Secure Payment Gateway System for Electronic Transaction: A Review”

Manju Sharma[#1], Jaideep Atri[*2]
[1]manjusharmaknl@gmail.com
[*]Assistant Professor
S. A. Jain College, Ambala City
[2]jds094@gmail.com

Abstract*— Today Internet transactions have become an integral part. Online shopping by card is not new. From purchasing of goods to paying for them, using electronic payment methods such as credit card, debit cards are increasing day by day. These transactions involve exchange of information over internet but today internet is not a secure media. Therefore need of payment gateway arise to make these transactions more secure. Due to tremendous increase in online transactions, number of attacks has also increase. We need secure communication techniques, algorithms and protocols to protect the information being shared. This paper gives an overview of payment gateway system along with the methods and the protocols that ensures more secure electronic transactions.

***Keywords*— Payment Gateway, Security, SSL, SET**

I. Introduction

The buying and selling of goods over the internet is known as E-commerce or electronic commerce. The electronic commerce is not limited to simply buying and selling but paying for it through internet.

The ease of purchasing and selling goods over the internet has increased the numbers of internet transactions being made. Internet transactions provide a convenient and efficient way. These transactions are generally made through credit and debit card. Before making a transaction customer need to enter some confidential information such as Cardholder name, PIN, account related information. This information is send to merchant and is stored at merchant side server. Merchant may or may not exploit Customer but if merchant server is not secure enough attackers may be able to get the customer data for misuse.

We know the numbers of frauds related to internet transactions are increasing day by day. Therefore, here arise the need of secure system that not only provide secure transactions but also authenticates customer and merchant and privacy of customer and transaction data. We need payment method that would not send customer data to merchant side. Here arise the needs of trusted third party or payment gateways.

Payment gateways provide a reliable and secure way as they follow certain security rules and communicate with banks through secure communication ways and technologies. Payment gateways acts as a bridge between the merchant’s website and the bank that process the transaction

II. WORKING OF PAYMENT GATEWAY SYSTEM

An easy way Payment gateway acts as an intermediate between the merchant and the financial institution. Payment gateway passes the details in secure manner.

Terminologies used:

Customer: an entity that will buy products and services by making payment through internet.

Merchant: entity that will receive payment form customer and will deliver products to customer in return.

Merchant Bank: Bank in which merchant is having account. The customer order amount is transferred to merchant bank account after successful transaction.

Card issuing Bank: Customer Bank that has issued card to customer. Customer bank will validate the details of the customer.

Firstly, customer visits a website and chooses some products and services he wants to buy. As soon as the customer places a n order, the details such as order amount and IP address of the customer along with the digital signature is send to payment gateway in encrypted form.

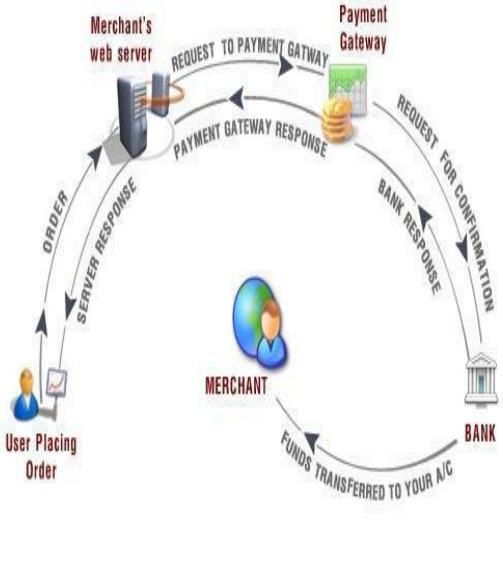

Fig1. Payment Gateway

Payment gateway will ensure the merchant site on the basis of digital signature. Payment gateway will show various payment options to the customer. On choosing the desired payment option, it sends the order details to the merchant's bank and merchant bank will contact card issuing authority of the customer. Bank then checks for the customer details and the order amount, bank can either reject or accept the transaction. Sometimes, bank rejects the transaction if there is not sufficient balance in the customer account .If details of the customer are verified then an bank response is generated for the payment gateway and the payment gateway will generate the receipt for the same .

Merchant website can now deliver goods to the customer. This whole process is actually very fast and all the information is send in encrypted form through secure network.

Payment Process takes place in two phases:

- **Authorization** (getting approval for the transaction that's stored with the order).

Any purchase made with a credit or debit card via a payment gateway must first be authorized by the credit card issuer. The payment gateway checks that the credit card is acceptable. The gateway affords you a secure link between you, your customer and your credit card processor. It also allows for fast and efficient transaction processing with an average response time of 2 seconds.

- **Settlement** (processing the sale, which transfers the funds from the issuing bank to the merchant's account).

