Ecommerce Transaction Security Challenges and Prevention

Methods- New Approach

N Priya, J Sridhar, M Sriram

Dept of CSE, Bharath University, Chennai

*Corresponding author: E-mail: priya_n@gmail.com

ABSTRACT

Nowadays technology grownup fast, ecommerce becomes the most used one in globalized business. In web business world, standard security methods are used to satisfy the basic things of online transaction. For many years research efforts are made for the customer merchant trade systems. Fraud detection models prevent the frauds and protect the merchants and customers. An existing fraud detection models are checking the merchant integrity in the transaction system of ecommerce. Some rules are defined to prevent the fake online stores. In India rural side people are not believing the online banking. So there should be a simple reliable and an easy to handle ecommerce system for all levels of people. So we proposed a secured architecture for online banking. We proposed a new Multi Authentication E-commerce Model which is acceptable by online customers.

KEY WORDS: Ecommerce, Mobile banking, Fraud prevention, online banking.

INTRODUCTION

Electronic commerce, otherwise known as e-commerce, is the kind of business transactions through the Internet or telecommunications technology. It involves the buying, selling or exchange of goods, services, and information through electronic networks. Ecommerce means all business transactions are done by web, it is conducting in a grand manner then it is called business. The essential components of ecommerce are Business and Consumer.

Most of the internet users buying the goods from internet by their credit card or debit card via a secure form. The debit/credit card is the essential thing used by consumers to buy products through internet. If any issues occur then it became a serious problem. so mode of payment must be a secure one. This payment system should be highly efficient, secured and fastening the process of transactions. So we proposed a secured transaction protocol for e-payment transactions. The e-commerce fraud prevention models are used not only for protecting the virtual store and goods also used to prevent theft identity and usage of fake credit cards. Also it should be able to find out online fake merchants. So a survey is made to analyze the merchant’s physical location that is known to customer. Hence, a component, which increase customer’s trust and confidence online through authentication and differentiate fraudulent virtual stores.

Essential security considerations for e-payment from:

Confidentiality: The information that required for online transactions should be kept confidential. If the user name and payment information is stolen by another business competitors then there loss in customers. So in e-commerce encryption is required for transferring information.

Data Integrity: E-commerce must give the medium for integrity. Also it confirms the internet didn’t allow any alteration in transmitting the data.

Authentication of participants: The participants first to find out the main two things which are essential for transactions.

Non-repudiation: The transaction should found the repetition of other activities like, confirming the purchase orders and the mode of payment. For this action we need both customer and the seller.

End client necessities: Different conventions including simplicity adjustability and operations between the seller and customer.

Ease of use: The system must be very simple and easy to handle for customers. Meantime they required a secured transaction and safety methods that give a protected application

Flexibility: The system must allow the customers to order things from any place like various internet resources. The customer require an adaptability organization, while the merchant is the substance giving the organization.

Reasonableness: The price of realizing and using the utility, what suitable for customers and merchants, since these end-users are unlikely to be prepared to pay significantly extra to participate in Internet e-commerce transactions. For example, consumers won’t pay registered certificate in order to conduct e-commerce transactions. Same Dealers not show interest in designing e-installment foundation.

Dependability: The business system should be trustable and the control of this transaction is dependent one.

Availability: Whenever the system required it should available for anyone

Processing time: It should be more sufficient for e-business end-customers.
Operations that connecting the customer and merchant: The system must be interoperable between unmistakable figuring stages, web programs and server programming groups with a particular final objective to engage its usage by the conceivable range of e-trade shoppers and shippers.

Ecommerce secure customs are the broadly sees sound working principles for secure satisfaction of data trade, besides the crucial structure to guarantee the insurance, uprightness, assertion of online exchanges. Their realkey to give online security. Web security tradition is the central examination domains in Ecommerce as the tries to propel the change of Ecommerce, and guarantee its security. Generally these traditions to send private information on the Internet without encouraging to individuals. In any case, they are not secured, a couple bumbles were found in cryptographic traditions following a couple of years of usage. The results of the cryptographic efforts are not changeable and expensive for associations and individuals. We consider how E-exchange security necessities are fulfilled by another tradition in light of portion entryway and propelled mark.

Proposed architecture for secured transaction:

Conditions Should Be Checked Before Transactions:

- Each customer and the agent have unique net banking account.
- Each agent should have server for mobile banking, companies and couriers through internet.
- Every customer must have unique account to mobile server

Description of secured transaction steps:

To register: Seller and the medium of payment and the bank authority those involve in the transaction must register their names and have a valid and approved certificate from corresponding authorities. Consumer should get a password for payment from the bank authority.

Request for Purchase: Cardholder first searching the needy things then he purchased from the online shop and added the list of items. Then they confirmed the order before buying. The cardholder sends the ID to the merchant for preventing any attacks during transaction.

Checking for authority: Merchant sends valid request for payment, also he verified the password and check the encryption and decryption keys for the authorized transaction without any outsiders intruding the transaction.

Response from authority: The corresponding bank responsible for money transfer verifies authorization request and allowed to make this transaction. The receiver of the bank authority sends an authorization response and issue bank certificate through the secure interbank financial network.

Request of Card holder: The client verifies the bank certificates and then sends his personal password for the merchant for authorized the transaction and collecting the money.

Consumer Response and process for payment: The receiving bank authority decrypts the password code and gives the immediate acknowledgement to the clients authorized request then debits money from the customer’s account and sending response to the client’s Bank server.

2. CONCLUSION

In this paper the payment security requirements identified and clear all the user issues and its drawbacks. In future we can analyze the security and its efficiency. In every web business transfer of money and the delivery of the product is the main issue. Also the money transfer is mainly depends fully on the bank authority. The information shared between customer and the bank and between companies should be confidential and used some secured algorithm. The security in electronic transaction made efficient by using new architecture.

REFERENCES


Kaliyamurthie KP, Udayakumar R, Parameswari D, Muguntham SN, Highly secured online voting system over network, Indian Journal of Science and Technology, 6 (6), 2013, 4831-4836.


Khanaa V, Thooyamani KP, Saravanan T, Simulation of an all optical full adder using optical switch, Indian Journal of Science and Technology, 6 (6), 2013, 4733-4736.


Sengottuvel P, Satishkumar S, Dinakaran D, Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling, Procedia Engineering, 64, 2013, 1069-1078.


