Online Payment System using Steganography and Visual Cryptography

Priyanka More, Pooja Tiwari, Leena Waingankar, Vivek Kumar

Department of Computer Engineering, Savitribai Phule Pune University, Pune-411041, India

Abstract - **In recent time there is rapid growth in E-Commerce market. Major concerns for customers in online shopping are debit card or credit card fraud and personal information security. Identity theft and phishing are common threats of online shopping. Phishing is a method of stealing personal confidential information such as username, passwords, credit card details from victims. It is a social engineering technique used to deceive users. In this paper new method is proposed that uses text based steganography and visual cryptography. It represents new approach which will provide limited information for fund transfer. This method secures the customer's data and increases customer's confidence and prevents identity theft.**

Keywords - ***Steganography; Visual Cryptography; Online shopping; Phishing***

I. INTRODUCTION

Online shopping also called as e-tail is a way of purchasing products over internet. It allows customers to buy goods or services using web browsers and by filling credit or debit card information. In online shopping the common threats are phishing and identity theft. Identity theft is a form of stealing someone's identity i.e. personal information in which someone pretends to be someone else. The person misuses personal information for purchasing or for opening bank accounts and arranging credit cards. As a result of identity theft, the customer's information was misused for an average of 48 days in 2012. Phishing is a method of stealing personal confidential information such as username, passwords, credit card details from victims. It is a criminal mechanism that uses social engineering. Phishing email directs the users to visit website where they take users personal information such as bank account number, password. It is email fraud conducted for identity theft. In 2013, Financial and Retail Service, Payment service are the targeted industrial sectors of phishing attacks.

The method which is proposed in this paper uses both steganography and visual cryptography. It reduces information sharing between customer and merchant server and safeguards customers information. It enables successful fund transfer to merchant's account from customer's account and prevents misuse of information at merchant side. In this system there are two shares of OTP which are combined to get original OTP. In this way the system provides secure transaction.

The rest of the paper includes: Section II gives Abbreviations used in this paper. Section III gives brief idea of steganography and visual cryptography. Section IV includes system architecture. Section V gives brief description of both merchant server and bank server. Section VI includes advantages of proposed system. Section VII gives conclusion of the paper.

II. ABBREVIATIONS

DB: Database

DS: Digital Signature

PC: Personal Computer

OTP: One Time Password

TP: Transaction Password

URL: Uniform Resource Locator

QR : Quick Response

III. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is a technique or a method of hiding the information into the image. It is the practice of concealing a file, message or image into another file, message or image. Steganography combines the word steganos and graphein. The meaning of steganos is covered or protected, the meaning of graphein is writing. The term steganography was first used in 1499 by Johannes Trithemius. The message which is hidden may be in invisible link between the visible lines of personal letter.

The advantage of this technique is that the hidden message does not pay attention to itself as an object scrutiny. It includes hiding of information within computer files. For the transmission purpose media files are considered as ideal because of their large size. Electronic communication involves steganography coding within transport layer. This term has been widely used including recent times even present day. In ancient Greece

people wrote text on wood and protect it with wax. In 1985 steganography entered into modern world with the advantage of personal computer being applied to traditional steganography problems. Hiding message within lowest bits of noisy images. Concealing information within encrypted data. The message which is to be hidden is encrypted then used to overwrite part of a much larger block of encrypted data.

Cryptography is the practice and the study of techniques for secure communication in the presence of third parties. It is special encryption technique in which visual information is encrypted in such a way that decryption does not require a computer.

This technique was developed by Moni Naor and Adi Shamir. Cryptography was developed in year 1994.Visual cryptography uses two transparent images. One image contains random pixels and other contains secret information. It is impossible to retrieve secret information from one of the images. But both transparent images are required to reveal the information. In this technique the image was broken into *n* number of parts so that someone can decrypt this image using these *n* numbers of parts. There is a need of expansion of space in visual cryptography but if one of the two parts are structured recursively, its efficiency can be increased to 100%. Visual cryptography can be used to conserve biometric templates where decryption does not require any complex computations.

IV. SYSTEM ARCHITECTURE

In this system there will be two servers, bank server (admin) and merchant server (product admin). Product admin will add the products and product related information in its database. Admin i.e. bank server will add users and merchant servers. User specific data includes user name, user id, transaction password and user password. While merchant server specific data includes server id, password and URL in the Admin's database.

