© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Securing E-Transaction Using Cryptography & Steganography

Awanika Welpulwar[1], Pranali Kalambe[1], Puja Bhute[1], Swati Ramteke[2]

[1]Department of CSE, RTMNU/KDK's SRMCEW, Nagpur, Maharashtra, India

[2]Assistant Professor, Department of CSE, RTMNU/KDK's SRMCEW, Nagpur, Maharashtra, India

ABSTRACT

In recent time there is rapid growth in E-commerce market throughout the world. Personal information security are major concern for customers and merchants due to increasing popularity of online shopping, debit or credit card fraud and banks specifically in the case of card not present. Identity theft and phishing are the threats of online shopping. This approach helps in safeguarding customer data and increasing customer confidence and preventing identity thief by giving extra level of security. This method uses combined application of Cryptography & Steganography.

Keywords: Steganography, Cryptography, Advance Encryption Standard(AES), Compression, Decompression.

I. INTRODUCTION

With the growth of information technology , now a days everyone has at least one smart device, such as mobile phones or tablet computers. In recent days there is rapid growth in E-Commerce market. Major concern for customers is common threats of online shopping. Now you can securely perform your online transactions with the help of this system as it provides three level of security. By this the customers an safely buy their products without any problem.

II. AIMS & OBJECTIVES

Payment portal, a channel between consumers and payment processors use numerous security tools to secure consumer's payment information, ordinarily card data during the online transaction.

III. SCOPE

This project is developed on the basis of more need of security in online transaction. Now a days online transaction is getting less secure with emerging ways to hack/crack ATM PIN or ATM card. That OTP will be sending on registered mobile number of the user and that OTP will be used to access online transactions. If user wants to use fingerprint system, he/she can select that option on the screen and can access.

IV. EXISTING SYSTEM

August 2014: International journal of advanced computer science and applications:

Two important aspects of security that deal with transmitting information for data over some medium light internet are strganography and cryptography. Steganography used to hiding the presence of a message and cryptography used to hiding the contents of message. Both of them are used to provide security. But neither steganography nor cryptography can simply fulfill the basic requirements of security i.e. features such as strongness , unnoticeable and ability etc. In existing system, in order to perform user authentication a basic text type of password and OTP is use. After being authorized the user will have to enter personal information to perform further transaction. Unsuspecting users may use these sensitive details anywhere. In the existing system only text

IJSRSET11844157 | Received : 13 March | Accepted : 24 March 2018 |

information is use, which may be vulnerable to attacks. So a new method based on the combination of both cryptography and steganography known as crypto-steganography which overcome each other's weakness and make difficult for the intruders to attack or steal sensitive information is being proposed.

V. RELATED WORK

1.PHISHING PROCESS:

Phishing is a very common attack in online transaction. Phishing is a method of stealing data in which attackers send fake email from various website to collect the user private information. User will unwittingly enter the password or other private information, thinking it is a legitimate website. Attacker collect these stolen data and use it to gain access to private areas of website. To tackle this, anti-phishing image base authentication technique have been proposed. If these use image steganography and cryptography, they will be more secure and eliminated phishing.

2.AES:

Advanced Encryption Standard (AES) is a symmetric-key algorithm [12,3] with a block size of 128 bits. It supports lengths of 128,192, and 256 bits. AES is a superior algorithm with advanced when compared with the data encryption standard (DES) [13]. In AES, there is no feistel network like in standard DES. The cipher consists of rounds; the number of rounds used depends on the key length; 10 rounds for a 128-bit key,12 rounds for 192-bit key, and 14 rounds for a 256-bit key. The whole algorithm operates on a 4*4 matrix of bytes. The first rounds comprises four distinct transformation function: sub bytes, shift rows, mix columns, and add round key. The final round contains three transformation the mix columns function is not used in the final round. Each transformation takes one or more 4*4 matrices as input ad prudes a 4*4 matrix as output.

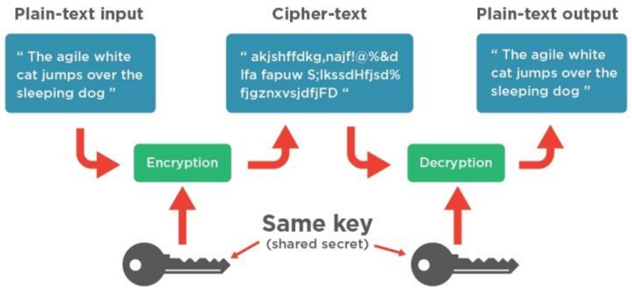

Plain-text input
" The agile white cat jumps over the sleeping dog "
Cipher-text
" akjshffdkg,najf!@%&d lfa fapuw S;lkssdHfjsd% fjgznxvsjdfjFD "
Plain-text output
" The agile white cat jumps over the sleeping dog "
Encryption
Decryption
Same key
(shared secret)

