

Online Secure Payment system using Steganography and Cryptography

Mrs. Rakhi Bhardwaj, Mr. Anurag Rachcha, Ms. Rujuta Desai

Trinity College of Engineering and Research.

University of Pune, India. bhardwaj.rakhi78@gmail.com rachcha.anurag13@gmail.com rujuta.desai.5@gmail.com

Mr. Saneesh Jose, Mr. Saurabh Vibhute

Trinity College of Engineering and Research.

University of Pune, India. snshjs101@gmail.com sourabh007v@gmail.com

Abstract— Internet has now provided the means for us to establish communication like never before ranging right from accurate representations to high speed data transmission. With the new technological innovations arriving everyday, one that reached the users is online shopping but it came with its own share of boon and bane. One of the imminent threat is that of intrusion and leak. Secret information can be hidden into sources of information. These information files like audio, video, text or image helps us to set up an invisible type of communication known as Steganography. In our project, we have used image steganography where we hide data inside stego image. Identity theft needs to be prevented, hence we propose a new approach by providing information that's only necessary for transaction while shopping online. This ensures privacy and personal data safeguarding for the user.

Keywords- Steganography, Cryptography, Transactions, Debit & Credit cards, Two-factor dividing.

I. INTRODUCTION

There has been a rise in the usage of E-commerce now. This has given rise to credit and debit card frauds along with the leak of private information of customers, online merchants and the banks. A typical scenario can be considered when the users access these E-commerce websites and provide the card details to complete the transaction. Attackers attack to gain this information using attacking techniques such as phishing etc.

If the sensitive data is acquired, data can be misused by the attacker in a number of ways. Hence, the proposed system offers a way to share just the necessary information to complete transactions which ensures there is data privacy and theft is avoided. It uses a combination of image cryptography and steganography. The process goes ahead by storing the user account details. The details may contain information such as the account number, debit or credit card number, PIN number. This information is stored into an image using steganography. This image is then split and both the halves created which undergo encryption. This ensures that we don't enter sensitive data on websites which are attackable, hence entering it only on the shopping portal.

Root of needed information is obtained upon emerging of the two halves. This addresses the information theft concern at its roots. It also facilitates successful transfer with extended security measures.

II. LITERATURE SURVEY

Various catastrophic and costly mistakes such as when shopping items bought using stolen card details,

industry penalties etc. happen on failure of payment systems.

Wordplay saw over 133,000 fraudulent transactions that were reported which meant that theft was done every 20 seconds. Upon survey, we found that there were some already proclaimed secure payment systems but consisting of their own limitations given as follows:

1. Support for only one type of image.
2. Unfriendly situations to perform encryption or decryption.
3. In visual cryptography schemes that were used for data hiding, flaws were found in encrypted shared file.

Hence, in our proposed system we use steganography and AES (Advanced Encryption Standard) algorithm.

III. MOTIVATION

There have been quite a few of motivation factors which are as follows:

1. Online shopping has been receiving ever-increasing attention.
2. Reducing the amount of burden on the shopkeepers, banks and merchants with various problems such as card data fraud and information security.

Time complexity can be reduced by our proposed system and an extra layer of security can be added to funds transaction process. It also provides a better service for the customer by systematically providing all the information about e-shopping.

Using just the account details, it makes it easier for the customer to make various transactions online. Provision for the customers who do not have much time in hand, to shop online and get other online payments done. Usage of steganography in these scenarios ensures that customer authentication password is safe thus maintaining customer privacy.

IV. OBJECTIVE

In our proposed system, the customer need only provide the bare minimum information to the seller on the E-commerce site. With this information it can confirm whether the transaction has been made successfully with the bank. Mainly, it is the account number of the card used for transaction that is shared with the seller. Once the seller confirms the account number to the authentic customer, it's related receipt of payment is issued.

The specific objectives of this System are :
 Only using account number, a customer can be given some means to perform online transactions. By not having to provide other sensitive and personal data, we save up a lot of time and also safeguard the other card details.