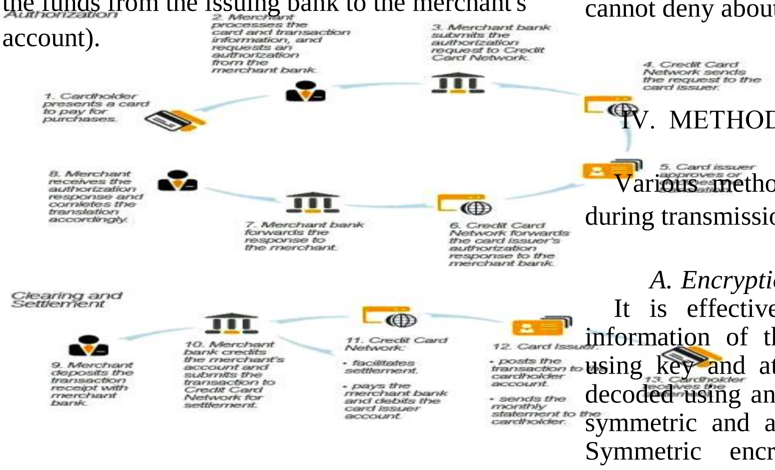
Authorization
1. Cardholder presents a card to pay for purchases.
2. Merchant processes the card and transaction information, and requests an authorization from the merchant bank.
3. Merchant bank submits the authorization request to Credit Card Network.
4. Credit Card Network sends the request to the card issuer.
5. Card issuer approves or
6. Credit Card Network forwards the card issuer's authorization response to the merchant bank.
7. Merchant bank forwards the response to the merchant.
8. Merchant receives the authorization response and comletes the translation accordingly.
Clearing and Settlement
9. Merchant deposits the transaction receipt with merchant bank.
10. Merchant bank credits the merchant's account and submits the transaction to Credit Card Network for settlement.
11. Credit Card Network:
• facilitates settlement.
• pays the merchant bank and debits the card issuer account.
12. Card Issuer:
• posts the transaction to the cardholder account.
• sends the monthly statement to the cardholder.
13. Cardholder receives the

Fig2. Payment process

At the end of the day, the Internet payment gateway groups all of your transactions together and sends them off to your bank in a single batch. This process, known as settling, passes the transaction to your bank so that you receive payment. Once the funds settle, it normally takes two business days for you to see the funds electronically deposited into your bank account.

III. REQUIREMENTS OF A SECURE PAYMENT SYSTEM

The most important requirement is to secure the credentials entered by customer. Attackers are able to intercept the information sent and can misuse it. To avoid this we need to consider some features that must be provided by payment system.

A. Data Confidentiality:

Data confidentiality implies that data entered by customer is safe and is kept confidential so that no one can misuse it.

B. Data Integrity:

Data integrity means during the communication process when data is send from merchant to gateway it needs to be same as entered by customer .there must be ways to check that data is not modified in between.

C. Authentication:

Authentication means verifying the customer before allowing him to make a transaction. This can be done by means of passwords, finger prints.

D. Non Repudiation:

It implies the assurance that the customer cannot deny about order placed or receipt received in return. Once a message form customer is sent to merchant, he cannot deny about the message.

IV. METHODS TO ENSURE SECURITY

Various methods can be used to ensure security during transmission:

A. Encryption:

It is effective way to secure the confidential information of the customer. The data is encoded using key and at the receiver side encoded data is decoded using another key. Encryption is done using symmetric and asymmetric cryptography technique. Symmetric encryption involves same key for encryption as well as decryption but in asymmetric key cryptography public key is used to encrypt and private or secret key to decrypt the encrypted information.

B.Digital Certificates:

It is used to authenticate the customer that he claims to be. Digital certificates ensure the secure transmission and avoid leaking of information .Digital certificates includes digital signatures that cannot be changed by the attacker .These are digitally signed by trusted certificate authority.

V. SECURITY PROTOCOLS

Various security protocols used are:

A. SSL(Secure Socket Layer)
B. SET(Secure Electronic Transaction)

A. Secure Socket Layer (SSL)

SSL stands for secure socket layer and was designed by netscape. It provides a secure medium for exchange of information on internet. It is most widely used protocol that provide a secure communication between browsers and the websites we visit .It ensures that both the end user and the website are legitimate not attacker .The information exchange is in the encrypted form. Sites that are secured have a padlock in the browser URL .Data transmitted through these sites remain confidential. When a site is having extended validation certificate than the address bar is green in color. This can be seen during credit card payment.

SSL certificate is issued by CA (certificate authority). Certificate authority issue certificate to sites after ensuring completely about the applicant .When an transaction is done the browser first checks for certificate ,if the websites is secured by SSL then the user is proceeded to pay else the browser warn the user that the website is not trusted .

