "phishing" or "normal." Third, a novel Bayesian approach to fuse the classification results from the text classifier and the image classifier is proposed.

"A Novel Anti-Phishing Framework Based on Visual Cryptography"[3] is an anti phishing framework basing on which we have developed our project. In this technique image Captcha is generated and divided into two shares of which one is put with server and other with user. These are later used so that Phishing can be avoided.

There are various mutual authentication methods using cell phones such as browsing using phones, password generation etc.

2.3 Disadvantages of Existing System

By doing a detailed study about the existing system to avoid phishing attack and the related work that has been done in order to overcome the problem of phishing we have observed the following disadvantages.

- In the existing system security level leans.
- It produces security which can be violated by the intruder by various attacks.
- Complexity in maintaining the tables for user id's and respective passwords.
- It may undergo the online attacks like phishing by intruder.
- Not only leading to online attacks there might be a chance of misleading the user with false authentication by phishing websites.
- If the confidential information of the user are attacked and known by the intruder it results in lots of loss to the user both financially and personally too.

Hence, we are proposing a new methodology to overcome the issue of Phishing. We are using a concept of Visual Cryptography to implement our idea.

2.4 Proposed System

In this approach, we propose multilevel authentication using graphical passwords. In this proposed system we are dealing with the authentication using visual cryptography. This methodology is based on the Anti-Phishing image Captcha validation scheme using visual cryptography. It provides password and other confidential information from phishing websites. The approach contains two phases which are *registration phase* and *login phase.*

In the registration phase a key string is asked from the user at the time of registration for the secure website. The string is concatenated with randomly generated string in the server and an image Captcha is generated. The image is dissolved into two shares such that one share is kept with the user and the other is kept in the server. The image Captcha is also stored in the actual database of any confidential website as confidential data. After registration user might change key string.

When the user logs in by entering his username then the user is asked to enter his share. The 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 end user is required to enter the displayed after checking it whether it matches with the Captcha at the time of registration. By this the mutual authentication is established.

Advantages of Proposed System

- It provides multilevel authentication which increases the security level.
- It provides the mutual authentication in which both user and the website are legitimate.
- It takes advantage of overcoming the problem of phishing attack.
- It boosts the user's confidence in using the online transactions.
- It is an anti-phishing visual cryptographic approach.

III. IMPLEMENTATION

Assumptions

The following assumptions were made while developing our project.

- Captcha is a combination of alphabet and numerals. No special characters are used for generation of Captcha.
- User must enter a key which includes alphabet and numerals only and it's length should be more than four.
- Captcha is of length five.
- For generating Captcha we have taken the first, third and fifth characters from K1.
- For generating K2, two random numbers are generated on the server side using random number generator function in JAVA.
- For generating key, the first, third and fifth characters are the ones taken from K2, second and fourth characters are taken from K2.
- This key is given as input to Imgjoin.java class which we have developed.
- This imgjoin.java class takes corresponding images of alphabet and numbers from database and joins them accordingly to form an image Captcha.

3.1Registration Phase

In registration phase, initially user is asked to enter his username and then a key (K1) which can be a combination of alphabet and numerals. After this, a key (K2) is randomly generated by server. Using these two keys a string is formed and this string is then used to form an image Captcha.

For Captcha generation, images of every alphanumeric character with some distortions are stored in database. Then, the string that has been generated with user key and server key is given as input to the code which retrieves all the images of the corresponding alphanumeric characters in the string and then joins them to form a Captcha.

If user is satisfied with this Captcha, he is then asked to enter a password. The concept of image processing and visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. In Visual Cryptography an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined.

In (2, 2) Visual Cryptographic Scheme, an image is divided into two shares and combination of these two shares reveals the original image. Then, this Captcha is dissolved into two shares using (2, 2) Visual Cryptographic Scheme namely share1 (S1) and share2 (S2). Share1 is then sent to user and share2 is updated in database along with username, Captcha and password. These credentials are later used to authenticate user as well as server during login.

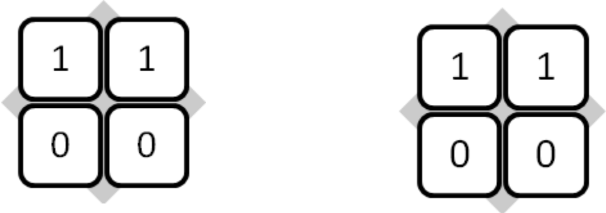
Generation of Shares

(2, 2) Visual Cryptographic Scheme is used. In this method, each pixel is divided into four sub pixels thus increasing the size of shares by four times to that of the original image Captcha.