V. SYSTEM REQUIREMENT

A. Software

1. Platform : Windows 7
2. Programming Environment : Eclipse Kepler
3. HTTP Server : Apache Tomcat Server 7
4. Design : HTML, Jsp

B. Hardware

1. 4GB RAM
2. Hard disk : 40 GigaBytes or higher
3. Speed : 1.80 GigaHertz

C. Backend

MySQL

VI. METHODOLOGY

1. Selection of topic
2. Preparing abstract and related documents
3. Collecting research paper related to topic
4. On-field survey of requirement gathering
5. Preparation of critique on the collected research papers
6. Technical research of different algorithms and crypto systems.
7. Designing block OR architectural diagram
8. UML diagrams
9. Creating project module by module

VII. SYSTEMARCHITECTURE

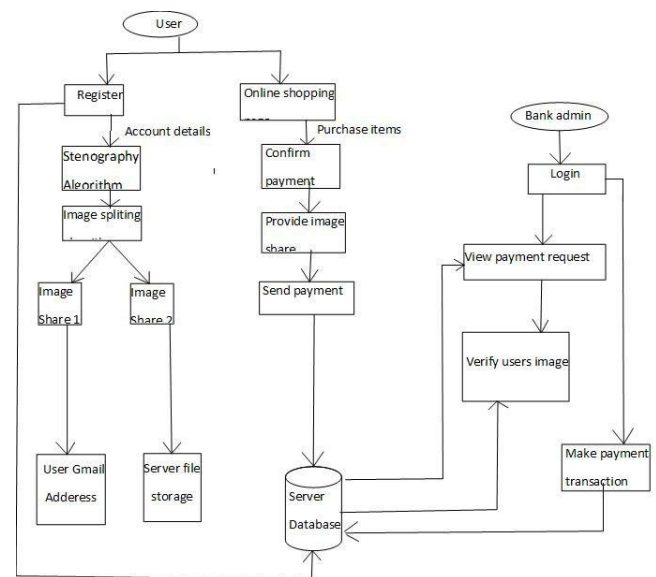


Figure 2. System Architecture

1. User has to register on Online Payment Portal.
2. User has to provide his/her Account details of any Bank and this details are stored into Banks Server Database.
3. Details such as account, debit and security pin numbers of the users are then hidden by the technique of steganography.
4. The image is then split into two halves, each is encrypted using the AES algorithm.
5. One Cryptographic share is sent on User's Gmail address and other share is stored on Server.
6. Once Registration is complete, user can do online shopping on Shopping Page and select an Item for purchasing.
7. Once item is selected, user is redirected on for Money Transfer. For Money transfer, user has to provide Account Number and Cryptographic share for authentication.
8. Request for Money Transfer is sent to Admin of Respective Bank. Admin after logging in to Portal can see Money Transfer requests from users of Bank.
9. Admin verifies customer by merging provided cryptographic share with Server stored image share and after getting full image, it is compared with original image. If Customer is authentic then Admin can confirm payment of user for an Item.
10. 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 merging

user share with Server share by Admin of Bank.

VIII. ALGORITHM

Steganography Algorithm :

An image can be configured to hide secret data which gives up an advantage over traditional cryptography alone.

Cryptography almost gives away the fact that there could be some kind of encrypted message provoking the attacker to decrypt. Hence, steganography helps with concealment inside files, images etc.

AES (Advanced Encryption Standard) :

It's a symmetric block ciphering technique for protection of the classified information. It is one of the most widely used algorithms out there which found its applications in both software and hardware.

Some of its valient features are as follows :

1. Symmetric key
2. Symmteric block cipher
3. 128 bit data, 128/192/256 bit keys
4. Better than triple - DES

It's a private key encryption technique, hence private key should be known by the sender and the receiver.

MySQL :

It's a computer programming language used by database software and also one of the two most frequently used language used for handling of database. RDBMS (Relational database management systems) that runs as a server which provides multi user access to a number of databases. MySQL is popular for adding, accessing & managing contexts in a database. This language is written in either C or C++.

