International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 12, December - 2013

A Review: Payment Gateway

Rishabh Bhasin
Student
Northern India Engineering College, Shastri Park

Kshitiz Gupta
Student
Northern India Engineering College, Shastri Park

Udit Gandhi
Student
Northern India Engineering College, Shastri Park

Mrs. Bharti Goel
Assistant Professor
Northern India Engineering College, Shastri Park

Abstract

In this paper, we explain the working of a payment gateway. The payment gateway provides a link between the Bank Account and the Merchant's account. For validating and authenticating the online transactions that are made when you go on an online shopping site. Thus it actually is an e-commerce application service provider service that authorizes payments for e-businesses, online retailers. Thus it acts like a check post which the customer shall pass so on to make his transactions well versed. If you compare the payment gateway to a normal point of sale check post, thus this analogy can be made b/w them. In our paper we study about the encryption and decryption methods which a payment gateway generally uses while it sends the credit card details to the browser. So the payment gateway makes a hit on the bank's database if the conditions are met and satisfied the payment is made and the customer gets the product. So our paper is all about the study of payment gateway.

1. Introduction

E-Commerce or online shopping is done by a credit card or a debit card. Nowadays when people are always on the go and busy with their lives so they hardly find time to shop in the marts. As a result they prefer to shop online. So when you go

Fig 1. Payment Gateway as a Black Box

On a website to purchase anything, you select the items you want and after that you add the items to the cart. So when you proceed to pay the payments you are redirected to a secure SSL encrypted page and then the Payment Gateway. So then the browser sends the encrypted format to the payment gateway. So now when you enter your credit card details the Payment Gateway first checks that whether the Merchant's account is valid or not, if it's valid then it proceeds to the next step, where it checks that the customer who's purchases the goods has a legal and a valid bank account to make the transactions. If the bank account details are legal and the customer has the minimum amount needed to make a transaction. So if all these check posts are met then merchant's account is legal and customer has a valid account with the minimum balance thus if the conditions are met, then the Transaction is made and all this is authenticated and secure. The credit card details are encrypted and everything remains safe as the 128 bit Encryption is used here, whole of this process takes just a few SECONDS. So thus it works like that, customer adds the items to his cart he is redirected to a page and the link of redirection is encrypted and sent to the page where you have to enter the credit card details, thus

when you click on the proceed to pay button payment gateway performs its function and makes a hit on the bank's database if hit is successful then the transaction is done, if it is not the valid message is delivered to the customer citing the reasons as to why the payment couldn't be completed.

.

2. Main Text

2.1. **Working**

Working of the payment gateway is very simple procedure. To start of with this, think of payment gateway as a black box, when you enter your credit/debit information, the things are processed , conditions satisfied and everything inside the black box, so if the conditions are true then transaction process is successful else the transaction process is unsuccessful. To verify the payments the credit cards and the user information it just takes 1-4 seconds. Payment gateway actually ensures that customer has enough funds i.e. Minimum balance to make a transaction and the merchant's bank account is legal and verified. If all these conditions are met then transaction is successful else it is not. Here SSL encryption is used (128 bit SSL).

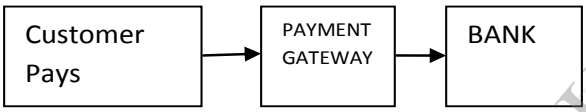

Fig 2. Showing Payment Gateway

3. Encryption

Transferring information over the network forms the basis of internet. When it comes to online payment it is necessary to keep in my mind that important information like transaction details is secured from the third party and security breach is not the case. For that we have this amazing technology called cryptography which is being used from the ancient times for example like Julius Caesar used to encode his confidential letters by shifting the alphabets so that nothing could be made out of that letter by enemies. Cryptography is the beautiful art of protecting information by encrypting the plain text into unreadable format. This unreadable format is known as cipher text. People who have got that secret key to decode the cipher text can only decrypt and read the secret information. Secure sockets layer (SSL) protocol created by Netscape Inc has become one of the famous encryption methods to secure information over the unsecured network called Internet. It is now being implemented in most of the web browsers. This protocol ensures the security of the confidential information by encrypting data that is transferred between user and client. This protocol also uses RSA algorithm to provide authentication of the session partners. The SSL protocol is further divided into 2 layers known as SSL handshake layer and SSL record layer.

SSL Handshake layer: This layer is divided into 3 sub protocols namely Handshake Protocol, Change Cipher Spec Protocol and Alert protocol. This layer helps establishing authentication between the two parties which then negotiate an encryption key

SSL Record layer: This layer helps exchanging session data between the communicating parties which are the client and the server in an encrypted fashion SSL is a great advantage over the traditional protocols as it makes it cushy to add confidentiality and integrity services to an otherwise insecure TCP based protocol. The best part is client can determine if they are talking to intended merchant or not. SSL transaction initiates with a handshake which is sent by the client to the merchant which is done for authentication. In return server sends its certificate. Certificate includes: public key associated with server, expiration date, owner of the certificate, domain name. On its flipside there are some limitations with this protocol. Though it is an excellent protocol but being a tool it is effective in one hand but can be misused easily by some other hand. The merchant or server cannot reliably identify fake users who uses stolen card to start online transactions.SSL does protect the communication link between merchant and client but the merchant is allowed to see client's payment information. There is no guarantee that merchant will not misuse that information. SSL encrypts all the communication data using the same key strength which is not necessary as all the data doesn't needs same level of protection. ***[1], [2]***

