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

Survey Paper on Securing Online Transaction Using Cryptography & Steganography

Nishi S. Mastkar[1], Mayuri R. Isankar[1], Farheen R. Sheikh[1], Dipali O. Singh[1], Swati Ramteke[2]
[1]Department of CSE, RTMNU/SRMCEW, Nagpur, Maharashtra, India
[2]Assistant Professor, Department of CSE,RTMNU/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 common dangers 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).

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. SURVEY

In the present era not only business but almost all the aspect of human life are driven by information. Hence ,it has become important to protect useful information from malicious activities such as attacks. Let us consider the type of attacks . Attacks are typically categorised based on the action performed by the attacker. An attack ,thus ,can be passive or active.

A. Passive attack

In passive attack the attacker only capture the information of system without affecting the system resources.

Passive attack are in the nature of monitoring of transmission . The term passive indicates that the attacker does not attempt to perform any modification to the data this is also why passive attacks are harder to detect.

There are two types of passive attacks

1.Release of message contents: In release of message contents opponents only can read the contents of message during the transmission.

2.Traffic analysis : In traffic analysis the opponent can determine the location and identity of communicating hosts and can observe the pattern of message , the frequency of message and the length and location of message but can’t modify it.

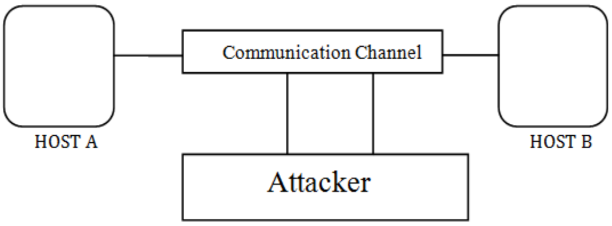

Figure 1. Passive attack

B. Active attack

In active attack the attacker can modify original information and send modified message to the receiver. During an active attack , the attacker introduces data into the system as well as able to change data within the system.

An active attack involve changing the information in some way by conducting some process on the information for ex.

This attack an be subdivided into 4 categories:

1.Masquerade: In masquerade one entity pretends to be another entity.

2.Replay: Attacker captures the message of sender and retransmit it to the receiver .

3. Modification of message: It involves capturing of data stream, altering it and then retransmitting it to the recipient to make an unauthorized effect. It may involve modification, deletion and reordering of data stream.

4.Denial of service: In this attacker disrupts service provided by server .

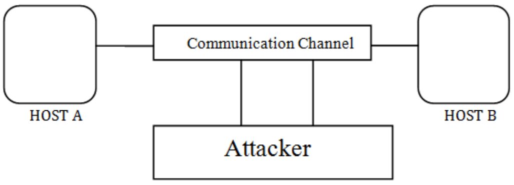

Figure 2. Active Attack

III. IMPORTANCE OF STEGANOGRAPHY

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 by 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.

IV. STEGANOGRAPHY AND 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.

V. 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 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.

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 .By crosschecking the OTP further payment is done. 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.

VII. 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. That OTP will be sending on register mobile number of the user and that OTP will be used to access online transactions. Here we will execute the techniques of cryptography & image steganography.

VIII. REFERENCES

[1]. European ATM security [online]. 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.