WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Design and Development of a Secured Transaction of an E-Commerce Application

Mrs. Divya Uchil

Department of Computer Application, S.D.M. College of Business Management, Mangaluru-575001, India
DOI: https://doi.org/10.55248/gengpi.5.0324.0832

ABSTRACT

A dedicated team makes sure that the Information technology team brand grows from strength to strength. Digital marketing has developed and has changed the way brands and businesses utilize technology and digital marketing for their marketing. It is becoming more prevalent as well as efficient, as digital platforms are increasingly incorporated into marketing plans and everyday life, and people use digital devices for shopping purposes. Security of online electronic transaction is major issue in today's life which needs to be taken care of. Various methods are proposed for the security of online transaction but it may fail in one or the other way. Secure Electronic Transaction (SET)protocol is one among them. The operation of SET depends on software that implements a series of protocols installed in the workstations or servers of four kinds of people and organizations. These are Cardholders (Buyer) Merchants (Seller), Payment gateways/acquirers, Issuer. The objective of the paper is to design a secured application for digital transaction.

1. Introduction

In the digital era ,the digital marketing allows brands to market their products and services 24/7. Customers online feel supported and valued. It is so pervasive that consumers have access to information any time and any place they want it. It is an ever-growing source of entertainment, news, shopping and social interaction. The consumers are now exposed not just to what company says about the brand. People now want brands they can trust upon , companies that they can rely upon, communications that are personalized and relevant. Here security of data plays an important role.

Data security has taken on heightened importance because of a series of high-profile "cracker" attacks that have humbled popular Web sites. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. Technologists are building new security measures to prevent hacking while others are working to crack the security systems. Encryption is one of the most effective means of ensuring data security and integrity .

II. LITERATURE SURVEY

The Internet is changing the way that goods (tangible and intangible) and services are produced, delivered, sold, and purchased. The trade on the Web has comes an essential requirement for enterprises because of the fast development in digital technologies. The e-commerce to m-commerce technology which has become a major service nowadays, every enterprise works hard to find out a way to sell and buy that can satisfy its requirements.

1.1 E-commerce security requirements

The use of e-commerce systems has growing at a phenomenal high rate. A large spectrum of products (tangibles and intangibles) is sold on the Internet, with payments made essentially by debit or credit cards. Because of online transactions there is an increasing concern related to the security of the payment systems used to process the data .Confidentiality of payment card information due to disclosure of this information to malicious adversaries could enable them to perform fraudulent transactions at the customer‘s expense

1.2 General form of the e-commerce process

Payment transaction model has the interactions of four roles:

Payer – The payer is an authorizer of a payment means supported by an issuer. Ordering a payment may be done using a card, a token, or a certificate. The payer is the customer or buyer in an electronic commerce scenario.

Payee – The payee is a merchant providing goods, services, and/or information and receiving electronically the payment for something purchased by the payer. Usually, the payee is simply referred to as the vendor, merchant, or seller in an electronic commerce scenario.

Issuer – The financial instrument that supports issuing payment cards (or means) by using cryptographic technologies which guarantees the association with ―real money. Its role is to provide the payer and the payee with instances of monetary value which are used in payment protocols to transfer ―real money from the payer to the payee.

Acquirer – This is a financial institution (a bank, for example) which transforms the cryptographic objects involved in the payment into ―real money on behalf of the payee

1.3 Security Requirements

The security requirements vary from one role to another. However, it appears that acquirer and issuer have very close requirements. In the following we examine individually the requirements of each role. Client Transaction confidentiality, especially the information occurring in the payment card, is a major security needed for a client which gives them the security. The nature of the transaction may require confidentiality. Various security protocols have been developed for e-commerce. The major protocols include:

1. The Secure Socket Layer (SSL) protocol: It is used to provide secure communication between Web browsers and Web servers.The SSL provides server authentication, data integrity, and client authentication.

2. The Transport Layer Security (TLS) protocol: This was introduced by the Internet Engineering Task Force

3. The Secure Electronic Transaction (SET) protocol: It facilitates secure electronic commerce transactions and provides confidentiality of payment card information, data integrity, authentication of both merchant and cardholder, and authorization of transactions.

