ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

E-commerce transaction security behaviour analysis with regard to SSL

Santhosh kumar G

Koneru Lakshmaiah Educational Foundation, KLEF, Vaddeswaram, Guntur- 522302,

Andhra Pradesh, India

Abstract

At present is the period of information communication technology in the E-commerce. E-Business is the totally accomplishment of this. In era of E-Business, the E-Transaction takes place over the communication network as well as Internet. At some stage in various phases of an electronic communication transaction, the information and data such as invention measurement, design, pattern, order details, online payment information as well as delivery information travels over communication network and internet. So now a days, thieves and hackers are finding the opportunities to take information related online payment transaction. For the reason that, the need for security in every online payment transactions are become mandatory for everyone and every organization to make safe transaction. To overcome this problem, two most popular E-commerce transactions secure protocols like Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) are used to fulfill the security job for E-commerce transaction. In this paper try to analyze how these existing security schemes SSL and SET to provide secure transaction in between customer and company. In addition, this paper also briefly considers how elements of these two protocols might be combined to offer both security and easiness of use.

Keywords: Electronic Commerce (E-Commerce), Electronic Transaction (E-Transaction), Electronic payment (E-payment), Secure Socket Layer (SSL), Secure Electronic Transaction (SET).

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

Introduction

Modern enlargement in Internet usage has increased the problem of online transactions. Every one using the web and apps for E- Business needs to be concern about the security of their personal information. Security and encryption in e-commerce is a growing need among companies and consumers. A Check Point report assured that cybercrime will remain constant in 2022, but that its attacks will be more complicated and intellectual. The drawbacks of online payment systems regarding security like unauthorized transactions or theft money, hacking of personal information and use it for identity theft, and attacking on data. But how it can be ensured is a big question and need to be solved. Encryption is one of the most powerful schemas of improving cyber-security for online transactions. More sensitive customer information such as (user names, passwords, bank details, etc.) can be protected through encryption protocols. This procedure is not very easy to give explanation but can be summed up in the use of a different unique code, which allows the sender and receiver to decrypt the data and information needed in the transaction. In this mode, the theft of such data makes no sense to cybercriminals, who will not be able to decipher them. SSL and SET are the most widely and powerful protocol used to provide the security solution for E-commerce transactions. Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) are the two main security protocols for securing e-commerce communications. Currently, SSL is almost always used in preference for e-commerce transactions security.

E-Commerce Security Protocols

Secure Socket Layer (SSL)

In 1994, Netscape developed its first standard of Secure Socket Layer (SSL) to implement secure environment to exchange the information over the Internet and made it public for implementation in fall 1994. SSL is a security protocol protects communications between client and server software running on a network that uses TCP/IP. SSL stands for Secure Sockets Layer and it is a protocol to enable encrypted and authenticated communications over the Internet. Secure Sockets Layer is the standard security tools for establishing an encoded link between a web browser and a server. SSL is the encrypted connection between web server and a browser which guarantees that

ISSN PRINT 2319 1775 Online 2320 7876

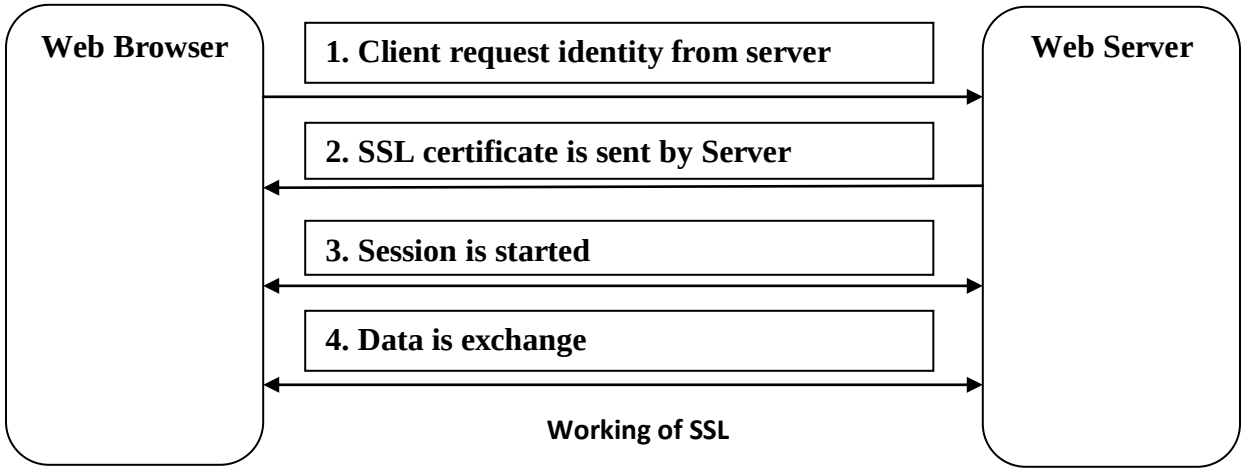
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

