International Conference - Innovation-2021-Innovation-2021
International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN : 2456-3307 (www.ijsrcseit.com)
Volume 8, Issue 3, May-June-2021

Prevention of Phishing Attacks on Online Voting System Using Visual Cryptography

Akshada Tingare[1], Pragati Shilote[1], Mohoni Raykar[1], Priyanka Pathare[1], Prof. Vandana Chavan[2]

[1]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Pune, Maharashtra, India

[2]Assistant Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Pune, Maharashtra, India

ABSTRACT

The aim of Voting System using Visual Cryptography is to provide facility to cast for critical and confidential decisions of internal corporate. It provides the flexibility of casting vote from any remote place. The confidentiality of the election is maintained by applying the appropriate security measures so that the voter can vote for any participating candidate but only if he logs into the system by entering the correct password which is generated by merging the two shares using Visual Cryptography scheme. The administrator is responsible for sending the shares, 1st share to voter email id before election and 2nd share will be available in the Voting System for his login during election. The voters get the secret password to cast his vote by the combination of share 1 and share 2 using Voting Cryptography. Phishing is an attempt by an individual or group which aims to get personal confidential information from unsuspecting victims. Internet voting focuses on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement and observation of the process.

Keywords : Authentication, Visual Cryptography, Image captcha phishing, Phishing, Open CV Library Algorithm, Online Voting.

I. INTRODUCTION

Due to rapid increase in the internet usage, sharing of information on the internet has started, however they are unaware that the network on it they are sharing files is secure or not. Thus, data security becomes a very serious issue these days [9]. Phishing is identified as a significant security threat known is phishing [12-13] every moment a new technique for doing fraud is being increased. Thus, the security in these cases should be elevated and should not be manageable with implementation. Now a days, most applications are safe with their underlying system. Phishing is identified as fraud that steals identification and personal data of people [10]. many information security techniques have been developed to protect information from hackers that includes Steganography, Cryptography and other encryption techniques. Steganography techniques is applied on any style of digital media like text, video, audio or footage. Visual cryptography and Secret Image Sharing are cryptography techniques that are used for materials, matter footage, and written

notes etc. website address of ABC Corporation but it doesn't take us to the legalized site. [11] In the existing system of phishing detection there is also an approach where the visual cryptography is used. In this approach when the user first registers at the bank server, then at the time of registration itself an image is chosen that's split into two shares. One share of image is kept at the server and user gets another share that he keeps with him. When the user wants to initiate transaction with merchant server, he sends his UID code to the merchant server. Merchant server then sends his sys Id & password along with the user's UID to the bank server. once bank server gets this request he initial verifies if the merchantserver is registered merchant. If so, he fetches the share of image associated with the precise UID code and sends it to the merchant server which then sends it to the user. once user gets the share of image, he combines it along with his share. If user gets the primary image that was selected at the time of registration, then he gets to know that the merchant is authenticated, and the user can now proceed the transaction. One-time passwords are passwords that are used once and only valid for one login session or transactions. Banks, governments and security-based industries deploying OTP system where user might have many passwords and use each password just once. OTPs can avoid number of shortcomings that are associated with traditional passwords that are valid for many transactions as users are reluctant to voluntarily change passwords frequently. Since OTPs are only valid for single use, an attacker has a smaller window of time to gain access to resources guarded by such an identification as a result of any previously taken passwords will most likely became invalid [11].

II. SECURITY ATTACKS

A. IP Spoofing Attacks

The basic protocol for sending data over the web network and many other computer networks is the Internet Protocol (IP). The first goal of an IP spoofing attack is to determine a connection that allows the attacker to gain root access to the host and to make a backdoor entry path into the target system. IP spoofing could be a technique used to gain unauthorized access to computers whereby the intruder sends messages to a computer with an IP address that indicates the message is coming from a trusted host. The attacker learns the IP address of a trusted host and modifies the packet headers so that it appears that the packets are coming from that trusty host. In computer networking, IP address spoofing or IP spoofing is that the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of impersonating another computing systems.

