

Secure Online Payment System using Visual Cryptography

Nikita Chaudhari¹, Priya Parate²

ME Student, Computer networking and Information Security, RGIT, Mumbai, India¹

Professor, Computer Engineering, RGIT, Mumbai, India²

Abstract: With the commencement of internet E-Commerce is rapidly growing market. Phishing is most popular attack possible in E-commerce environment as Phishing means is the attempt to gain sensitive information of an user such as usernames, passwords, and credit card details, by impersonating as a credible entity in an E-commerce. In this paper we have proposed new approach for secure online payment system using Visual Cryptography. In this Visual cryptography is applied on confidential data such as One-time password from which two shares are generated. One share is send to Client through Email and other is send to Merchant. Merchant in tern send share to Client, So that two-way authentication is done as well as whether the site is Phishing or non-phishing website -is detected.

Keywords: Online Shopping, Phishing, Shares, Visual Cryptography.

I. INTRODUCTION

Online Shopping is also known as electronic retail is form of electronic commerce which allows consumers to directly buy goods or services from a retailer or seller over the Internet using a web browser. Phishing is one of the most important threats in Online Shopping. And it is the attempt to acquire sensitive information such as usernames, passwords, and credit card details, by impersonating as a credible entity in an electronic communications.

In this paper we propose new approach for Secure Online shopping by using Visual Cryptography. Visual Cryptography minimizes the data share between Client and Merchant Server but enabling successful fund transfer without misusing sensitive information of Client or Consumer.

II. VISUAL CRYPTOGRAPHY

Visual Cryptography is Secret Sharing Scheme where it is an encryption technique to hide information in an image in such a way that it can be decrypted by combining two shares. Share is nothing but a random pixel image which gives no information to an attacker about the data. Shares are generated using visual cryptography algorithm. One of the best techniques is Moni Naor and Adi Shamir, which was developed in 1940. Visual Cryptography creates two shares of same image, one image contains random pixel and other image contains secret information.

In this scheme we are considering black and white image having binary resolution i.e. white pixel means 0 and black pixel means 1. We are considering 2*2 matrix for each pixel in an given image. A single pixel will have 2 matrixes. One matrix will be randomly selected and another will be generated according to pixel colour i.e. black or white pixel. We are using (2,2) VCS i.e. two sub pixel for each pixel in the secret message. Figure 1 shows Illustration of (2,2)VCS scheme with 2 sub pixel construction.

Pixel	Probability	Shares #1 #2	Superposition of the two shares	
□	$p = 0.5$	 		White Pixels
	$p = 0.5$	 		
■	$p = 0.5$	 		Black Pixels
	$p = 0.5$	 		

Fig. 1. Illustration of (2,2)VCS scheme with 2 sub pixel construction.

No share leads to an original pixel because every time random pixels are encrypted to create secret image. When the two shares are superimposed with each other, the value of the original pixel can be determined.

III. RELATED WORK

A brief survey related to work in online payment is described in this section. An online payment system using steganography and visual cryptography is presented in [1] but the paper doesn't focus on phishing. There is no way to detect whether the site is Phishing website or Non-Phishing website. The other concept is Captcha and Its techniques for Providing Security in Web and Applications is presented in [2]. Here CAPTCHA that uses video understanding to distinguish between humans and machines but the paper only focus on differentiating humans with machine but not covering all the possible attacks done by humans.

IV. CURRENT METHODOLOGY

In current scenario, There are mainly 3 entities involved namely Customer or Client, Merchant server and Bank Server. The task of Customer or Client is to first make an account at merchant server. Client needs to fill username, password, e-mail address, residential address, credit card

details and other confidential information in order to login to merchant site.

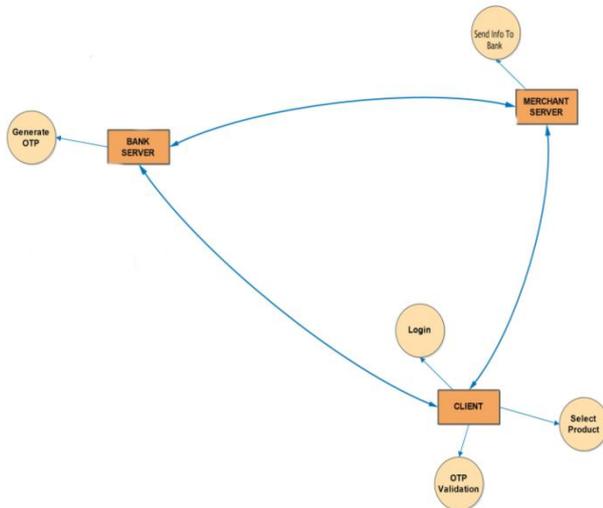


Fig. 2.Current Methodology

After login is successful, Client will select product which he/she wants to purchase. After making a request to purchase a product, Merchant server will send this information to Bank server. In turn Bank server will send OTP to Client in order to authenticate the request raised by Client. At client side OTP is validated and purchase order is placed. This OTP is valid till 10mins.