Here, we are using binary image Captcha. So we obtain the pixel values of each and every pixel in the image Captcha. If the pixel is white, then we use identity matrices and if the pixel is black we use complementary matrices to fill up the four pixels in the shares S1 and S2 corresponding to the pixel in original Captcha where each 2X2 matrix contains two 1s and two 0s in random order.

For example, '1' represents 'white' and '0' represents 'black'.

If the pixel value is 1, then the share can be

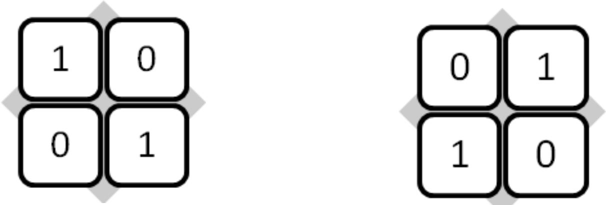


1	1
0	0

1	1
0	0

Figure 5 Pixel values for Share if pixel value is 1

If the pixel value is 0, then the share can be



1	0
0	1

0	1
1	0

Figure 6 Pixel values for Share if pixel value is 0

In this way all the pixels are divided into four sub pixels and thus shares are generated.

The values of the matrices are given so because while reconstruction if the pixel value in both the shares is same they are assigned the same value in reconstructed image. If the pixel value in both shares is different, then 0 is assigned making it complete black.

So, if the original pixel is white in original image, in reconstructed image we get half black and half white pixels which provides a greyish look, else if the original pixel is black in original image, in reconstructed image we get complete black pixel.

3.1.1 Login Phase

In Login phase, user enters his username and uploads his share i.e. (S1). Then, the (S2) corresponding to the username that is stored in database is retrieved and these two shares are combined using the (2, 2) Visual Cryptographic Scheme to form the Captcha.

Now, if the server is not genuine, then it does not possess the share2 of the user, so the Captcha that was generated during registration cannot be regenerated and thus the server is authenticated.

At the same time, user is also authenticated by the server because only legitimate user possesses the share1 of his. This is first level of authentication.

But there is a chance of sharing his PC or Laptop with his acquaintances and as he stores his share in his PC or Laptop there is a chance of his acquaintances or even people whoever use his laptop logging into his account.

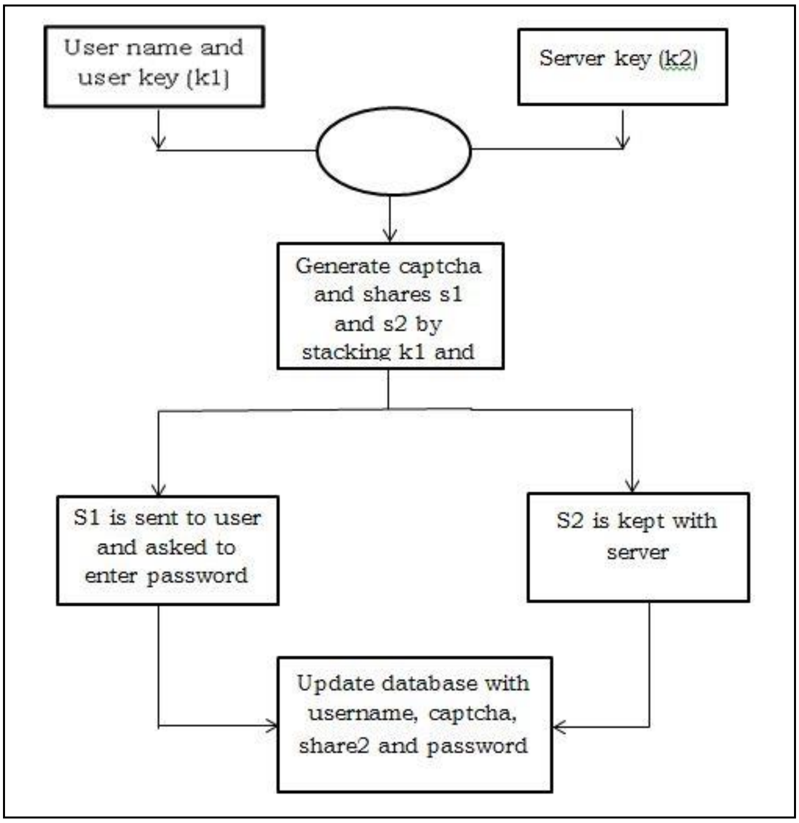

User name and user key (k1)
Server key (k2)
Generate captcha and shares s1 and s2 by stacking k1 and
S1 is sent to user and asked to enter password
S2 is kept with server
Update database with username, captcha, share2 and password