4. The 3-D Secure Protocol. This has been developed by Visa .It provides cardholder authentication for merchants using access control servers and the Visa Directory Server.

1.4 Transaction security with SET

Once registration is done, the cardholder and merchant can perform their transaction, which have five steps to be followed in this protocol:

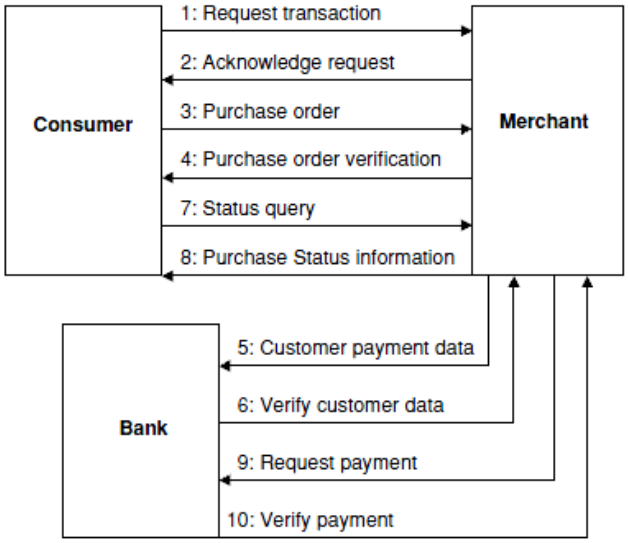
1. The customer browses the website and selects the goods to purchase. Then the customer sends the order and payment information, which includes two parts in one message: the purchase order (say part a) and the card information (say part b). While the former information part is for the merchant, the latter is for the merchant‘s bank only.

2. The merchant forwards the card information to its bank to check with the issuer for payment authorization.

3. On receipt of the authorization from the issuer, the merchant‘s bank sends it to the merchant.

4. The merchant completes the order, sends confirmation to the customer and then captures the transaction from his/her bank.

5. The issuer finally prints a credit card bill (or an invoice) to the customer. SET relies on cryptography and digital certificate to ensure message confidentiality and security. Message data is encrypted using a randomly generated key that is further encrypted using the recipient‘s public key.



1. The customer needs to opens an account .The customer will obtain a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.

2. The customer receives a certificate. After verification of documents like identity, the customer receives an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer‘s RSA public key and its expiration date. It also establishes a relationship, guaranteed by the bank, between the customer‘s key pair and his/her credit card. A merchant who accepts a certain variety of cards must be in possession of two certificates for two public keys: one for signing messages and one for key exchange. The merchant needs a copy of the payment gateway‘s public-key certificate.

3. The customer places an order .This is a process that may involve the customer first browsing through the merchant‘s Web site to select items and determine their prices. The customer then sends the list of the items to be purchased from the merchant, who returns an order form containing the list of items, their individual prices, a total price, and an order number.

4. The merchant is verified. In addition to the order form, the merchant sends a copy of his certificate, so that the customer can verify that he/she is dealing with a valid store.

5. The order and payment are sent The customer sends both an order and payment information to the merchant, along with the customer‘s certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer‘s certificate enables the merchant to verify the customer.

6. The merchant requests payment authorization The merchant sends the payment information to the payment gateway, requesting authorization that the customer‘s available credit is sufficient for this purchase.

7. The merchant confirms the order. The merchant sends a confirmation of the order to the customer.

8. The merchant provides the goods or service. The merchant will now ship the goods or provides the service to the customer.

9. The merchant requests payment .This request is sent to the payment gateway, which handles all of the payment processing.

1.5 Securing Electronic Payment

The objective of an electronic payment system is to transfer a monetary value from the payer to the payee by using a payment protocol and a financial institution or network which links the exchanged data to real world value. The financial network may be built of individual financial institutions (i.e., banks or authorized service providers). Five key phases can be identified in a commercial transaction

1. Getting means of payment -This phase entails using the appropriate means of paying for objects and obtaining digital cash in a given currency.

2. Service discovery -During this step, the client discovers the available services and selects one or some of them based on a set of factors including price.

3. Payment negotiation -When an e-service has been selected by a customer, the client can negotiate payment based on specific parameters such as payment means and authentication mechanism.