Figure 1. Encryption & Decryption

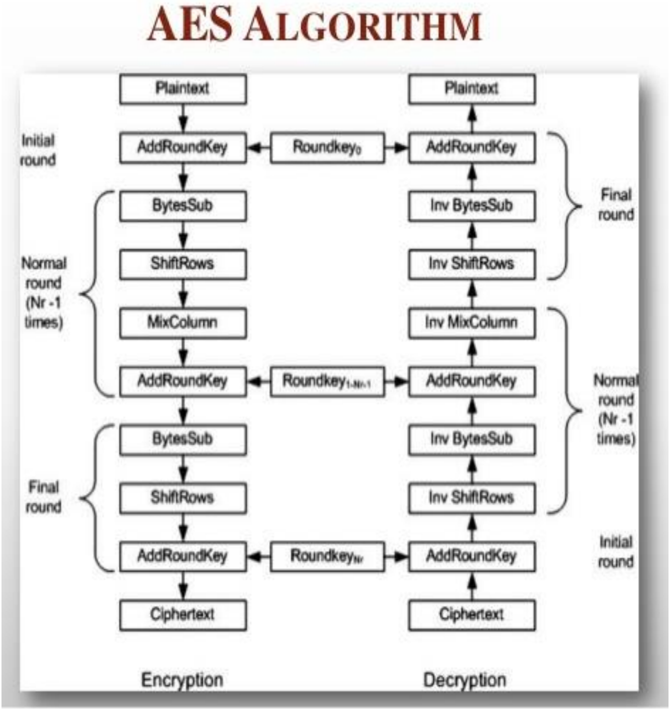


Figure 2. AES algorithm

VI. PROPOSED SYSTEM

In a proposed solution the information submitted by customer or user is secured by three level of security. We can securely perform the online transaction with the help of this system. This system works as follows. User will have to register in order to get access to the system. User will have to provide his username and password in order to login to the system. Here all the products can be viewed by the user along with its other details like short description ,cost and also image of the product. In order to perform any transaction here the user needs to provide his bank information like his account no. card no. CVV no. and pin no. to make the payment. Once the user enters username and password, the system sends OTP which will contain four letter password. The PIN and

OTP are encrypted using AES 256.Here the sensitive information of the user will not only be encrypted but also sent along with the image so that the intruder does not come to know about the hidden message.

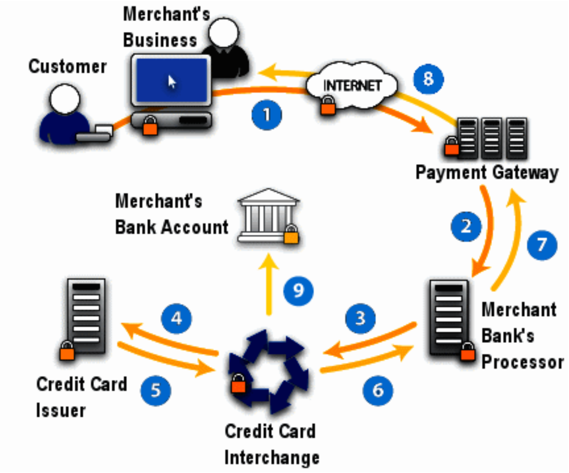


Figure 3. Transaction Process

Implementation of project:

The implementation of project is based on Java. There are two projects one for e-commerce & another is web service for account data. In e-commerce website once the account is registered, the user can buy the products & add to its cart to proceed further. After adding the products to the cart the user can remove the items if they don't want to buy it before payment. For payment user needs to provide their account details. The account details consist of account number, CVV & PIN number. The payment process is handled by the web service. The account details are encrypted using AES 256 and also encrypted data is sent along with the image so that the intruder does not come to know about the hidden massage. Then the encrypted & the steganographed data is decrypt & desteganograph with the same secret key and the details are compare with the user's data ,if the data input is correct then the payment get successful otherwise it will show the error.