Figure 7 Registration Phase

To avoid this problem, we are using another level of authentication. Here, user after verifying the regenerated Captcha, if he finds it to be the same that was generated during registration phase, he then enters the Captcha as well as password in order to login. If regenerated Captcha does not match with that was generated during login phase user identifies the website as phishing website.

Then, if both Captcha and password are checked against the password and Captcha that are stored in the database, if they match user is allowed else rejected.

Second level of authentication ensures that the person logging in is legitimate user of the account by asking him to enter the password in addition to share1.

In this way both user and server are authenticated and thus the technique helps in ensuring the safety of the sensitive information of innocent people by preventing phishing attack.

3.2 Advantages of Proposed Methodology

This method helps in enabling even a not so well aware user in detecting the Phishing website and hence secures his personal and sensitive information from being gathered by others.

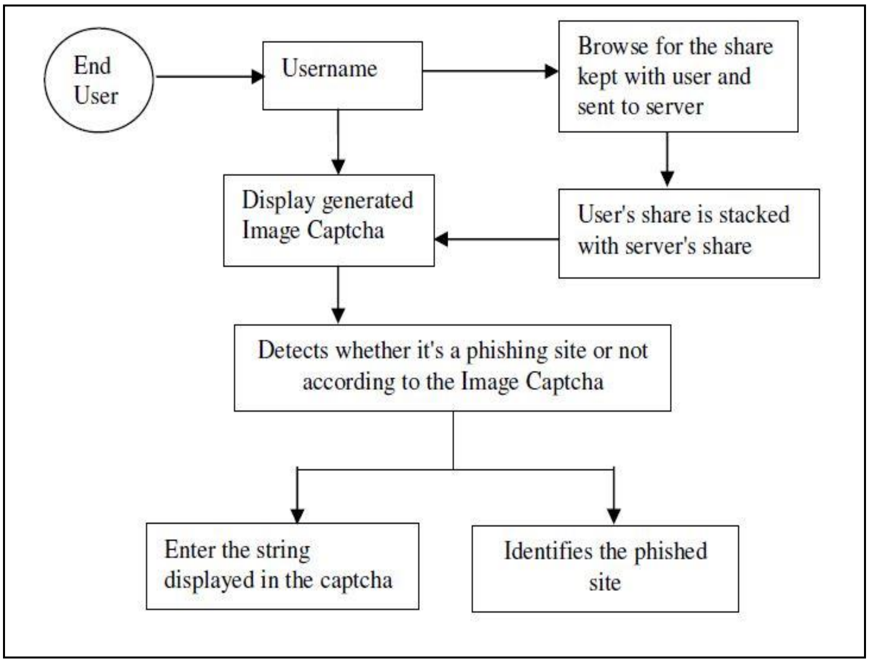
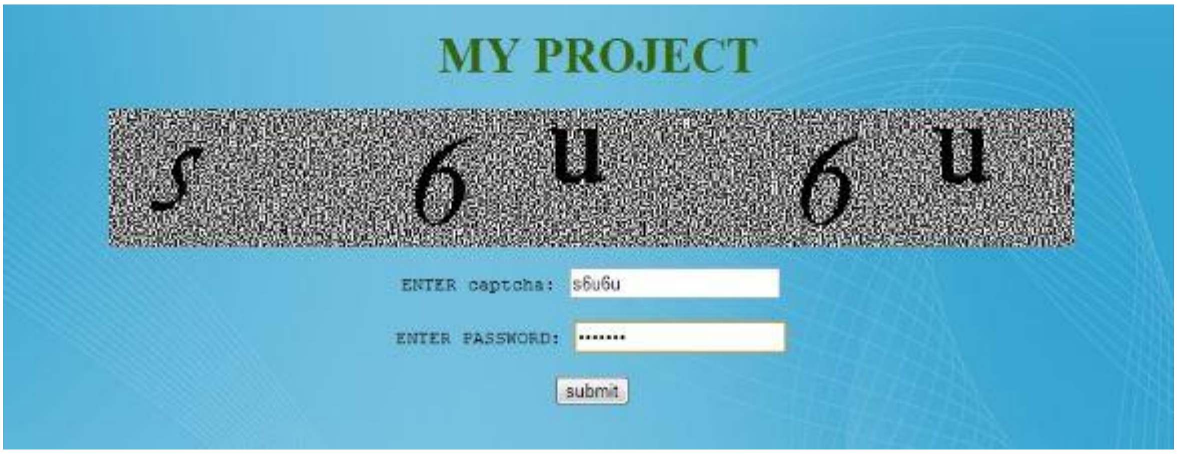