4. Service utilization -During this phase, the customer utilizes the selected service, while making on-going payments.

5. Termination -This phase includes the action performed after the utilization of service has ended. Actions involve reclaiming any unspent money or obtaining a proof of payment and service use.

III. PROPOSED SYSTEM

In proposed system only certified sellers and buyers can participate, this will ensure the security because only legitimate users will be able to take part in the online electronic transactions. Sellers and buyers will be certified by the certifying authority. Certifying authority will certify the user when user may be seller and buyer wants its certification to participate in the transactions. The username or passwords which the buyer enters may be credit card number or online banking username and password should be secure and no one else should be able to read the sensitive information hence we use multiple encryption scheme for the security of information. We also check for the hacking or attacks on the e commerce application and the sensitive information sent over the network.

Certification of Entities Participating in the Transaction:

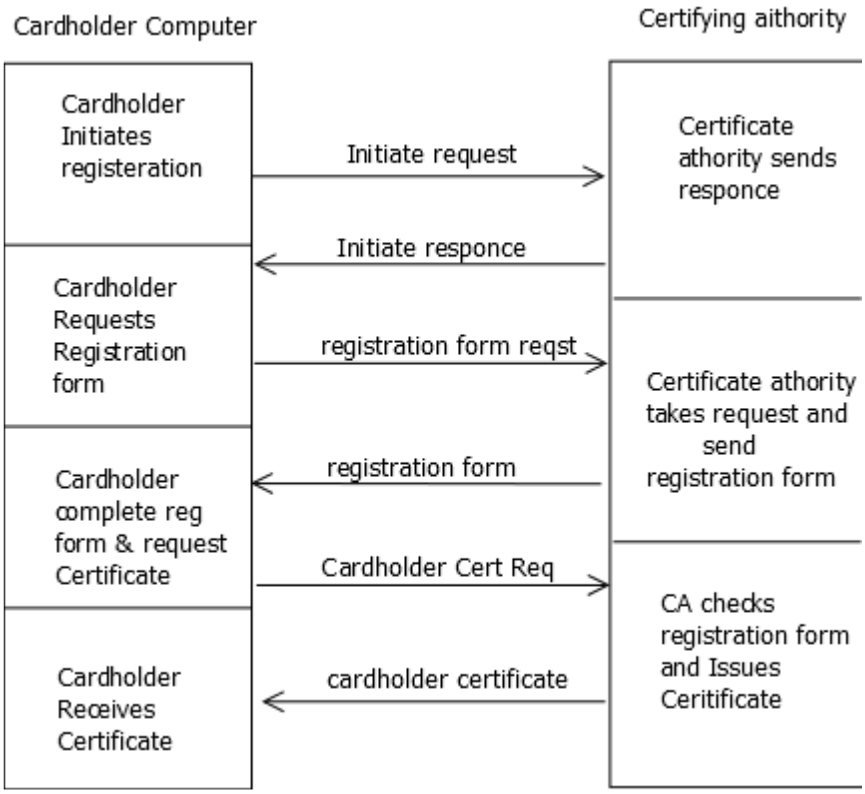
Everyone normally pay for goods purchased over the Internet by giving the merchant their credit card details. To prevent this information from unwanted people from stealing the card number, the message undergoes a session of the secure sockets layer (SSL) protocol. In this arrangement the cardholder and merchant should trust each other. That requirement is undesirable in face-to-face transactions, but over the internet it has many risks.

- The cardholder is protected from eavesdroppers but not from the merchant itself. Some merchants are dishonest. They do not protect the sensitive information.