4. Decryption

Decrypting the data or the information means to retrieve the data back which was sent as the encrypted data. Thus decryption and encryption both are used just to protect the important credit card details and the bank account details from the fraudulent activities and thus provide the customers a sense of security, over the site. Thus to make this very online shopping experience safe authenticated and good in all respect we encrypt and decrypt the credit card information and other sensitive information that is required for processing the payments over the internet. We use private key decryption algorithms. How it works actually is that the credit card information is encrypted and sent to the payment gateway web server, thus payment gateway checks the account balance authenticates and verifies payments, thus it generates a hit on to the bank database, if the hit turns out to be positive then the message is decrypted and sent to the payment gateway web server and this the message from the payment gateway web server then decrypts the message and sends it to the customers bank which then encrypts the message and receives the confirmation message, thus this is how encryption and decryption works hand in hand. Transferring of information securely and efficiently is done since ancient times to protect information from third parties called adversaries. When it comes to online payments using payment gateways, it is really necessary to protect the sensitive information of users from hackers online. This is done with a beautiful art know as cryptography. Cryptography is the process of protecting information by encrypting the plain text into unreadable format. This unreadable format is known as cipher text. Decryption is the reverse operation of encryption. For secret-key encryption, you must know the key that was used to encrypt the data. Decryption of the cipher text to plain text can only be done if the decoder has the secret key which has been set by the encoder to encrypt the data. The encoder of the encrypted data or the cipher shares the decoding technique or makes it public in order for it to make it possible to get back the original data also called the plaintext. Secure socket layer (SSL) protocol created by Netscape Inc. is now been used by most of the browsers to encrypt data on one of the most unsecure network, internet. SSL is a great advantage over the traditional protocols as it makes it cushy to add confidentiality and integrity services to an otherwise insecure TCP based protocol. The best part is client can determine if they are talking to intended merchant or not.SSL transaction initiates with a handshake which is sent by the client to the merchant which is done for authentication. In return server sends its certificate. Certificate includes: public key associated with server, expiration date, owner of the certificate, domain name. On the other hand, it has some disadvantages too, such as: The merchant or server cannot reliably identify fake users who uses stolen card to start online transactions, SSL encrypts all the communication data using the same key strength which is not necessary as all the data doesn't needs same level of protection, etc.

Taking control of your SSL and SSH encrypted traffic and ensuring it is not being used to conceal unwanted activity or dangerous content is done using policy-based decryption and inspection. Using this you can confirm that SSL and SSH are being used for business purposes only, instead of to spread threats or unauthorized data transfer. ***[1]***.

5. Mobile Payment Gateway

Mobile Payment Gateway is well an alternative to the standard payment gateway as many people consider paying with their credit cards as unsafe mode of payment transaction as they fear that the sensitive information like credit card details and their personal information can be hacked or leaked by the third party. So Mobile Payment Gateway comes to the play now, here instead of credit card you can use your mobile phone as a term of credit. For example when you go on your choice list you are directed to pay so then you are redirected to any online shopping site then after you select the mode of payment that is via the credit or the debit card, now here lies the point. Most of the buyers feel insecure of entering their sensitive credit card and personal details fearing that they may be scanned by the hackers or anyone doing the illegal activities. So in that situation when you use your Mobile Phone as they means of paying the money thus the cost of the thing being deducted from your prepaid mobile balance. Thus this use of mobile phone instead of the credit or debit cards, this terminology is called the Mobile Payment Gateway. Mobile Payment Gateway has it's certain merits and demerits. Its merits can be that the transaction payment and all the other activities can be performed faster as there is no need to enter your credit card details.So all the authentication and verification

and transferring of funds in done within a second or two. Thus it can be integrated by standard easy API's very easily. Its demerits can be well it may be a faster method but it may not ensure full security over the internet. ***[2]***.

5.1 Types of Mobile Payment Gateway

Card based mobile payments – using mobile as the credit card.[1]

Card based payment acceptance. The card based payment includes the models where cards are used which are of different types and different geography cards are used for payments.

Contactless card based mobile payments –Deals with Near Field Communication Technology [NFC]

Cardless mobile payments – Includes cardless payments like with the use of mobile wallets [2]

Carrier Billing –Paying the payments via the operators balance, that is by the use of prepaid balance, considered safe by the users as it doesn't require the use of credit cards.

6. References

[1] Ailya izhar, Aihab khan, Malik Sikandar Hayat Khiyal, Wajheed Javed, Shiraz Baig, in Article named "Designing and Implementing Electronic Payment Gateway in Developing countries" published in "Journal of theoretical and Applied Information Technology" vol. 26 no. 2 which can be found on the site www.jatit.org.

[2] Ajeet singh , Karan Singh , Shahazad , MH khan. Manik Chandra in Article named " A Review: Secure Payment Transaction System for Electronic Transaction" published in "International Journal of Advanced Research in Computer Science and Software Engineering" Vol. 2 Issue 3 march 2012 which can be found on the site www.ijarcsse.com