B. Trust exploitation

It refers to an individual taking advantage of a trust relationship inside a network. The goal of a trust exploitation attacker is to compromise a trusty host, using it to stage attacks on other hosts in a network. If a host in a network of a company is protected by a firewall (inside host), but is accessible to a trusty host outside the firewall (outside host), the inside host are often attacked through the trusted outside host.

C. Password Attacks

Types of Password Attacks:

1. Non-electronic Accounts

It is a non-technical attack that is the performed even without sound technical knowledge.

2. Active Online Attack Types:

a. Password guessing: Attackers create possible passwords by collecting information from social media accounts and other online sources.

Criminals use the default password provided by manufacturers to crack accounts.

b. Brute-force attacks: Attackers make multiple attempts with possible combinations until they crack the account.
c. Dictionary attacks: Attackers load dictionary files of passwords and runs it against user attacks.
d. Rule based attack: Attackers load dictionary files of passwords and runs it against user attacks.
e. Trojan/Keylogger/ Spyware: Either of these viruses or malware are run in the background to track the passwords.
f. Hash injection attack: The attacker injects a compromised hash into a local session and uses it to retrieve the domain admin account hash. To log on to the domain controller, use the extracted hash.

3. Passive Online Attack:

a. Man-in-the-middle: The attacker gains access to the communication channel to extract confidential information.
b. Wire-sniffing: Packet sniffer tools on the local area network are used to access and track the network traffic.
c. Replay attack: Packets and authentication captured using a sniffer are used to extract relevant information, and then they are placed on the network to gain access.

4. Offline Attack:

a. Rainbow table: Captured password hashes are compared to the precomputed tables to recover passwords.
b. Distributed network attack: The technique is used to recover passwords from hashes using excess power of machines to decrypt passwords.

D. Confidentiality and Integrity Attacks:

Confidentiality breaches can occur once an attacker attempts or tries to get access to read-sensitive information. These attacks can be very difficult to detect because the attacker can copy sensitive information without the knowledge of the owner and without leaving a trace. A confidentiality breach can occur just because of incorrect file protections. as an example, a sensitive file could mistakenly be given global read access. Unauthorized copying or examination of the file would probably be difficult to track without having some type of audit mechanism running that logs every file operation. If a user had no reason to suspect unwanted access, however, the audit file would in all probability ne'er be examined.

E. Phishing, Pharming and Identity theft

Two of the most common ways in which thieves acquire personal data to help them in identity theft are phishing and pharming. Phishing utilizes bulk e-mail messages to entice recipients into revealing personal data. Pharmers, on the opposite hand, cast a wide net for the unwary.

Identity theft continues to be a problem. In computing, phishing is an endeavour to criminally acquire sensitive information, such as usernames, passwords, and card details, by masquerading as a trustworthy entity. Phishing is usually carried out by email or instant message (IM), although typically phone contact is attempted; the phisher usually directs users to enter details at a web site. Phishing is an associate degree example of social engineering. Pharming is an attack aimed at redirecting the traffic of a website to another website. Pharming is conducted either by ever changing the hosts file on a victim computer or by exploiting a vulnerable Name System (DNS) server. Pharming has become a significant concern to businesses hosting e- commerce and on-line banking websites.

F. Accessibility Attacks

Availability means that information is accessible by authorized users. If an attacker is not able to compromise the first two elements of information security (see above) they may try to execute attacks like denial of service that would bring down the server, making the website unavailable to legitimate users due to lack of availability. DoS attacks attempt to compromise the availability of a network, host, or application. They are considered a major risk because they can easily interrupt a business process and cause significant loss. These attacks are relatively simple to conduct, even by an unskilled attacker. Botnet is a term for a collection of software robots, or bots, that run autonomously and automatically. They run on groups of "zombie" computers controlled by crackers. Among the different kinds of threats, there is the possibility of occurrence of phishing in voting systems [4],and the social phishing scams have to be avoided or otherwise their effects can be easily wide spread in an election process.

The geography of phishing attacks in first quarter of 2015 is given in figure 1 [5].