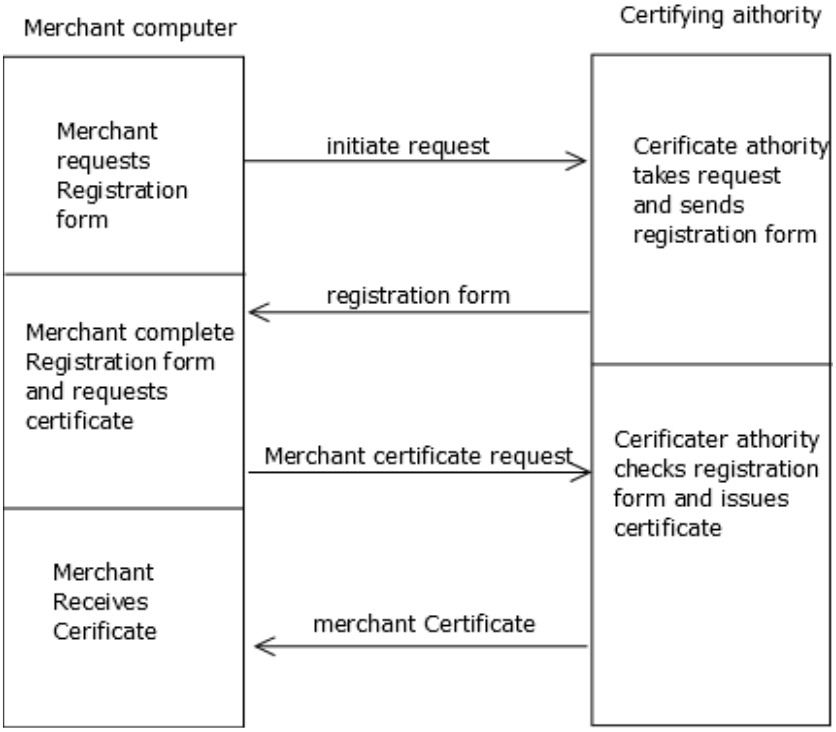
- The merchant also needs to be protected and should have some protection against dishonest cardholders who supply an invalid credit card number.

The card holder needs to be also be protected as in many countries the law protects the cardholder. The aspect of registration of merchant as well as cardholder is dealt with here. The First figure shows the registration of cardholder ,the second figure shows the registration of merchant.

Card Holder Registration



Merchant Registration



Encryption of Sensitive Information Using Multiple Encryption .

The model of sensitive data transfer secure(SDTS) provides the following benefits. Firstly, this makes the system more complex because the changes made are at byte level and thus, it is very difficult to predict by the hackers that what exactly is happening. Secondly, this provides tightly coupled security because the complexity of the system is increased to larger extent. It encrypts the bytes using standard RSA algorithm. With reference to the online transaction processing apps, the information to be processed is not sent over the network in unsecured manner, but a security key corresponding to the information is picked from database table to secure the real time data or information from being exposed on the network or to the people who are not intended to view it.

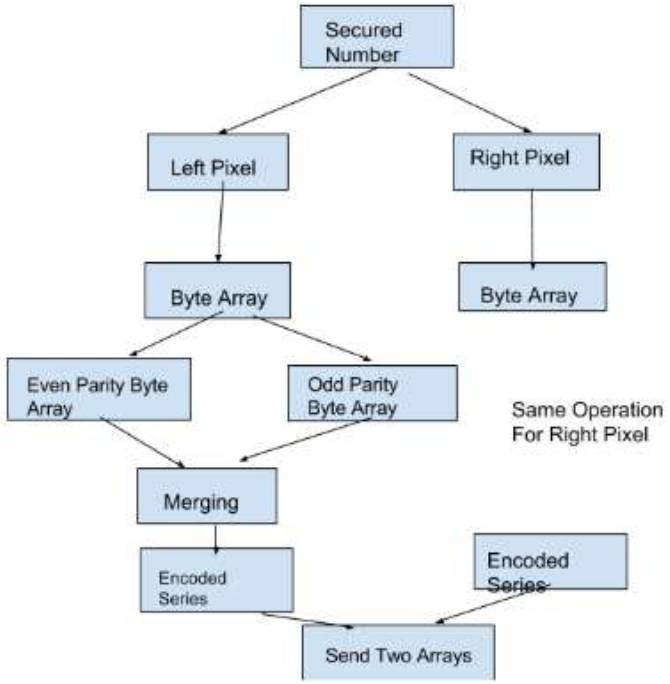
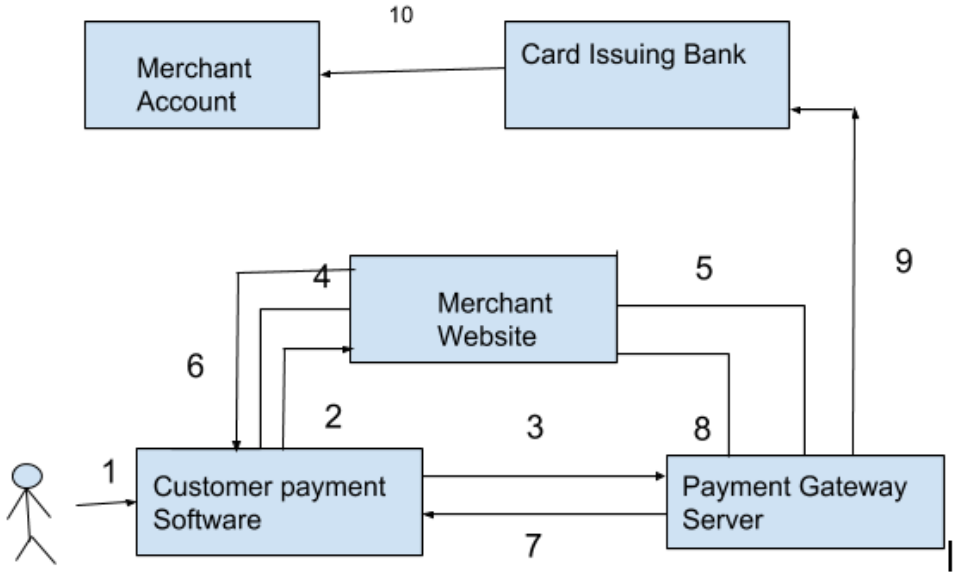