End User
Username
Browse for the share kept with user and sent to server
Display generated Image Captcha
User's share is stacked with server's share
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the captcha
Identifies the phished site

Figure 8 Login Phase

IV. RESULTS

The below screen shows the user his Captcha by taking his share and server's share and regenerating it. The screen also asks user to enter his password in order to authenticate him.



MY PROJECT

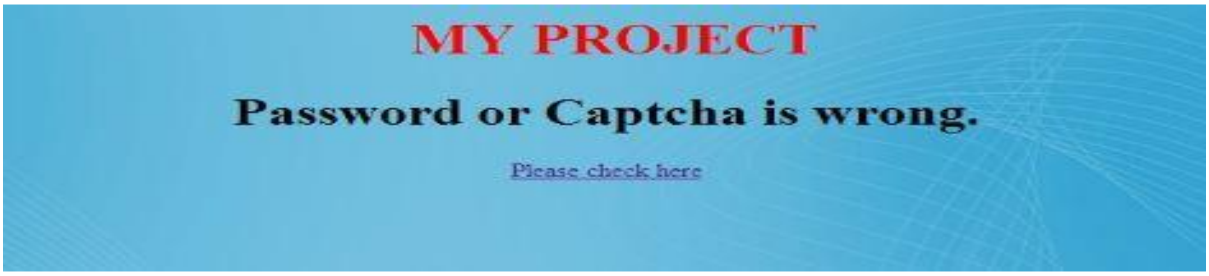
s 6 u 6 u

ENTER captcha: s6u6u

ENTER PASSWORD: •••••••

submit

Figure 9 Screen showing the reconstructed Captcha to the user during login



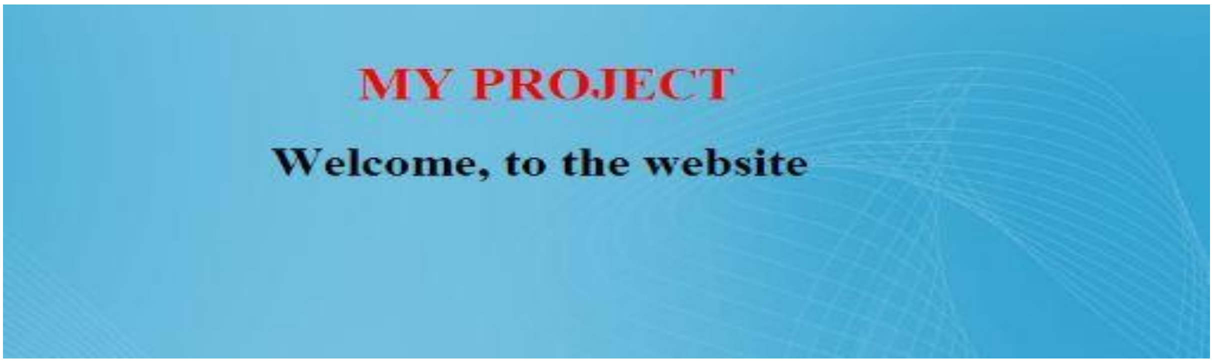
MY PROJECT

Password or Captcha is wrong.

Please check here

Figure 10 Screen Showing Login Failure

This screen shows the message saying either of user's password or Captcha has been wrongly entered after checking them against the ones that were stored in database.