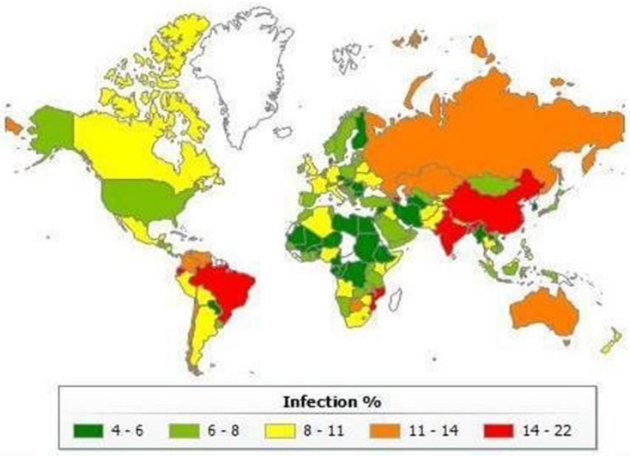

Fig 1. Literature Survey

III. LITERATURE SURVEY

Comparative study of classifiers model-based features is shown in the table 1

Table 1: Analysis of literature survey

COMPARATIVE ANALYSIS OF LITERATURE SURVEY

Sr. No.	Paper Name	Methodology	Result
1	The Phishing Guide Understanding & Preventing Phishing Attacks	multi-tiered approach(client-side, server-side and enterprise)	66.45%
2	Visual Cryptography	Visual Cryptography(basic)	72.55%
3	Segment-based Visual Cryptography	Visual Cryptography using seven segment display	77.75%
4	CAPTCHA: Using Hard AI Problems For Security	AI problems (Stegnography)	85.30%
5	A Text-Graphics Character CAPTCHA for Password Authentication	Text-Graphics Character Captcha	89.54%
6	Hashed Based Visual Cryptography Scheme For Image Authentication	Visual cryptography	90.15%
7	Visual Cryptography and Chaotic Image Encryption for the Security Of Biometric System	Visual cryptography	91.13%
8	Image Authentication using Visual Cryptography and Encryption algorithm	RSA algorithm & Visual cryptography	94.20%

Table 1. Comparative Analysis

IV. VISUAL CRYPTOGRAPHY FOR ANTI-PHISHING

Recently Phishing is most popular attack. Phishing is a form of online identity theft that aims to steal the sensitive information. Phishing is done to acquire confidential information such as Usernames, passwords, and card details by disguising as a legitimate entity in an electronic communication. In this paper we have introduced a new method, which can be used as a safe way against phishing, which is named as "Visual cryptography for Anti-phishing". In that approach website cross verifies its own identity to the end users and it make a system is secure and authenticated as well. In this technique we used the concept of image processing and an improved visual cryptography. Visual Cryptography (VC) is a method of encrypting a secret image into the shares, such that

after stacking a sufficient number of shares the secret image is disclosed in that method an image- based authentication is performed using Visual Cryptography (VC).

The image captcha is decomposed into 2 shares that are stored in separate database servers, one with user and one with server such that the original image captcha is revealed only when that two shares are simultaneously stacked. Once the original image captcha is disclosed, the user can use it as the password.

V. EVOLUTION OF VOTING SYSTEMS

There are different types of voting systems starting from the early days and upto the current technological trends. These are explained in the following section.

A. Paper ballot system

Paper ballot system is the most commonly used method in voting system. The system was widely used before the invention of electronic voting system. Paper ballot system uses paper and stamp method to cast a vote. Every voter makes use of one ballot and it is not shared. The disadvantages in this system are:

i) time consuming,
ii) booth capture,
iii) low count speed.

B. Electronic voting system

An electronic voting system is a type of voting system which allows voters to cast their confidential votes using Internet. The disadvantages in this system are:

i) People poor in computer knowledge face difficulty in voting,
ii) security problems,
iii) cost.

C. Online voting system

Online voting system is the most recent used electronic voting system in which the voted ballot is transmitted over the public Internet through web from anywhere in the world. Security is the most important drawback of this system [7].