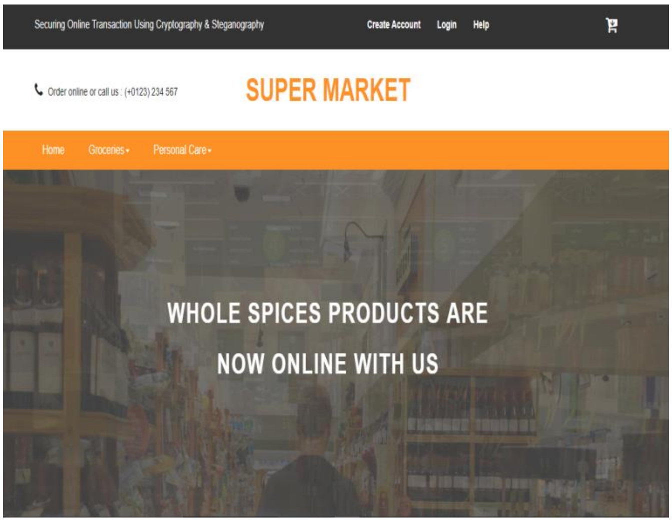
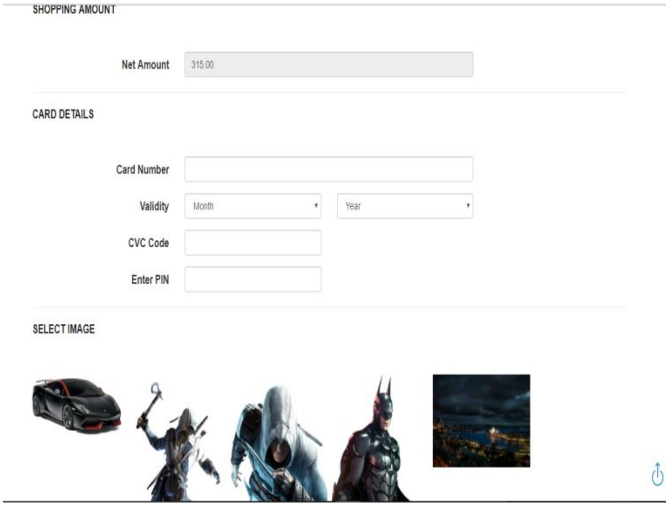

Securing Online Transaction Using Cryptography & Steganography
Create Account
Login
Help
Order online or call us : (+0123) 234 567
SUPER MARKET
Home
Groceries
Personal Care
WHOLE SPICES PRODUCTS ARE
NOW ONLINE WITH US

Figure 4. Homepage



SHOPPING AMOUNT

Net Amount 315.00

CARD DETAILS

Card Number

Validity Month Year

CVC Code

Enter PIN

SELECT IMAGE

Figure 5. Payment portal

VII. STEGANOGRAPHY CONCEPT

Steganography word comes from Greek which means "covered writing". In spy-craft, the steganography and cryptography both are related with each other .The aim of the steganography is transmitting a message on channel where some information is already being transmitted. It is a data hiding technique .The main goal of steganography is to hide message into the other message that the attacker does not even detect message because there is other message is present. The attacker can only detect the message by the secret key without secret key not even slightly chance of observing communication channel, because here the hidden communication takes place.

Steganography is very much important now a days because digital techniques allow hide the information into another information and it is valuable in many situations. Steganography and cryptography both are intended to protect the important information from the attacker or third party for this the expert suggest for giving the multiple level security to the transaction. Steganography is very much important in many fields like military, navy etc. in this place the secret information must be secure from the other parties.

VIII. STEGANOGRAPHY WITH CRYPTOGRAPHY

Nowadays our transaction is not secured from the third parties. They can steal the information and use it for illegal works. So the expert gave the concept of steganography and cryptography to provide the extra level of security to our transaction. Steganography and cryptography both are related to each other. Steganography hide the presence of message in video or image format and cryptography converts the original text into cipher text. We can say that steganography completes cryptography.

IX. CONCLUSION

This project is developed on the basis of more need of security in online transaction. Now a days online transaction is getting less secure with emerging ways to hack/ crack ATM PIN or ATM card. Here the combine technique of cryptography & image steganography is applied that provides customer data privacy & prevents misuse of data. The proposed method can be applied to the different E-Commerce & in physical banking.

X. REFERENCES

[1]. European ATM securityonline. Available :http://www.european-atm-security.eu/atm-industry.[accessed:12 November 2014].

[2]. N. Haller, C. Metz, P. Nesser, One-Time password system, RFC 2289, Feb 1998.

[3]. Secure Hash Standard (SHS), FIBS PUB180-4, March 2012.

[4]. D. Eastlake, P. Jones. A US secure hash algorithm 1(SHA1), RFC 3174, September 2001.

[5]. Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The Security of shopping online," Proceedings of 2011 International Conference of Electronic & Mechanical Engineering and Information Technology(EMEIT), vol.9,pp.4693-4696,2011.

[6]. Javelin Strategy & Research, "2013 Identify Fraud Report", https://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.

[7]. Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceeding of 1995 Conference Science & Systems, Johns Hopkins University, pp. 482-489, 1995.