Online Secure payment System Using shared Images

[1]Prof. Anuja Zade,[2] Bhupendra Singh ,[3] Jawed Ansari, [4] Akshit Pandita
[1234] JSPM, s RSCOE Tathawade Pune 33

Abstract - *As a quick growth in online shopping is seen in recent time throughout the world. By increase in online shopping, many type of frauds like phishing, credit or debit card fraud are takes place. For the security of customer this paper has presents a new approach for providing limited information only that is necessary for fund transfer during online shopping there by safeguarding users data and increasing users confidence and preventing identity theft. The method uses combined application of steganography and visual cryptography for this purpose.*

Keywords – visual cryptography, online shopping, Stenography, Phishing, safeguarding.

I. INTRODUCTION

A high-speed welfare in E-Commerce market has been witnessed in recent times throughout the world. With increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major burden for customers and banks specifically in the case of CNP (Card Not Present). 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 thieving someone's identity i.e. personal information in which someone pretends to be someone else. The person misuses personal information for opening bank accounts and arranging credit cards. Proposed system presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby protecting customer data and gaining customer confidence and preventing identity theft. The approach uses combined application of Steganography and image cryptography for this purpose. User Account Details such as Account Number, Debit Card Number and Secret Pin Number are hidden into an Image using Steganography technique and Image is split into two Shares and shares are encrypted. [1]As Online Shopping Portals are insecure for Customer's Account Details, Customer has to provide only Account Number on Shopping Portal and Secret details of Bank account are obtained from adding user image share with Server image share by admin of the Bank.

This system 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.

Once you think your computer is safe to use but there is rise through social media. In social media we are much more open about ourselves online. Now days 61% of people say that they uses social networking sites. Illustrating the central role that such sites now play in our lives. [1]As we become more confident using these networks, we can begin to feel 'untouchable'. We forget that criminals will use the personal information for their benefits like your date of birth and where you live is enough for someone to begin building the profile needed to apply for a credit card in your name. So while most people wouldn't give this information to a stranger in real life, they will happily post it online where they did not care about it.

Types of frauds:

Spam and Identity Theft

Identity fraud terms used to [2] refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. In this identity of person is seal through social network sites and this information is used for wrongful purpose.
In identity theft E-mail address of the user is used for terrorist activities, defamation, fake E mails.

Credit Card Fraud

There are various mods of Credit card fraud are as follows:
Duplication: Card is with owner and is duplicate is made by stealing data of the owner.
Skimming: Collection of data from the card's magnet and copy it to blank card.
Call center leaked: The card information in sold to Fraudsters.
Bank back office data: By hacking the bank server and getting the personal information.
Data theft: Stealing the information by sending spam E-mails.
Man in middle attack: Gaining the access when customer is contacting with vendor for payment and accessing the information.

Investment Fraud

Various investment schemes typically target stock investors, trying to steal money and investors' identities. Some of these scams will come in the form of an online newsletter.[2] In these newsletters, frauds will offer inside information on stocks, for a fee, and offer false data instead of real information. Online bulletin boards have also become a hotbed of fraudulent activity.

Companies often use online bulletin boards to publish information; however, a bogus board will release disinformation. A pump and dump scheme can start with a fraudulent newsletter or bulletin board where secret or private information is offered. The object of this scheme is to alter stock values. After effectively hindering a stock, the schemer will sell his or her own stock in a timely fashion for personal gain.

II. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Cryptography involve in which data is converted into unreadable format for unauthorized user.[1] Cryptography involve generating code that allow the information to keep secret. In data security it uses cryptography on several levels. The data cannot be read without a key to decrypt it.

In Cryptography the sender and receiver uses pair of key to authenticate each other.

Secret Key Cryptography: Here only one key is used for encryption and decryption.

Public Key Cryptography: Here two key is used for encryption and decryption. One key is used at sender side and another key is used at client side.

Hash Functions: These are different from Secret Key Cryptography and Public Key Cryptography.Here no key is used at all that why its s called as one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged.

STEGANOGRAPHY

The term Steganography consist of hiding the secret message into normal message and the extraction is done at destination point only.

PUBLIC KEY CRYPTOGRAPHY

Public key cryptography or asymmetric key cryptography is an encryption scheme that uses two keys –

Public key

Private Key

In symmetric key algorithms that depends on one key that for both encrypt and decrypt, each key performs a unique function. Here in Public key cryptography
The public key is used to encrypt.
The private key is used to decrypt.

It is not conventional to compute the private key depending on the public key. [3]Because, the public keys can be freely distributed, it allows users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, and identifying only the owners of the private keys can decrypt content and create digital signatures.

Since the public key has to be shared with user but it is very large and it is difficult to remember so that's why it is being encrypted in the image having some digital signature

Digital certificates are issued by entities known as Certificate Authorities (CAs).

TRANSACTION IN ONLINE SHOPPING

In traditional online shopping as shown in Fig. 2 consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, payonlinesystem, WebMoney and others.[3] In the payment portal consumer submit his or her credit or debit card details such as credit or debit card number, name on the card, expiry date of the card.

