ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

The Role of SSL & SET Protocol in E-Commerce

Rahul Kumar[1], Arun Kumar Shukla[2], Ajit Pratap Singh[3]

M.Tech Student, Dept. of CSE, S.H.I.A.T.S -Deemed University, Allahabad, India [1, 3]

Asst. Prof, Dept. of CSE, S.H.I.A.T.S -Deemed University, Allahabad, India [2]

Abstract: This century is the era of online shopping. The number of internet users is rapidly increasing day by day as now internet has reached to every home. This leads to increase in online transaction. E-commerce is also known as electronic commerce or EC. E-commerce refers to the buying or selling of products or services over internet which involve the use of Electronic transaction that reduces the use of paper work. The major issues of E-commerce are to protect assets from unauthorized access. There are lots of shopping websites like flipkart, snap deal, Amazon, paytm etc are asking for personal information like credit card number, password etc and these information's are transmitted over the web so it is necessary to protect these information. In this paper we study the E-commerce and its model and two most popular protocols SET and SSL which ensures security of transaction made over the internet.

Keywords: E-commerce; SSL; SET.

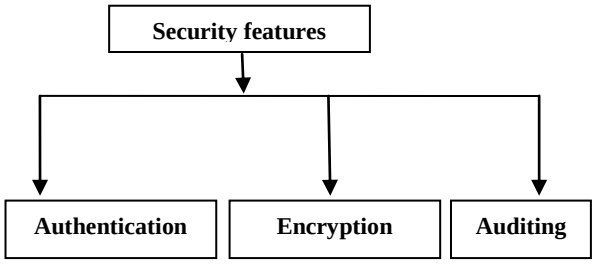
I. INTRODUCTION

In the emerging global economy, E-commerce is a core component that acts as a catalyst for economic development. Recent growth in the use of Smartphone's has radically increased the use of internet. Everyone is now using web & Smartphone's for purchasing goods electronically therefore security of the personal information is a major concern. [3]The major concern or security issues regarding E-commerce transactions are:

- Unauthorized access of personal information
- Hacking transaction and stealing money
- Financial fraud
- Illegal transaction i.e. Money laundering

Security is an important concern of any transaction that takes place over the internet. The following are considered important requirements for E-transactions are:

- **Confidentiality:** Unauthorized user should not be able access the information during transaction.
- **Integrity:** When information is transfer from sender to receiver over the network then it should not be altered. Information should be exactly same as send by an authorized entity.
- **Availability:** Information should be available at any time upon the requirement.
- **Authenticity:** Mechanism should authenticate user before allowing him to access the information.
- **Non Repudiation:** Mechanism by which sender or receiver should not denial from transmitted message.



Security Features: There are certain securities features which are considered important are discussed below:

- **Authentication:** System must ensure that only an authorized person is allowed to use the service.
- **Encryption:** Encryption is the process of hiding information by the use of mathematical formula or keys to transform a message into a secret message that is not easily understood by everyone.
- **Auditing:** Merchant use auditing to prove that you bought specific merchandise.

II. E-COMMERCE

The use of electronic medium for purchasing or selling of goods is known as E-Commerce [1]. From fig1: E-Commerce is the emerging modern business style which addresses the need of customer and reduces the cost of product and at the same time it improves the quality of product and services.

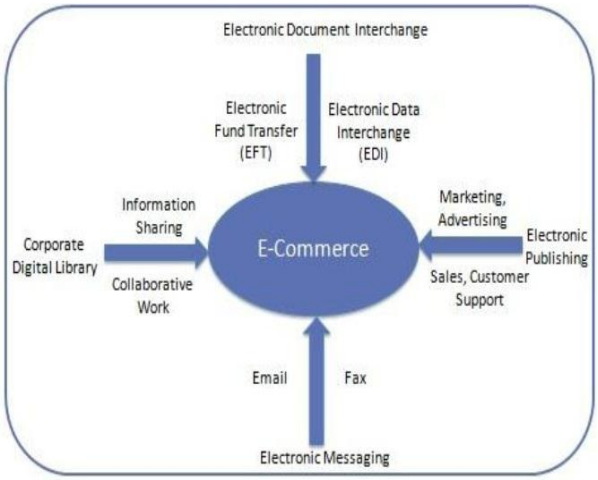


Figure 1

DOI 10.17148/IJARCCE.2015.4939

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

It is also known as paperless exchange of information which can be done by the following ways:

- Electronic data exchange
- Electronic mail
- Electronic bulletin board
- Electronic fund transfer

A. Features of E-commerce

E-commerce provides the following features:

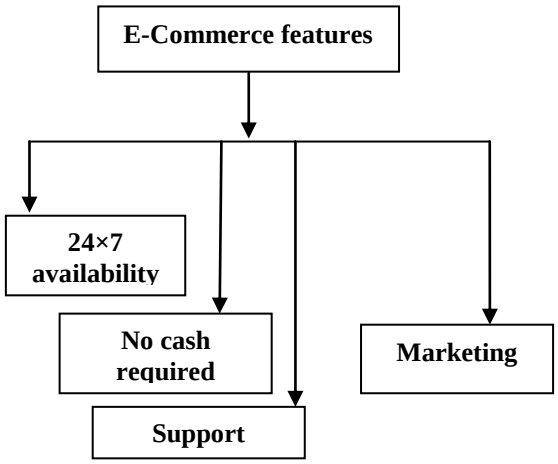


Fig2: E-Commerce features

- **24×7 availability:** E-Commerce services are available to the customer any time. They provide 24×7 services to the customer.
- **No cash required:** E-Commerce makes the use of internet banking, credit card transaction etc for purchasing product which does not required physical payment, and all transactions are handles electronically.
- **Support:** E-Commerce provides pre sales and post sales assistance to their customers.
- **Marketing:** E-Commerce makes the use of digital marketing for promoting their products and services. The use of social media for marketing purpose is on the peak and this social media marketing also helps in branding of new product in the market.
- **Cash on delivery:** Online shopping websites are now providing faster way to deliver the product at your door steps. In fact cash on delivery is also available with many E-Commerce sites.

B. E-Commerce business models

E-Commerce business model can be divided into the following:

- **Business to Business (B2B):** In business to business model, website sells its product to intermediate buyer and this buyer then sells the products to the customer.

- **Business to consumer (B2C):** In business to consumer model, websites sell its product directly to the customer.

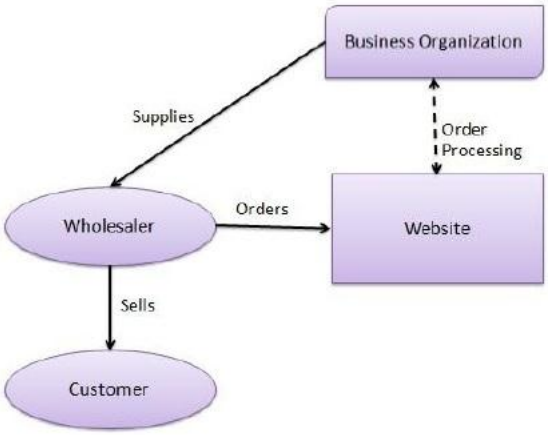


Fig 3: B2B Model

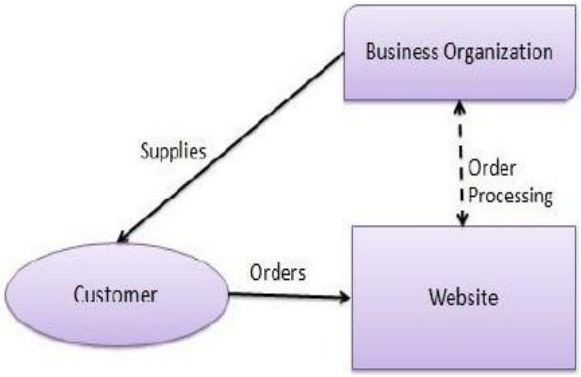


Fig 4: B2C Model

- **Consumer to consumer (C2C):** In consumer to consumer model, consumer sells its assets by publishing their product on website to the other consumer.

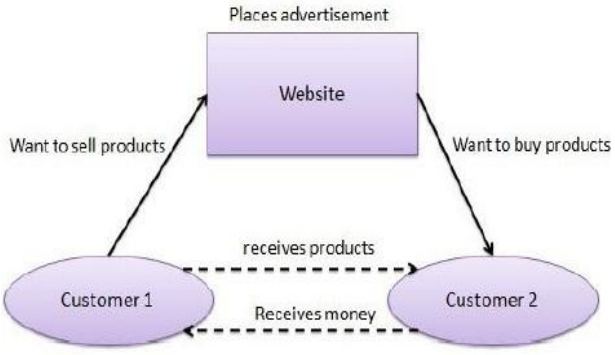


Fig 5: C2C Model

- **Consumer to business (C2B):** In consumer to business model, end consumer creates product and services which is consumed by business organization.

- **Government to business (G2B):** In government to business model, government uses website to approach business organization. Example website support tender, auction etc.