all data passed between them will be remain safe. SSL mainly used to provide three important things like, Privacy, Authentication, and Message Integrity.

Working of SSL

With the help of SSL connection each side of the connection must have a Security Certificate. Security Certificate must be required in each side (web server and web browser) of the SSL connection to make safe online transaction.

SSL security works based on public-key and private key cryptography. The working of SSL is as follows.



The working of SSL is as follows.

Step 1:

The client sends the request to web server for identify itself.

Step 2:

The server sends copy of its SSL certificate with keys

Step 3:

The server acknowledges the client to start an SSL session.

Step 4:

The client uses the session keys generated in step 2 to encrypt its data and exchange it with the server.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

SSL certificate

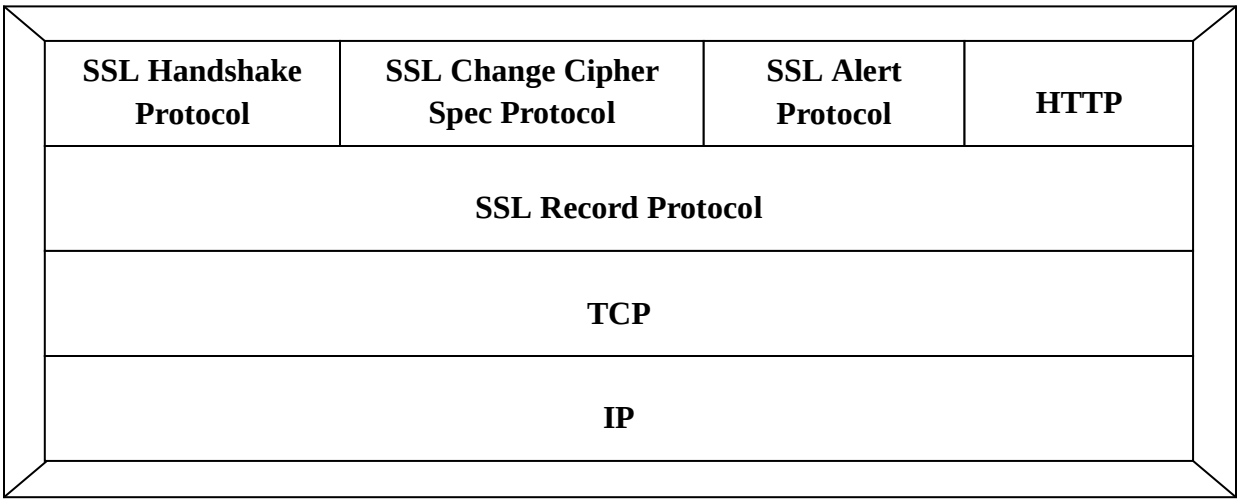
SSL certificate is a type of digital certificate that provides authentication for a website and enables an encrypted connection. It consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decrypt information.

An SSL certificate helps to transfer secure information's such as:

1) Login identifications information.
2) Bank and credit card transactions information.
3) Personally identifiable information (such as name, address, date of birth, mobile number and so on.).
4) Proprietary (branded) information.
5) Authorized documents and agreements.
6) Medical records.

SSL Layered Architecture

SSL always runs on the top of TCP and it provides reliable and secure end-to-end connection service. SSL Layered Architecture Consists of two layers follows.



ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

SSL Architecture

Secure Sockets Layer protocol has two layers (Layer1 and Layer2).

1.1.1.3.1 First Layer Protocol:

SSL Record Protocol included in first layers**.** The SSL record protocol provides security to other higher level protocols like HTTP handshake protocol, change cipher protocol and alert protocol. The SSL record protocol provides two services for SSL connections:

1) **Confidentiality: -**

   A shared secret key that is used for conventional encryption of SSL payload.

2) **Message Integrity: -**

   A shared secret key that is used to construct (Form) a message authentication code.

Second Layer Protocol:

There are three higher-layer protocols are included in second layer such as SSL Handshake Protocol, SSL Change Cipher Spec Protocol and SSL Alert Protocol.

1) SSL Handshake Protocol
2) SSL Change Cipher Spec Protocol
3) SSL Alert Protocol

1) **SSL Handshake Protocol:**

   SSL Handshake Protocol is the first protocal of the second layer. The most complex part of SSL is the handshake protocol.It allows the webserver and webclient to authenticate eachother, encryption, MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record. The handshake protocol is used before any application data are transmitted.

2) **SSL Change Cipher Spec Protocol:**

   SSL Change cipher spec protocol is the second protocal of the second layer. It is one of the three SSL-specific protocols that use the SLL Record protocols. Change cipher spec protocol is the simplest protocol. Change cipher spec protocol is consists of a single message, which consists of a single byte with the value 1.

3) **SSL Alert Protocol:**

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

SSL Alert protocol is the third protocal of the second layer and it work on SSL Record protocol. SSL Alert protocol consists of a two bytes. The First byte indicates**warning(1) or fatal(2).**A Fatal alert will terminate the connection. The Second byte indicate specific error code.

Secure Electronic Transaction (SET)

It is protocol specially designated to secure payment transactions and authenticate the parties involved in the transaction in any type of networks including Internet. VISA and MasterCard developed the SET standard with collaboration from leading software companies such as Microsoft, Netscape to e-commerce websites to secure electronic debit and credit card payments. SET was created to provide the trust needed for consumers. The protocol uses cryptography and digital certificates to provide confidentiality of the information, ensure payment integrity, and authenticate merchants, banks, and cardholders during SET transaction.