Diagram of the proposed System



Algorithm

1. Customer starts Ol-pay on his terminal. He is then prompted to enter a secret password to further access the system.

2. After successful entry of the password, customer opens the Ol-pay browser where he visits the merchant‘s website and places the order.

3. The OLTP system in the Authentication module of Ol-pay synchronizes itself with the payment gateway server (GS).

4. An request Detail, RequestDet is created automatically by the software and encrypted using the public key of the payment gateway

5. Merchant sends the received RequestDet to GS. GS after verifying the customer notifies the merchant about authenticity of the customer.

6. Merchant then creates a transaction bill, TranBill which is: TranBill = EnCrypt [(Merchant ID ,Merchant‘s Acc. No. , Payment details)]

7. Customer verifies the order information .The Authentication module of the software sends T_ID obtained of the merchant to GS for merchant authentication.

8. GS sends T_ID to the corresponding merchant and merchant in turn sends the TranBill to GS. GS decrypts the TranBill using merchant‘s public key and authorizes the merchant and notifies the customer of merchant‘s authenticity.

9. GS then sends payment details and customer‘s details to the issuing bank.

10. Issuing bank after verifying the payment due with the credit card limit of the customer transfers the requested funds to the merchant‘s account and both, the customer and the merchant are notified of the transaction status.

IV. CONCLUSION

The proposed System ensures the privacy and the security of data, which in turn affects costumers trust in electronic transaction. It encrypts the data at the byte level seeing towards that all transactions are secured making the digital marketing reliable.

References:

[1] Model Checking for E-Business Control and Assurance Bonnie Brinton Anderson, James V. Hansen, Paul Benjamin Lowry, and Scott L. Summer

[2] Provably Secure Integrated On/Off-Line Electronic Cash for Flexible and Efficient Payment Chun-I Fan and Vincent Shi-Ming Huang

[3] Verifying the SET Registration Protocols Giampaolo Bella, Fabio Massacci, Member, IEEE, and Lawrence C. Paulson

[4] E. Clarke, O. Grumberg, and D. Peled, Model Checking. Cambridge,MA: MIT Press, 1999.

[5] Comments on the Security of Fast Encryption Algorithm for Multimedia (FEA-M) A. M. Youssef, and S. E. Tavares, Member, IEEE.

[6]Baldinger, A. & Rubinson, J. (1996) “Brand Loyalty: The Link Between Attitude

and Behavior,“ *Journal of Advertising Research*, 36 (6): 22-35.

[7] Dick, A. & Basu, K. (1994) “Customer Loyalty: Towards an Integrated Conceptual Framework,” *Journal of the Academic Marketing Science*, 22(2): 99-114.