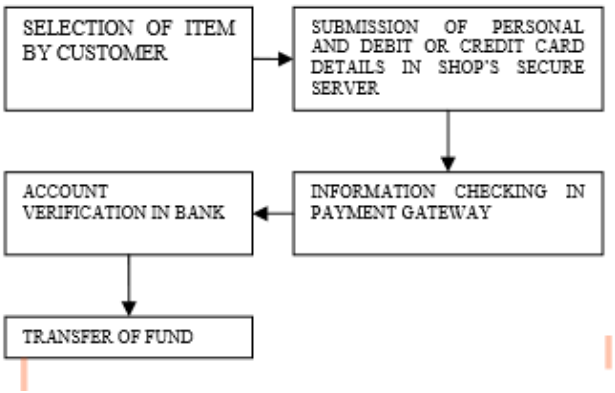

Fig. 2. Transaction in online shopping.

Details of information sought from shopper vary from one payment gateway to another. [4] For example, payment in IRCTC website requires Personal Identification Number (PIN) when paying using debit card whereas shopping in Flipkart or Snap deal requires Visa or Master secure code. In addition to that merchant may require a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard), which is basically an authorizing code in CNP transactions. According to the PCI Data Security Standard, merchants are prohibited from storing CVV information or PIN data and if permitted card information such as name, card number and expiration date is stored, certain security standards

are required. [5]However recent high profile breaches such as in Epsilon, Sony's PlayStation Network and Heartland Payment Systems show that card holders' information is at risk both from outside and inside. [4]A solution can be forcing merchant to be a PCI complaint but cost to be a PCI complaint is huge and the process is complex and time consuming and it will solve part of the problem. One still has to trust the merchant and its employees not to use card information for their own purposes

III. PROPOSED PAYMENT METHOD

In the proposed solution, information given by the customer to the online merchant is minimized by providing only sufficient information that will only verify the payment made by the said customer from its bank account. [5]This is achieved by the introduction of a central Certified Authority(CA) and combined application of stenography and visual cryptography. The information received by the service provider can be in the form of account number related to the card used for shopping or card information. The information will only validate receipt of payment from authentic customer. The process is shown in Fig. 3. In the applied method, customer unique password(authencation) in connection to the bank is hidden inside a cover text using the text based stenography method as mentioned in section IV. Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form. Now a snapshot of two texts is taken. From the snapshot image, two shares are generated using visual cryptography.

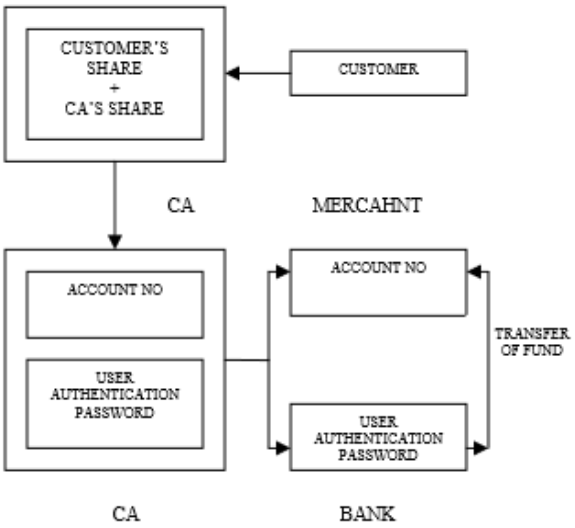

Fig. 3. Proposed payment method

Now one share is kept by the customer and the other share is kept in the database of the certified authority. During shopping online, after selection of desired item and adding it to the cart, preferred payment system of the merchant directs the customer to the Certified Authority portal. In the portal, shopper submits its own share and merchant submits its own account details. Now the CA combines its own share with shopper's share and obtains the original image. [6] From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text. Customer authentication information is sent to the merchant by CA. Upon receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account. After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information.

Advantage

Proposed method minimizes customer information sent to the online merchant. So in case of a breach in merchant's database, customer doesn't get affected.

It also prevents unlawful use of customer information at merchant's side.

Presence of a fourth party, CA, enhances customer's satisfaction and security further as more number of parties are involved in the process.

Usage of steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy.

Cover text can be sent in the form of email from CA to bank to avoid rising suspicion.

Since customer data is distributed over 3 parties, a breach in single database can easily be contented.

Security Threat

During payment, merchant's payment system requires to direct the shopper to CA's portal but fraudulent merchant may direct shopper to a portal similar to CA's portal but of its own making and get hold of customer own share. To prevent this type of phishing attack, an end-host based approach can be implemented for detection and prevention of phishing attack.

IV. CONCLUSION

In this paper, a payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. The method is concerned only with prevention of identity

theft and customer data security. In comparison to other banking application which uses cryptography.

V.REFERENCES

[1] *http://smallbusiness.chron.com/types-internet-fraud-work-61078.html*

[2]*https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture12.pdf*

[3]*http://searchsecurity.techtarget.com/definition/RSA*

[4]Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm Abhishek Gupta, Sandeep Mahapatra, Karanveer Singh, 978-1-4577-0240-2/11/$26.00 ©2011 IEEE

[5] A Double Security Approach for Visual Cryptography using Transform Domain 978-1-4673-6994-7/15 $31.00 © 2015 IEEE DOI 10.1109/ICACC.2015.32

[6] Hiding Secret Message using Visual Cryptography in Steganography 978-1-4673-6540-6/15/$31.00 © 2015 IEEE

[7] Proposed Symmetric Key Cryptography Algorithm for Data Security978-1-5090-2084-3/16/$31.00 ©2016 IEEE 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016).

Biography

Bhupendra Singhpursuing Bachelor of Engineering form JSPM, s Rajarshi Sahu College of Engineering

.

Akshit Panditapursuing Bachelor of Engineering form JSPM, s Rajarshi Sahu College of Engineering