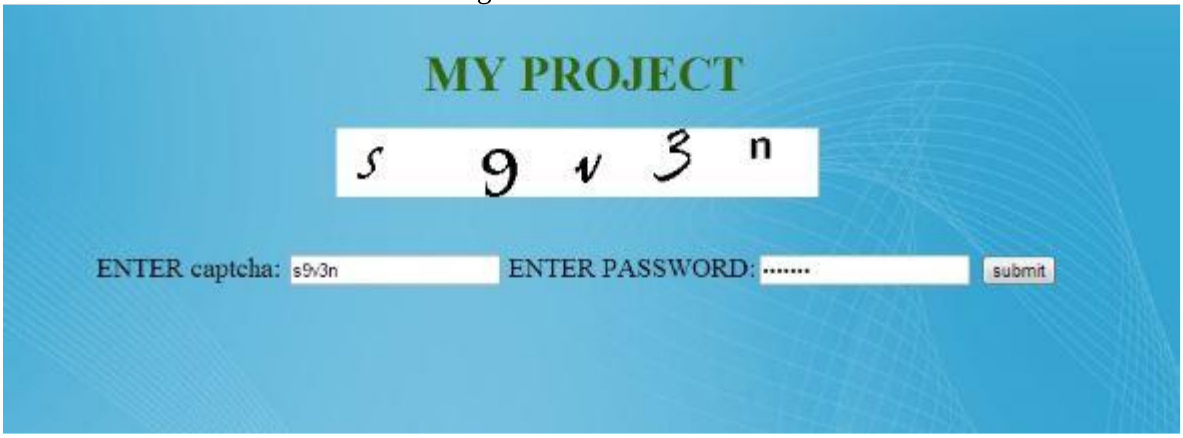


MY PROJECT

Welcome, to the website

Figure 11 Screen Showing the Successful Login of a User

The above screen shows successful login of the user.



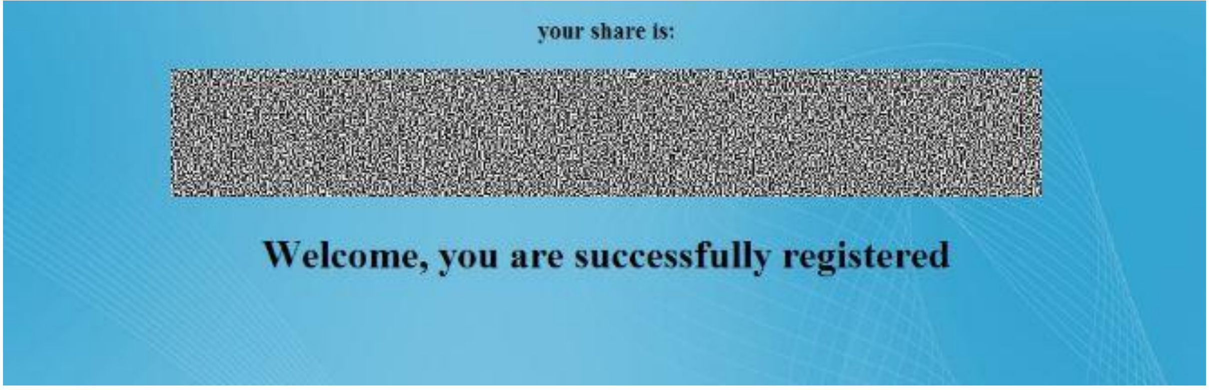
MY PROJECT

s 9 v 3 n

ENTER captcha: s9v3n ENTER PASSWORD: •••••••

Figure 12 Screen Showing Generated Captcha to User

This figure shows the generated Captcha from user and server keys and requesting user to enter his password for successful registration.



your share is:

Welcome, you are successfully registered

Figure 13 Screen Showing Successful Registration Message

This figure shows the screen showing user his share and a success message on his successful registration.

V. CONCLUSIONS

In this paper, we have proposed Multi-level Authentication using graphical passwords, which is a generalization to improve the security from online attacks . The main attack which we can overcome by this approach is phishing. This approach overcomes the false sensations causing by the phishing websites. This resembles password authentication but not exactly the same. In this approach we are achieving mutual authentication in which both the user and the website are authenticated. So the user can be free from the tension of phishing websites and the server can be free from mal-users. In this approach even if the intruder gets the password he can't do anything because of the share which will be generated during the registration phase. So we can conclude that this approach is quite better than other approaches. We analyze the performance of this approach of multi-level authentication basing on some metrics including the success rate, response time and efficiency. The result of this approach is well and quite good. When combined with any other authentication techniques its performance could be further improved.