Some major issues related to online voting system based on security are:

- Most of the applications are giving high security towards the Password Security and they are not focusing on phishing attacks. By phishing, attackers get the passwords from the client and they go into the relevant sites with right secret key.
- There is no efficient method to safeguard the websites from the phisher attacks. Other than the given voting systems the voter can use other voting methods to cast their votes.

VI. PROPOSED ONLINE VOTING SYSTEM

Taking an online voting system into consideration to elect the president or any other government authorities. Detection and prevention of Phishing attacks can be done using the technique as described in figure 2.

When government is going to held elections the election officer or administrator uses online voting system to cast vote. During this process people who are eligible to cast vote has to upload the password image, it has to move from local system to web server. Then the password image is divided into two shares, this system proposed the Visual Cryptography technique. Before dividing the image into two shares the image is first converted into Monochrome Image (Black and White Image).

Given a secret image S to the user, a set P of n participants and a strong access structure, a Visual Cryptographic Scheme (VCS) for General Access Structures (GVCS) encodes S into n shares of transparencies. Modeling of minimizing the pixel expansion for a (k, n)-VCS into an integer linear program (ILP), to ensure that the constraints for GVCS can be satisfied. The pixel expansion of a GVCS can thus be minimized by solving the corresponding ILP.

The proposed ILP is generalized for (k,n)-VCS. It can be applied to construct the basis matrices with the minimum pixel for a GVCS. The optimal pixel expansion of a GVCS can be acquired, especially for those applications that really need a GVCS with the smallest shares. After Image is divided into two shares one share has to be sent to the relevant voter through email, for which SMTP technique is used [8].

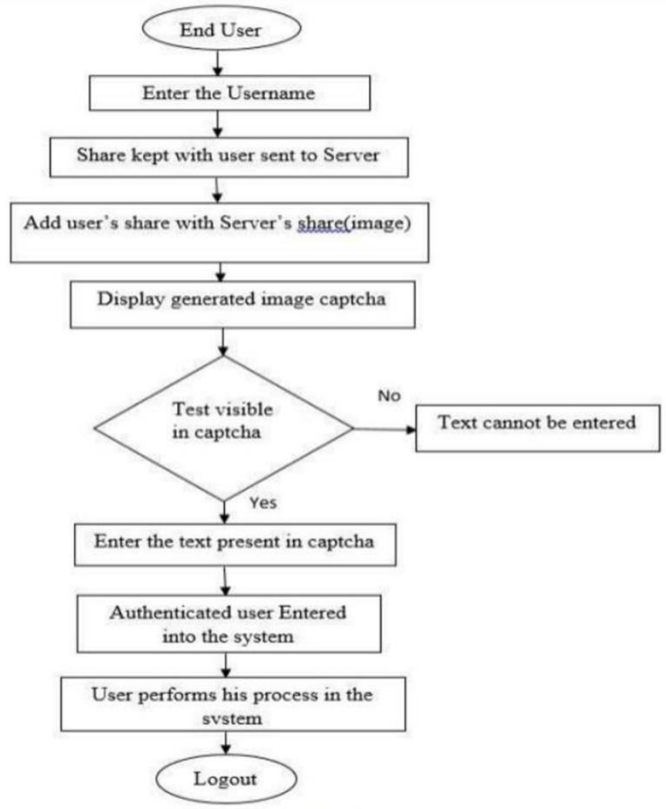

Figure 1. Proposed Online Voting System

Fig 2. Proposed Online System

The image of text captcha is split into two shares namely share1 and share 2. From Figure 3, we can easily identify three different forms of input and output. Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. In case1 and case2, it is shown that correct images are formed and the captcha can be reconstructed properly whereas in case3, different shares are used and hence the captcha cannot be generated properly. After entering the captcha, user is allowed to cast his vote. In case 3, the two shares are different and thus the output is not the proper image captcha. Hence user cannot be able to enter the captcha and thus the user is logged out of the system.

For Online Voting system there are many powerful validations to make the voting successful. Some of them are:

- Once voter has casted his vote , he is not able to vote again This can be accomplished by making his password to be expired.
- Whenever the voter did his voting, the corresponding voting count of that candidate has to be increased.
- Proper authentication is been provided so that the voters will not have unambiguous regarding the security of voting using online voting system. This can be achieved by the combined usage of visual cryptography and anti-phishing process.