DOI 10.17148/IJARCCE.2015.4939

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

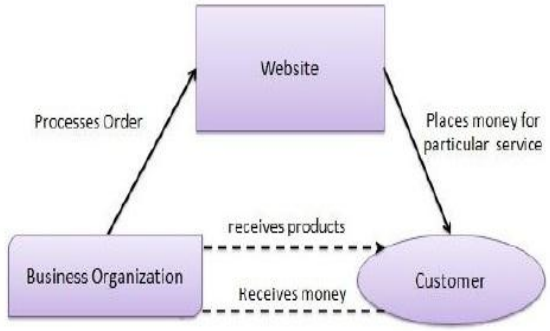


Fig 6: C2B Model

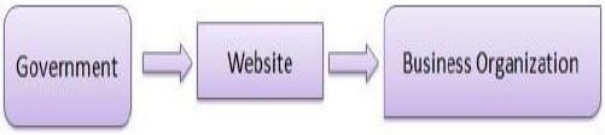


Fig 7: G2B Model

- **Government to citizen (G2C):** In government to citizen model, government uses websites to approach consumers.

Fig 8: G2C Model

- **Business to government (B2G):** In business to government model, in which government uses websites to trade and exchange information with various business organizations.

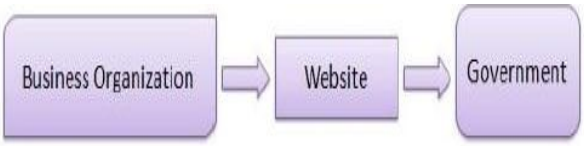


Fig 9: B2G Model

III. ELECTRONIC PAYMENTS METHODS

E-Commerce or electronic commerce sites makes the use of electronic payment and this mode of payment is also refers to as paperless monetary transaction. [2]E-Commerce transform the mode of doing business from manual processing to electronic processing as this reduces the processing cost, paperwork etc. Some modes of payment are discussed below:

- **Credit card:** Credit card is a small plastic in which magnetic strip is embedded and this card contains a unique number that is attached to an account. Fig10:This card is issued by a financial company , when customer purchase anything via this card then financial company pays on the behalf of customer but they charge interest on it.

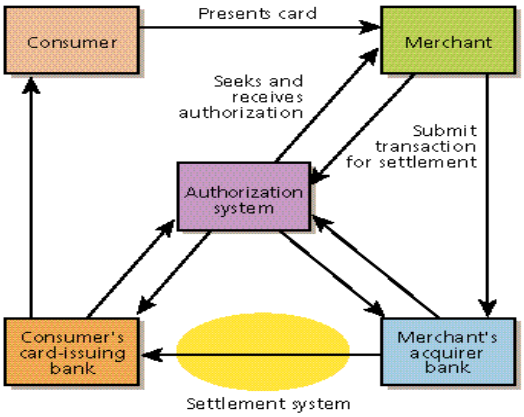


Fig10: Credit card system

- **Debit card:** Debit card is like a credit card , is a small plastic in which unique number is mapped with the account number but the customer need to open the bank account before getting a debit card. When the customer purchase anything via this debit card, the amount of good which he has purchased is debited from his account.
- **E-Money:** E-Money refers to the transfer of payment over network from one financial body to another financial body. E-Money is the efficient way of money transfer in which no middle man is involved and its safes time also.
- **Electronic fund transfer:** EDF is one of the most popular methods to transfer money from one bank account to another bank account but the most important thing account can be in same or different bank. This fund transfer can be done using personal computer or ATM.

IV. E-COMMERCE SECURITY PROTOCOL

A. Secure socket layer

The secure socket layer (SSL), was developed by Netscape in 1994 to provide security of information exchange over the internet. SSL is a computer networking protocol that is used to encrypt communication between the user and web server. Secure socket layer provides server authentication, client authentication and at the same time it provide encrypted communication between the client and server [6, 7].

SSL concepts [8]:

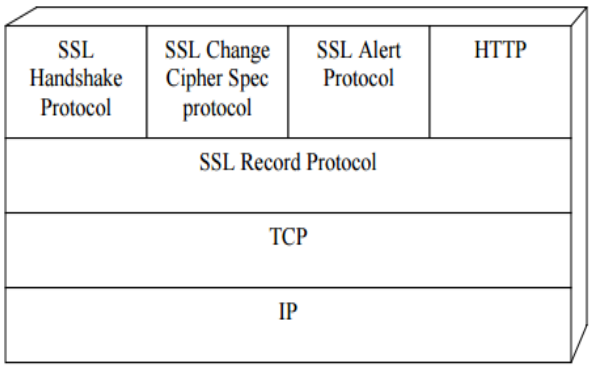


Fig11: SSL Architecture Protocol

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

- SSL Session: SSL handshake protocol creates the mutual understanding between the client and server. It is an association between client and server in which number of states are associated with each session.
- SSL Connection: Connection takes place in transport layer.SSL connection is a peer to peer relationship, and is transient. Many connections are associated with one session.