IX. CONCLUSION

Thus, our proposed system of online secure payment system using steganography and cryptographic algorithm ensures that there is no sensitive data theft, furthermore makes sure that the information with merchants are safeguarded. Another important issue is addressed i.e. customer data security. An application for this can be made for various E- commerce websites as well as physical Banks.

X. FUTURE SCOPE

Our scope is specially in the online transaction to make

a secure payment system. It provides facility to the customer to do payment by online transactions using just the account detail. Sensitive data like account details can be secured and eventually save time. It mainly provides a way to just show particular information which are necessary to perform transactions on the E-commerce website.

REFERENCES

- [1] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, The security of shoppingonline Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology EMEIT, 9, pp. 4693-4696, 2011.
- [2] Javelin Strategy & Research, 2013 Identify Fraud Report <https://www.javelinstrategy.com/brochure/276>.
- [3] Anti-Phishing Working Group APWG, Phishing Activity Trends Report, 2013 <http://docs.apwg.org/reports/apwg-trends-report-q2-2013.pdf>.
- [4] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman Hiding Information in Document Images Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.
- [5] J. Chen, T. S. Chen, M. W. Cheng, A New Data Hiding Scheme in Binary Image Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.
- [6] Hu ShengDun, U. KinTak, A Novel Video Steganography Based on Non-uniform Rectangular Partition Proceeding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.
- [7] Daniel Gruhl, Anthony Lu, Walter Bender, Echo Hiding Proceedings of the First International Workshop on Information Hiding, pp. 293-315, Cambridge, UK, 1996.
- [8] K. Bennet, Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text Purdue University, Cerias Tech Report 2004-2013.
- [9] S. Premkumar, A. E. Narayanan, New Visual Steganography Scheme for Secure Banking Application Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies ICCEET, pp. 1013-1016, Kumaracoil, India, 2012.
- [10] <http://oxforddictionaries.com/words/what-is-the-frequency-of-the-letters-of-the-alphabet-in-english>.
- [11] "Model-based Steganography", P. Salee, In: Proceeding of the 2nd International workshop on digital water marking, Seoul, Korea, October 20-22 2003, LNCS, vol.2939, pp. 254-260.
- [12] "Steganography and Steganalysis: An Overview", J. Silman, SANS Institute, 2001.
- [13] "Techniques for data hiding", W. Bender, D. Gruhl, N. Morimoto, and A. Lu, IBM Systems Journal, Vol 35, No. 3-4, pp 313-316.
- [14] "High capacity image steganographic model", Lee, Y.K.

-
- and Chen, L.H., Visual Image Signal Processing, 147:03, June 2000.
- [15] "Hiding data in the OSI network model", T. Handel, M. Sandford, , In Anderson, R., ed: Information Hiding: Proceedings of the 1st International Workshop on Information Hiding, Cambridge, U.K., Springer June 1996, pp 23-38.
- [16] "Steganalysis of Images Created Using Current Steganographic Software," N.F. Johnson and S. Jajodia, Proc. 2nd Int'l Workshop in Information Hiding, Springer-Verlag, 1998, pp. 273-289.
- [17] "An overview of image Steganography", T. Morkel, J.H.P. eloff and M.S. Olivier, information and computer security architecture (icsa) research group.
- [18] "Lossless 3D Steganography based on MST and Connectivity modification", by P. Amat, W. Puech, S. Druon and J.P. Pedebay, Signal Processing: Image communication 25(2010), Elsevier, pp 400-412.
- [19] In: Proceedings of IEEE International Conference on Communication Technology, Z. Zhao, N. Yu, and X. Li, "A novel video watermarking scheme in compression domain based on fast motion estimation", 2003, pp. 1878-1882.
- [20] "Information hiding techniques for steganography and digital watermarking", Stefan C. Katzen Beisser and N. F. Johnson, Artech House 2000, ISBN 1-58053-035-4, pp 67-71.