VI. FUTURE SCOPE

We had made an attempt to overcome the problem of phishing. In this approach we included multi-level authentication which includes the registration phase and login phase. The shares which are generated are the main and plays a crucial role in this approach. In this multi-level Authentication scheme we improved the level of security. We have included the black and white images in our approach. Further it can be implemented by using colour images also. This approach can be extended by including the security question to improve the security level. The Captcha dissolving can be used in any other effective way to overcome the mischievous things by the intruders. And problem of pixel expansion in VCS can also be reduced using any other algorithms to increase efficiency.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors wish to thank many anonymous referees for their suggestions to improve this paper. The authors would like to thank all the authors mentioned in the reference section and everyone who helped in this work.

REFERENCES

[1] Wen-Pinn Fang,"Non-expansion Visual Secret Sharing in Reversible Style", IJCSNS, VOL.9 No.2, February 2009.

[2] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[3] Divya James and Mintu Philip, "A Novel Anti Phishing Framework Based on Visual Cryptography", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[4] Wen-Pinn Fang, "Visual Cryptography in reversible style,"IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007, 11, 26～2007, 11, 28.

[5] Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method"', in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.

[6] Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedingsof IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010

[7] Sid Stamm, Zulfikar Ramzan, "Drive-By Pharming", v4861 LNCS, p495-506, 2007, Information and Communications Security - 9th International Conference, ICICS 2007, Proceedings.

[8] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)", IEEE Transactions on Dependable and Secure Computing, v3, n4, p301-311, October/December 2006.

[9] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Antiphishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v10, n2, p 58-65, March/April 2006.

[10] JungMin Kang, DoHoon Lee, "Advanced White List Approach for Preventing Access to Phishing Sites", 2007 International Conference on Convergence Information Technology, ICCIT 2007, p 491-496, 2007

[11] Nirmal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'", in Proceedings of IEEE- International Conference on Emerging Trends in Robotics and Communication Technologies, 2010.

[12] Tianyang Li.; Fuye Han.; Shuai Ding and Zhen Chen.; "LARX: Large- scale Anti-phishing by Retrospective Data-Exploring Based on a Cloud Computing Platform", in Proceedings of IEEE- 20th International Conference on Computer Communications and Networks, 2011.

[13] Qingxiang Feng.; Kuo-Kun Tseng.; Jeng-Shyang Pan.; Peng Cheng and Charles Chen.; "New Antiphishing Method with Two Types of Passwords in OpenID System", in Proceedings of IEEE Fifth International Conference on Genetic and Evolutionary Computing, 2011

[14] Maher Aburrous .; M. A. Hossain.; Keshav Dahal.; "Modelling Intelligent Phishing Detection System for e-Banking using Fuzzy Data Mining", in Proceedings of IEEE Conference on CyberWorlds, 2009.

[15] Haijun Zhang , Gang Liu, and Tommy W. S. Chow, “Textual and Visual Content Based Anti-Phishing: A Bayesian Approach,” IEEE Trans. Neural Netw., vol. 22, no. 10, pp. 1532–1546, Oct. 2011.

AUTHORS

P.S.V Vachaspati is currently working as Assistant Professor in Dept. of C S E in Bapatla Engineering. He has 3 papers published in various International journals and conferences. His research areas include Security & Cryptography, Neural Networks.

A. S. N. Chakravarthy did his Master’s Degree from JNTU Hyderabad and PhD from Acharya Nagarjuna University, Guntur. He is currently working as Associate Professor in Dept. of C S E in JNTUK University College of Engineering Vizianagaram. He has 37 papers published in various International journals and conferences. He is Reviewer and Editorial board member for various international journals. His research areas include Cryptography, Biometrics, and Digital Forensics.

P. S. Avadhani did his Master’s Degree and PhD from IIT, Kanpur. He is presently working as Professor in Dept. of Computer Science and Systems Engineering in Andhra University college of Engg., in Visakhapatnam. He has more than 50 papers published in various National / International journals and conferences. His research areas include Cryptography, Data Security, Algorithms, and Computer Graphics.