SSL Handshake Protocol: SSL handshake protocol the client and the server to authenticate each other before any application data is transmitted. Fig12: Handshake consists of:

- Allow the client and server authenticates each other.
- Allow client and server to negotiate encryption and MAC algorithms.
- Allow the client and server to negotiate cryptographic keys to be used.

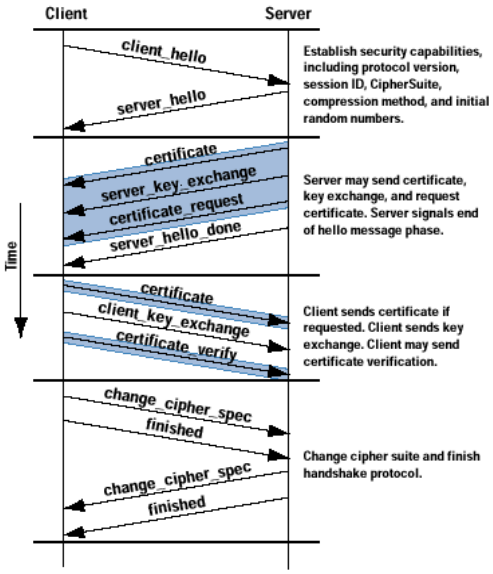


Fig12: Handshake protocol action

SSL Record Protocol: SSL Record protocol provide security services to higher layer protocol.SSL built the path between sender and the receiver and it encrypt this path before the data is sent.

SSL Alert protocol: SSL alert protocol is used to send alert message when some failure or abnormal condition occur. This alert message is also called "warning messages". Alert message has two fields: "warning" or "fatal" with the corresponding alert code. It is also used for the following purpose:

- It sends alert on closure of connection.
- It notify when the certificate are absent.
- It notify when unwanted certificate is received.
- It notify in the case when certificate has expired.

SSL Change Cipher Spec protocol: SSL change cipher spec protocol consists of single message with only one byte with value 1. Causes pending state to become current state, hence updating cipher in use .A single byte is sent after new cipher parameter have been agreed upon.

HTTP: Hyper transfer protocol operates on the top layer of secure socket layer which handles the transfer service for web client/server interactions.

How Does SSL work with our Browser?

HTTP is insecure because if personal information like credit card, password etc are transmitted over the network then there will be lots of possibilities that attacker can easily hack your information therefore data must be sent through browser using HTTPS. Fig13: The browser works behind the scene by retrieving SSL certificate on connection to secure site. The browser checks the validity of certificate and whether the authority which is issuing certificate is trusted or not. If SSL checks fails then browser informs that it is not a trusted websites.

Fig13

Advantages of Secure Socket Layer (SSL):

- SSL is supported by most of the browsers and there is no need for downloading any extra software.
- SSL system is not so complex therefore it results in increase of transaction speed.
- There are various types of security options are available after client and service authentication.

B. Secure electronic transaction

Secure electronic transaction is a system used for securing credit card financial transaction over insecure network such that merchant and card holder can securely conduct E-commerce transaction over network. SET uses cryptography technique for providing secure transaction over unreliable network. By the use of cryptography, SET provides confidentiality and secures payment integrity and at the same time authenticates both merchant and card holder [4, 5].

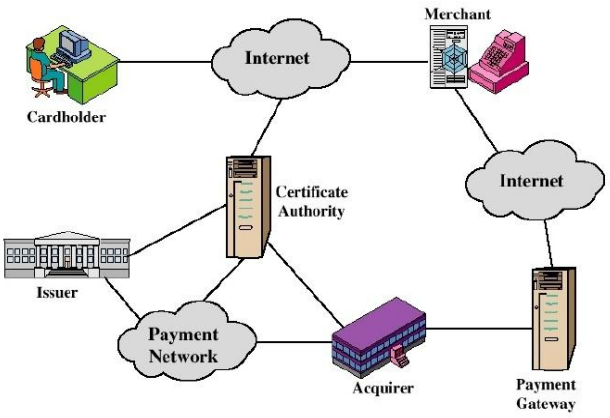


Fig14: Participants involved in SET Transaction

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

The participants involve in a SET transaction are discussed below:

- **Card holder:** The consumer who uses the payment card to purchase goods or services is known as card holder. The most important benefit of using payment card is: Its processing is fast and requires no paper work
- **Merchant:** The business or organization sells goods or services to the consumer in the SET transaction over an unreliable network are known as merchant.
- **Issuer:** The financial institution issues payment card to the customer and when customer buys anything from the market then financial institution who issues this payment card pays on the behalf of customer.
- **Acquire:** Acquire is a financial institution who verifies the payment of the cardholder when he buys anything from the market.
- **Payment Gateway:** Payment gateway is an application that provides a secure path between E-commerce website and your internet merchant account by authorizing the card payments.
- **Certificate authority:** Certificate authority issues digital certificate to merchant, card holder and payment gateway. This certificate authority is responsible to ensure that all persons who are involved in the transaction are legitimate users.

SET provides three features:

- SET provide secure path between the parties who are involved in the transaction.
- Trust by the use of X.509V3 digital certificate.
- SET guarantees that payment information will be confidential and it is only known to the parties who are involve in the transaction.

Advantage of SET:

- SET provide confidentiality on payment information.
- SET ensures integrity of data which is transmitted over an unreliable network.
- SET ensures the parties involved in the transaction are legitimate.
- SET hides the order information from the payment gateway.

V. CONCLUSIONS

E-Commerce deals with purchasing or selling of goods and services via internet but the transaction is done through electronic means. E-Commerce and M-Commerce is growing rapidly day by day with increase in the number of internet users and Smartphone's device therefore it is necessary to protect E-Commerce assets from unauthorized access. Secure socket layer and secure electronic transaction are the two popular E-commerce security protocols. In this paper we have discussed about the role of secure socket layer (SSL) and secure electronic transaction (SET) in E-commerce security.

VI. ACKNOWLEDGMENT

I express my sincere gratitude to my guide **Er. Arun Kumar Shukla** (Asst. Prof) who assisted me throughout this work. I thank him for providing me confidence and most importantly he supported and guided me whenever I needed. I am also thankful to my friend Ajit Pratap Singh for his contribution during this research work.

REFERENCES

[1] Asuman Dogac, Electronic Commerce. Journal Of Database Management, Fall 1999.
[2] Singh Sumanjeet, " Emergence Of Payment Systems In The Age Of Electronic Commerce: The State Of Art", Global Journal Of International Business Research Vol. 2. No. 2. 2009 .
[3] Dr.Nada M.A.Al-Slamy, "E-Commerce security" IJCSNS-VOL.8 No.5, May 2008
[4] Electronic Payment System- ISA 767 (2008) Secure Electronic Commerce George Mason University
[5] "SET Secure Electronic Transaction LLC. " Purchase, NY: SET Secure Electronic Transaction LLC, 2001. Available From Www.Setco.Org
[6] Mayu Mishina. Is electronic commerce a good idea for you? AS/400 Systems Management, July 1998. Netscape Corp. Appendix E, Introduction to SSL. Page 213-229.
[7] Taher Elgamal. The Secure Sockets Layer Protocol (SSL). Danvers IETF Meeting, April 1995.
[8] Nikos Drakos. Security & Electronic Commerce: SSL Protocol. Security & Electronic Commerce Appendix, University of Leed,1997

BIOGRAPHIES

Rahul Kumar was born in Uttar Pradesh, India, in 1992. He has received B.Tech degree in Computer Science & Engineering in 2012 and then worked as a Guest Speaker in Govt. I.T.I from 2012 to 2014. Currently perusing M.Tech degree in CSE from Sam Higginbottom Institute of Agriculture, Technology & Science, Deemed-to-be- University in Allahabad (U.P).

Arun Kumar Shukla is currently working as Assistant professor in the Computer Science and IT Department in Sam Higginbottom Institute of Agriculture, Technology & Science, Deemed-to-be-University in Allahabad (U.P). He has done his bachelor of Engineering from Jawaharlal Institute of Technology from Khargone (M.P) in the year 2006 and Master of Engineering from I.E.T. - D.A.V.V., Indore in the year 2011. He has also worked on the post of Lecturer and Sr. Lecturer in Malwa Institute of Technology, Indore from January, 2007 to June, 2011.

Ajit Pratap Singh was born in Uttar Pradesh, India, in 1990. He has received B.Tech degree in Computer Science & Engineering in 2013 from UPTU and Currently perusing M.Tech degree in CSE from Sam Higginbottom Institute of Agriculture, Technology & Science, Deemed-to-be-University in Allahabad (U.P).