When Client is logged in, sensitive information such as credit card details can be captured by attacker or the site can be a phishing website.

V. PROPOSED SYSTEM

In order to purchase any goods customer needs to fill his/her confidential details at Merchant site but Customer doesn't know whether merchant is genuine or not. In proposed solution, Fraud detection and prevention mechanism is applied which is achieved by introducing third party i.e. Bank Server. Bank Server will have all the necessary details needs to purchase any goods by customer. Customer will have an account created at Bank Server. At the time of login at bank server, customer will fill username, password, e-mail address etc. In return Bank server will provide user ID to Customer. With the help of user ID, Customer will login to Merchant server to purchase any goods. Merchant Server will also login to Bank Server. Merchant Server will provide Server Name, Server ID, URL etc to the Bank Server.

Following Steps shows the flow of complete system

1. Client will select product on our site.
2. Client will login to our system.
3. After successful login verification request will go to Merchant for verification.
4. To verify Merchant Server ID, UID and Server key will be sent to Bank Server.
5. At Bank Server, an entry for server ID and UID is present or not is checked.
6. If the entry is found then One-Time Password i.e. OTP is generated else random image is generated.

7. Generate QR code.
8. On QR code performs Visual Cryptography to generate two shares. One share for Merchant and other for client.
9. Send Share1 to Merchant Server.
10. Send Share2 to Client through email.
11. Now At Client side, Combine or superimpose Share1 and Share2 in order to extract OTP from image.
12. If OTP is present goto 13.
13. Enter OTP for verification.
14. Send OTP to Bank server for verification.
15. If OTP is validated that means Merchant server is validated.
16. If OTP is invalid means Merchant is phishing.
17. Now Admin i.e. Merchant server proceeds for payment.

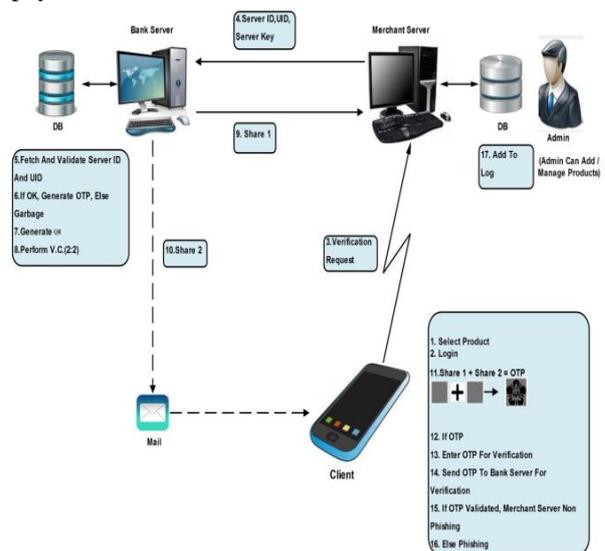


Fig. 3.Secure Online Payment System Using Visual Cryptography

VI. CONCLUSION

Now a day's phishing attacks are as common as it captures and stores the users' secret information. The proposed method preserves secret information of users, Verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website then in that state, the phishing website can't display the OTP for that specific user due to the fact that the OTP is generated by the stacking of two shares, one with the user and the other with the actual database of the website.

REFERENCES

- [1] Souvik Roy , P. Venkateswaran, "Online Payment System using steganography and Visual Cryptography," IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1–5, 1-2 March 2014.
- [2] K.V. Reddy, D.Shiva Rama Krishna, D.C.Janardana Reddy, "Captcha and Its Techniques for Providing Security in Web and Applications," in International Journal of Research (IJR) e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015.
- [3] Archana B. Dhole, Prof. Nitin J. Janwe, "An Implementation of Algorithms in Visual Cryptography in Images," in International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013
- [4] The Data genetics website [Online]. Available: <http://www.datagenetics.com/blog/november32013/>