Certificates issued by authority has the details like domain name , company name , issuing date and the expiry date .Along with all this it also contains details of the issuing authority.

SSL use two important protocols:

SSL HANDSHAKE PROTOCOL: An SSL handshake protocol initiates the communication by authenticating client and server. First, client sends a request to server, in respect to the request generated by client, server response back to the client and a connection is established.

SSL RECORD PROTOCOL: SSL record protocol provide security to the information being transmitted .The information exchanged in the network is passed to server in encrypted form.

SSL provides authentication of client and server along with it authentication to the communication channel between them.

VI. Problems With SSl

SSL provide secure connection but there are some problems associated with SSL also. There are many certificate authorities and some of the authorities issue certificates without even verifying properly about the website.

SSL provide secure communication link between the merchant and the customer but there is no assurance that the merchant will not misuse the customer credentials.

SSL ensures authentication of merchant but does not ensure about the authentication of customer. Some illegitimate user can use information of customer to make a payment.SSL cannot identify those transactions being made.

B. Secure Electronic Transaction (SET)

SET is open protocol used for transaction over insecure network. SET uses cryptographic technique and digital certificates to ensure integrity, confidentiality of information. SET protocol provides high security. It authenticates the customer before proceeding for a transaction

.It ensures data integrity and confidentiality of transmitted data. It ensures secure connection not only between buyer and seller but also between all the parties involved in communication. It provides more security than SSL. Various participants involved in SET protocol are:

A. *Cardholder*: The customer who uses card for making payment.

B. *Merchant:* Merchant is seller from which the customer is purchasing goods.

C. *Issuer:* Issuer is the bank who issued card to the customer.

D. *Acquire*: Acquire verifies the payment made by the customer. Payment gateway: is the medium through which customer pays for the services and goods he has purchased from the merchant.

E. *Certificate authority*: CA is the authority that issues certificates to merchant, card holder and payment gateway.CA ensures that the merchant, cardholder and the payment gateway are legitimate.

F.

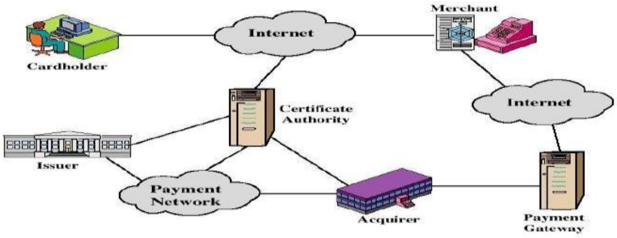

Fig3: Participants involved in SET protocol

VII. ATTACKS ON INSECURE PAYMENT SYSTEM

A. Snooping attack: The attacker monitors the network to retrieve information like user IDs and passwords shared through that network.

B. Spoofing attack : In this attack , the attacker tries to fool the computer by pretending that it is legitimate user.One type is IP spoofing in which attacker fake the IP address such that it seems to come from a location that it is not actually from.

C. Tampering attack: This attack is basically on the integrity of data. During the transmission, attacker tries to modify the data.

D. Hijacking attack: Attackers tries to hijack the connection after the successful authentication by the legitimate user.

E. PIN guessing attack: In this, attacker performs the attack by faking the digits or guessing the digits.

F. Capture replay attack: Attacker can record the transaction and can modify the data and can replay the transaction. Attacker can also do price manipulation in captured transaction.

VIII. CONCLUSION

E-commerce is increasing day by day. Nowadays people prefer to buy and sell goods online by making an online payment. While paying for goods, customer enters some details that need to be kept confidential. To maintain confidentiality, we use various cryptographic techniques and protocols that ensure security of customer data.SSL and SET ovide secure ways to maintain the integrity and confidentiality of data. We need to improve the techniques to ensure more security so as to avoid data being retrieved by the attackers.

REFERENCES

[1]. Rahul Kumar and Ajit Pratap Singh ,Arun Kumar Shukla " The Role of SSL and SET protocol in E-Commerce" in international journal of advance research in computer and communication engineering Vol.4, issue 9, September 2015.

[2]. Ajeet Singh, Karan Singh, Shahazad, M.H Khan and Manik Chandra "A Review: Secure Payment System for Electronic Transaction" in International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 3 , March 2012 .

[3]. Mr. Pradeep Kumar Panwar , Mr.Devendra Kumar " Security through SSL" in International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 12, December 2012.

[4]. Atul Kahate, "Cryptography and network Security", 3edition, TMH publications, 2013, ISBN 10: 1259029883 / ISBN 13: 9781259029882.

[5]. William Stalling, "Cryptography and Network Security", 4th edition, Prentice Hall Publications, 2005, **ISBN**-13: 978-0-13-187319-3.