ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Online Payment System Using Cryptography Techniques

Mr.Dilip Bahadur Malla
MCA 3rd Year, II Sem,
CMR College of Engineering & Technology,
Hyderabad.

Ch.Dayakar Reddy
MCA, M-Tech, MPhil, Ph.D,
Professor and HOD,
CMR College of Engineering & Technology,
Hyderabad.

ABSTACT:

A rapid growth in E-Commerce market is seen in recent time throughout the world. With ever increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks specifically in the case of CNP (Card Not Present). This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of Steganography and visual cryptography for this purpose.

INTRODUCTION:

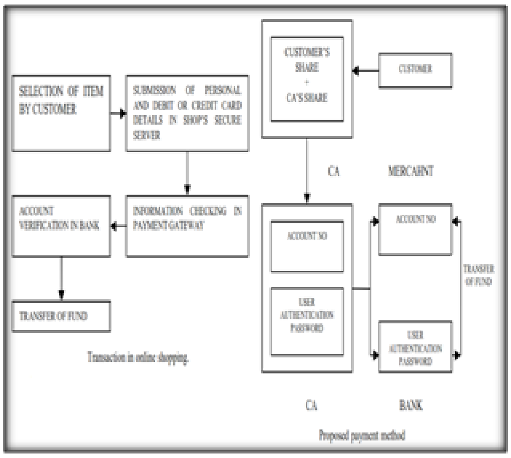
Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier[1]. Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft[2]. Phishing is a criminal mechanism that employs both social Engineering and technical subterfuge to steal consumers 'personal identity data and financial account credentials.

In 2ndquarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others. In this paper, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side.

The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking. The rest of the paper is organized as follows: Section Gives brief description of text based steganography and visual cryptography. Section III contains related works. Section I presents the proposed steganography method. Section Provides method of transaction in online shopping. Section VI presents proposed payment method. Section VII concludes the paper.

SYSTEM ARCHITECTURE:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal


SELECTION OF ITEM BY CUSTOMER
SUBMISSION OF PERSONAL AND DEBIT OR CREDIT CARD DETAILS IN SHOP'S SECURE SERVER
ACCOUNT VERIFICATION IN BANK
INFORMATION CHECKING IN PAYMENT GATEWAY
TRANSFER OF FUND
Transaction in online shopping.
CUSTOMER'S SHARE + CA'S SHARE
CUSTOMER
CA
MERCAHNT
ACCOUNT NO
USER AUTHENTICATION PASSWORD
ACCOUNT NO
USER AUTHENTICATION PASSWORD
TRANSFER OF FUND
CA
BANK
Proposed payment method

EXISTING SYSTEM:

Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others.

Draw Back:

In result to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility in sentence construction. So to hide a large message, this technique requires large no of words and creates a complexity in sentence construction. Disadvantage of this technique can be used in its advantage by applying it to online banking to createspam mail to hide one's banking information.

PROPOSED SYSTEM:

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of Steganography and visual cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer.

Advantages:

Proposed method minimizes customer information sent transfer of fund 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 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.

IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

MODULES:

1. STEGANOGRAPHY PROCESS

In this module, Steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence. This gives flexibility and freedom from the point view of sentence construction but it increases computational complexity.

2. ENCODING

1. Representation of each letter in secret message by its equivalent ASCII code.
2. Conversion of ASCII code to equivalent 8 bit binary number.
3. Division of 8 bit binary number into two 4 bit parts.
4. Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
5. Meaningful sentence construction by using letters obtained as the first letters of suitable words.
6. Encoding is not case sensitive.

3. DECODING STEPS:

1. First letter in each word of cover message is taken and represented by corresponding 4 bit number.

2. 4 bit binary numbers of combined to obtain 8 bit number.
3. ASCII codes are obtained from 8 bit numbers.
4. Finally secret message is recovered from ASCII codes.

4. TRANSACTION IN ONLINE SHOPPING:

In this module traditional online shopping 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, pay online system, Web Money and others. 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.

5. CUSTOMER AUTHENTICATION:

Customer unique authentication password in connection to the bank is hidden inside a cover text using the text based Steganography method. 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. Now one share is kept by the customer and the other share is kept in the database of the certified authority.

6. CERTIFICATION AUTHORITY ACCESS:

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. From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text.

7. Final Authenticated Information Results:

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.

CONCLUSIONS:

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 Steganography and visual cryptography are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

REFERENCES:

Jihui Chen, XiaoyaoXie, and Fengxuan Jing, "The security of shoppingonline," Proceedings of 2011 International Conference on Electronic andMechanical

Engineering and Information Technology (EMEIT), vol. 9,pp. 4693-4696, 2011.

Javelin Strategy & Research, “2013 Identify FraudReport,”ttps://www.javelinstrategy.com/brochure /276.

Anti-Phishing Working Group (APWG), “Phishing ActivityTrendsReport,2013,” http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf .

Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O’Gorman,“Hiding Information in Document Images,” Proceedings of the 1995Conference on Information Sciences and Systems, Johns HopkinsUniversity, pp. 482-489, 1995.

J. Chen, T. S. Chen, M. W. Cheng, “A New Data Hiding Scheme inBinary Image,” Proceeding of Fifth International Symposium onMultimedia Software Engineering, pp. 88-93, 2003.

Hu ShengDun, U. KinTak, “A Novel Video Steganography Based onNon-uniform Rectangular Partition,” Proceding of 14th InternationalConference on Computational Science and Engineering, pp. 57-61,Dalian, Liaoning, 2011.

Daniel Gruhl, Anthony Lu, Walter Bender, “Echo Hiding,” Proceedingsof the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.

Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, “Techniquesfor Data Hiding,” IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

K. Bennet, “Linguistic Steganography: Surevey, Analysis, andRobustness Concerns for Hiding information in Text,” PurdueUniversity, Cerias Tech Report 2004—2013.

J.C. Judge, “Steganography: Past, Present, Future,” SANS Institute,November 30, 2001.

M. Naor and A. Shamir, “Visual cryptography,” Advances inCryptograhy: EUROCRYPT’94, LNCS, vol. 950, pp. 1–12, 1995.

Jaya, Siddharth Malik, AbhinavAggarwal, Anjali Sardana, “NovelAuthentication System Using Visual Cryptography,” Proceedings of 2011 World Congress on Information and CommunicationTechnologies, pp. 1181-1186, Mumbai, India, 2011.

ChetanaHegde, S. Manu, P. DeepaShenoy, K. R. Venugopal, L MPatnaik, “Secure Authentication using Image Processing and VisualCryptography for Banking Applications,” Proceedings of 16th International Conference on Advanced Computing andCommunications, pp. 65-72, Chennai, India, 2008.

S.Premkumar, A.E.Narayanan, “New Visual Steganography Scheme forSecure Banking Application,” Proceeding of 2012 InternationalConference on Computing, Electronics and Electrical Technologies(ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.

K. Thamizhchelvy, G. Geetha, “E-Banking Security: Mitigating OnlineThreats Using Message Authentication Image (MAI) Algorithm,”Proceedings of 2012 International Conference on Computing Sciences(ICCS), pp. 276 – 280, 2012.