VII. PROPOSED ALGORITHM

Algorithm for image comparison:

OpenCV library of Java:

To compare two images –

1. Read Both of them using the Image.IO.read() method
2. Get the height and width of both of them to make sure they are equal.
3. Get the pixel values and, get the RGB values of both of the images.
4. Get the sum of the differences between the RGB values of these two images.
5. Calculate the percentage of the difference using the following formula – Average = difference /

weight * height * 3; Percentage = (Average / 255) * 100

Algorithm:

Step 1 - Check if dimensions of both the image match.
Step 2 - Get the RGB values of both images.
Step 3 - Calculate the difference in two corresponding pixels of three-color components.
Step 4 - Repeat Step 2-3 for each pixel of the images.
Step 5 - Calculate the percentage by dividing the sum of differences with:

Number of pixels, to obtain the average difference per pixel 3, to obtain the average difference per color component 255, to obtain a value between 0.0 and 1.0 which can be converted into a percent value Compare two Images using Open CV Library in Java.

VIII. ADVANTAGES

1. The system which uses visual cryptography enhances the security level of the system.
2. User login is safe and secure. Voters can vote from any place.
3. Voter can login in to the account only if he/she has successfully uploaded the image share which is provided on their email.
4. This system will cause voter to cast vote only once.
5. If will be efficient for voters living in remote locations.