Client will select the product and log in to respective site. Then verification request is sent to merchant server. Merchant server will verify the user name, user id and along with that it will add server id, server key and send it to the bank server for the verification. Bank server will verify the server id, server key of merchant server. If it is ok then bank server will generate one OTP through steganography. If the merchant server is fake then it will not generate OTP. After OTP generation it will form two shares using visual cryptography. One will be sent to the client via email and other will be sent to the merchant server. Merchant server will send the second share to the client. After having two shares, at client side these two shares are combined and original OTP gets generate.

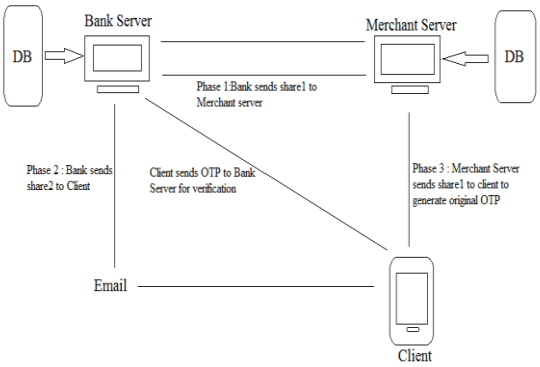

Figure 1. System Architecture

In phase 1, bank server will communicate with merchant server by sending share1 to the merchant server. In phase 2, bank server will communicate with client by sending share2 to the client. In third phase, there is communication between merchant server and client and original OTP gets generated by combining share1 and share2 at client side. In fourth phase, if the generated OTP is valid then required transaction will be carried out.

V. MERCHANT AND BANK SERVER

In the given system admin i.e. bank server adds and manages servers. It generates server id and password. It also manages users. Product admin i.e. merchant server adds and manages products. Android client selects product, login to the website, enters merchant address, user id and sends request to merchant server for verification. Then the client receives share1 in response. Received share2 is uploaded via email. Then share1 and share2 are combined. After combining share1 and share2, if QR code is formed it is scanned to view OTP. Client enters appeared OTP on the screen. If OTP is verified transaction page appears. After entering transaction password if it is matched transaction gets carried out successfully.

Merchant server is product admin. It receives request from client with user id. Then merchant server sends its own server id, password and received user id to bank server. In response bank server sends share1 to the merchant server. Then merchant server sends share1 to the client.

To check whether the system prevents phishing, one fake server is created. Fake server receives request from client with user id. Fake server sends its fake server id, password and received user id to bank server. Bank server sends fake share1 in response. Then fake server sends fake share1 to the client.

Bank server authenticates user and merchant server. It receives merchant or fake server request. It verifies received server id and password. Then it verifies user and fetches email id. It generates OTP. After

generating OTP, QR code of OTP is generated by applying visual cryptography. It sends share2 to client via email. If the merchant server is valid then bank server sends share1 as response to the particular merchant server else it sends fake share to the merchant server. If merchant server is valid, share1 and share 2 are combined to generate original OTP in the form of QR code.

VI. ADVANTAGES

1. The proposed system provides two way authentication i.e. authenticating client and merchant server.
2. Two shares of the OTP are created with the help of visual cryptography to make the system secure.
3. It helps to prevent phishing.
4. It prevents identity theft.
5. The system provides security to users data.

VII. CONCLUSION

In this paper, steganography and visual cryptography are combined to provide secure transaction in online shopping. It secures customer's confidential information at merchant side and hence prevents misuse of data. This method is mainly concerned with preventing identity theft and providing customer data security. It also prevents phishing. The system authenticates client as well as merchant server.

REFERENCES

[1]. Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceeding of IEEE Students' Conference on Electrical, Electronics and Computer Science , Jadavpur University, Kolkata-700032, India, 2014.

[2]. 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 Intelligence, 2010.

[3]. N. Chou, R. Ledesma, Y. Teraguchi, and D. Boneh, "Client-side defense against web-based identity theft," in *Proc. 11th Annu. Netw. Distribut. Syst. Secure. Symp.*, San Diego, CA, Feb. 2005.

[4]. 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, v 3,n 4, October/December 2006.

[5]. M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994.