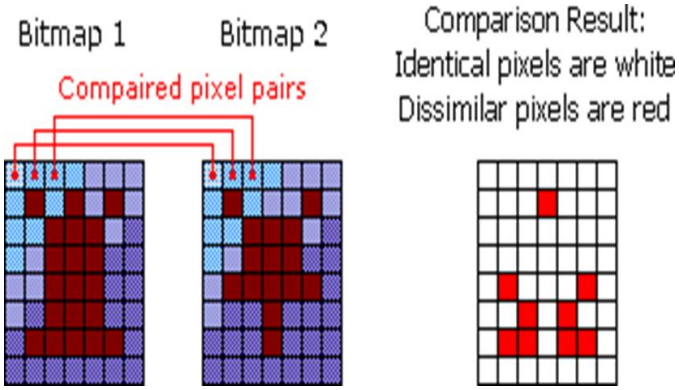

Fig 3. Comparison of Images

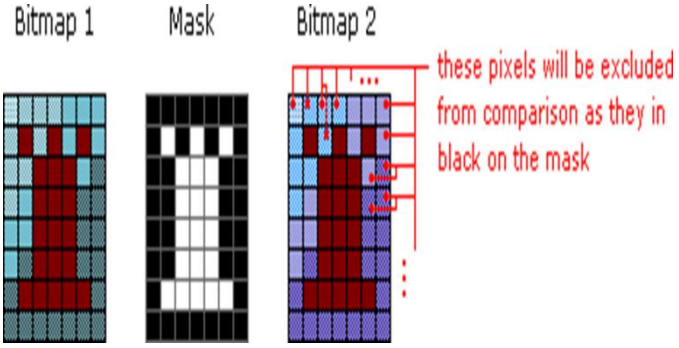

Fig 4. Pixel matching

IX. IMPLEMENTATION

1. User Registration in system

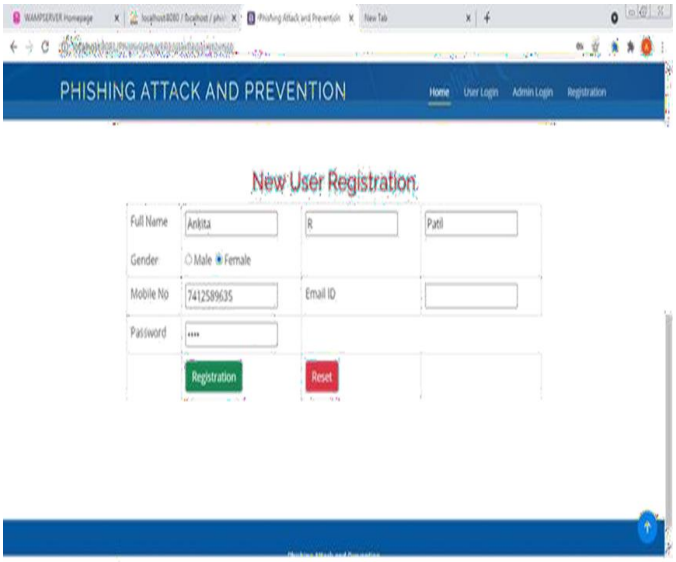

Fig 5 Registration

2. Sending Image share through mail

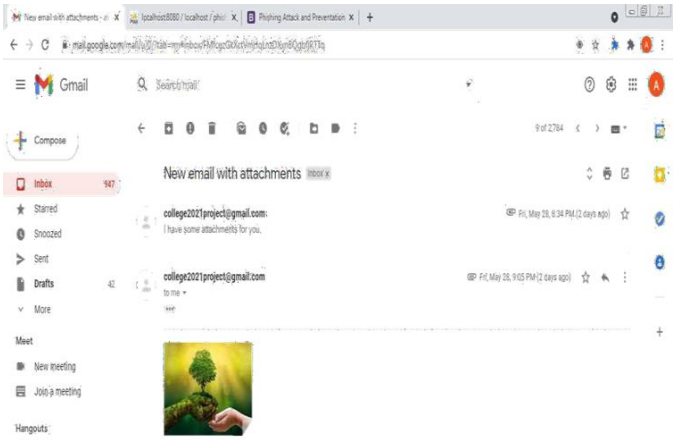

Fig 6. Image process

3. Detection of Phishing attack

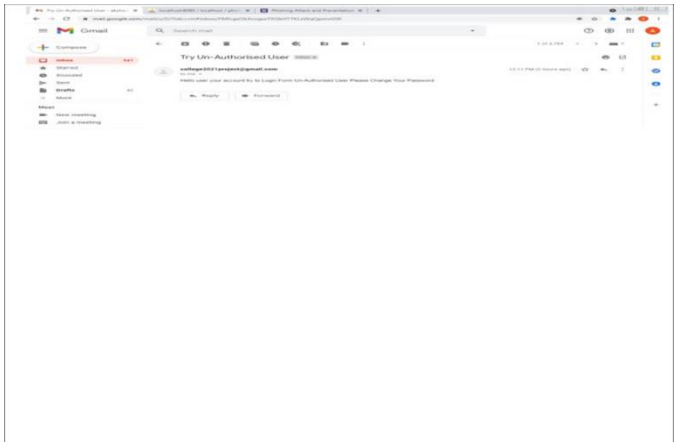

Fig 7. Detection of attack

4. Voting System

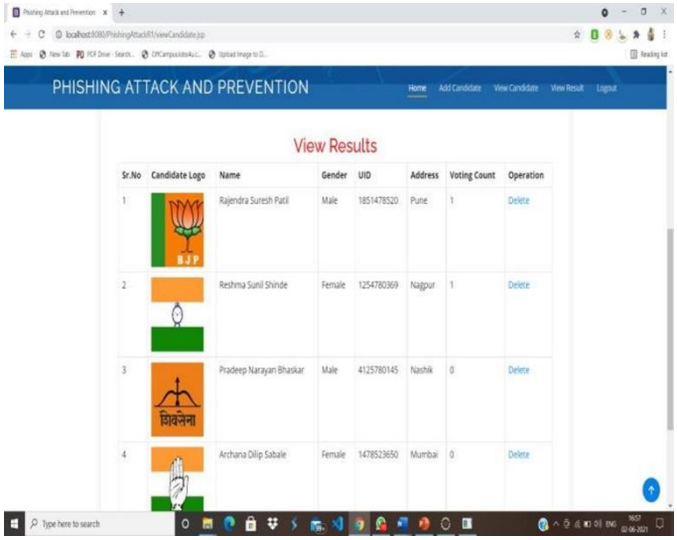

Fig 8. Voting process

5. Prevention using visual cryptography

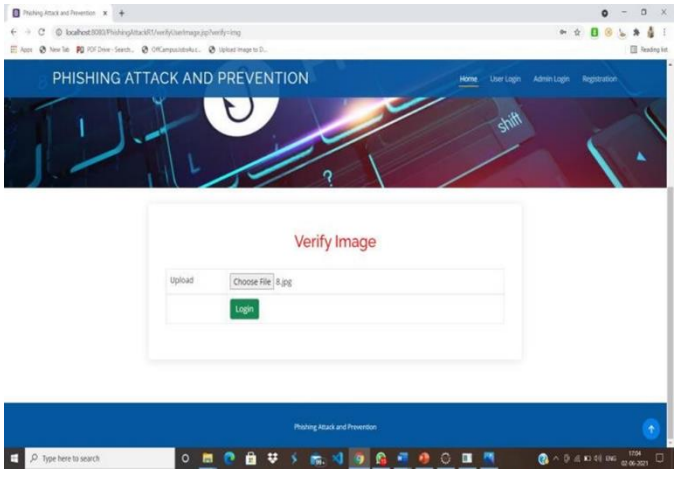

Fig 9. Prevention of attack

X. CONCLUSION

At present generation attacks are more in online systems, phishing has become major network security issue, leading many losses by hacking the confidential data that are used by the user. Phishers creates their own fake websites which is exactly similar to the original website including applying DNS server name, setting up web server and creating web pages similar to genuine website. So in this paper we are going to design link guard algorithm which is a character based. It has capacity to detect many attacks using APWG (anti phishing working group).Open CV Library is used for prevention of phishing attacks . Proposed online voting system will be very effective and it will be useful for voters and organization in number of ways and it will reduce the cost and time of voters and organization both.

XI. REFERENCES

[1]. NetworkSecurity, https://en.wikipedia.org/wiki/Network_security, accessed on May 2015.

[2]. JoeyPaquet, http://users.encs.concordia.ca/~paquet/wiki/index.php?title=Capability_maturity_model, accessed on May 2015.

[3]. Villafiorita A, Weldermariam K, Tiella R, “Development, Formal verification and evaluation of an e-voting system with VVPAT”, IEEE Transactions on Information Forensics and Security, 2009, p.no. 651- 661.

[4]. Abdalla Al-Ameen and Samani Talab, “The Technical Feasibility and Security of E-Voting”, The International Arab Journal of Information Technology, Vol.10, No.4, July 2013, p.no.397-404.

[5]. https://securelist.com/analysis/quarterly-spam-reports/69932/spam-andphishing-in-the-first-quarter-of-2015/, Phishing attack, accessed on 12.09.2015.

[6]. M. Mounika Reddy and B.Madhura Vani, "A Novel Anti phishing Framework based on Visual Cryptography", International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, Issue 9, Sep 2013, P.No.3434-3436.

[7]. Mayur Patil, Vijay Pimplodkar, Anuja R.Zade, Vinit Vibhute, Ratnakar Ghadge, "A Survey on Voting system techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 1, Jan 2013, p.no. 114-117.

[8]. Shyong Jian Shyu, Ming Chiang Chen, "Minimizing Pixel expansion in Visual cryptographic scheme for General Access Structures", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 25, No. 9, Sep 2015.

[9]. Liang H., & Xue Y., "Understanding security behaviours in personal computer usage: A threat avoidance perspective", Association for Information Systems, 11(7), pp. 394–413, 2010

[10]. Ollmann G. The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[11]. Anti-Phishing Working Group, Global Phishing Survey: Trends and Domain name use in 1H2009, 2009Anti-Phishing Working group .http://www.antiphishing.org/.

[12]. Yuancheng Lia et al., "A semi-supervised learning approach for detection of phishing web pages", Optik, (124), pp. 6027– 6033,2013 .

[13]. Nalin Asanka Gamagedara Arachchilage, Steve Love, Security awareness of computer users: A phishing threat avoidance Perspective, Computers in Human Behavior (38), 2014.