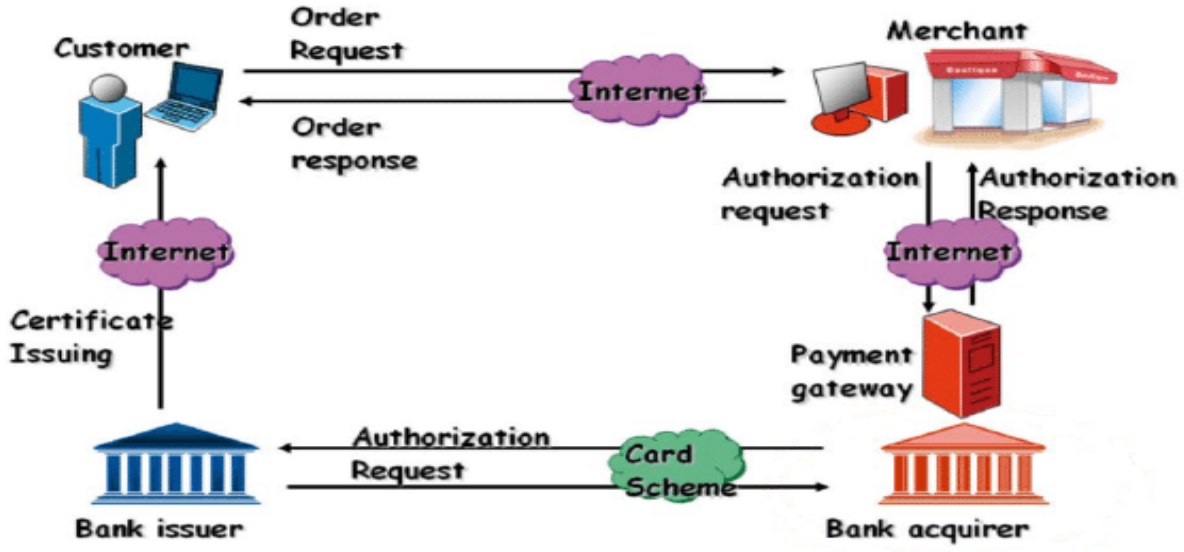


Figure 1: Secure Electronic Transactions

SET Specifications*:*

Privacy via cryptography

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

The SET protocol uses two forms of cryptography to ensure the confidentiality of the transactions. First, an asymmetric form known as RSA is used for signatures and public-key encryption of symmetric encryption keys and bank card numbers, and then a symmetric form called DES takes care of the encryption of the data that is to be transmitted during the transaction. It might be of interest to take a closer look at these two forms of encryption, so let's start with RSA.

RSA

RSA builds on the concept of asymmetric or *public-key cryptography* in order to solve the key management problem. It uses pairs of so called *private* and *public* keys that are mathematically related to each other. The public keys are shared over any network (including the Internet) and used to encrypt messages to the owners of them. The owner then decrypts the message using his/her private key. This way anyone can send an encrypted message, using only the public keys, but only who has private key can decrypt the message.

DES

DES was originally developed at IBM, and is the most well-known and widely used cryptographic system in the world. It is a symmetric cryptosystem, which means that both the sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single user encryption, such as to store files on a hard disk in encrypted form. In a multiuser environment, secure key distribution may be difficult as it requires access to completely safe communication. This is also its major disadvantage compared to asymmetric public-key cryptography which provides an ideal solution to this problem. Why is then DES used in the SET protocol? It's used because it's much faster than RSA, generally at least 100 times as fast.

So how the SET protocol does combines the better of the two encryption methods? It does so by encrypting the message data using a randomly generated symmetric DES encryption key. This key is, in turn, encrypted using the message recipient's RSA public key. This second encryption

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

is referred to as the "digital envelope" of the message and is sent to the recipient along with the encrypted message itself. After receiving the digital envelope, the recipient decrypts it using his or her private key and obtains the randomly generated symmetric key and then uses the symmetric key to unlock the original message.

Advantages of SET Protocol

- Confidentiality, authentication and data integrity was verified by a large collection of security proofs based on formal methods.
- SET prevents merchants from seeing the customer payment information, since this information is encrypted using the payment gateway's public key.
- To ensure merchant privacy, SET prevents the payment gateway from seeing the order information.

Disadvantages of SET

- The customer must install additional software, which can handle SET transactions.
- The customer must have a valid digital certificate.
- Implementing SET is more costly than SSL for merchants as well.
- Adapting their systems to work with SET is more complicated than adapting them to work with SSL
- SET employs complex cryptographic mechanisms that may have an impact on the transaction speed.

Review of Literature

Robinson (2008) develops the fundamental concepts surrounding cryptography, such as public key/private key encryption, Diffie-Hellman Key Exchange, block ciphers, Hash algorithms, DES, AES, the implications of IP Security(IPSEC) and Internet Key Exchange (IKE), elliptic curve cryptography, SSL/TLS used heavily in Web-based applications, Wi-Fi, and other embedded security concerns. Next, Robinson makes a case that developing strong encryption

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

protocols in software for small devices may be too cost prohibitive, and these designers should consider including cryptographic hardware in the embedded designs.

Zanin at al. (2007) in their study present a new distributed signature protocol based on the RSA cryptographic algorithm, which is suitable for large-scale ad-hoc networks. This signature protocol is shown to be distributed, adaptive, and robust while remaining subject to tight security and architectural constraints. The study reveals that the robustness of this protocol scheme can be enhanced by involving only a fraction of the nodes on the network. Zanin et al. demonstrated that their protocol scheme is correct, because it allows a chosen number of nodes to produce a valid cryptographic signature; it is secure, because an attacker who compromises fewer than the given number of nodes is unable to disrupt the service or produce a bogus signature; and it is efficient, because of the low overhead in comparison to the number of features provided.

Toubba (2006) stresses the importance of strong encryption key management and granular access control to Web-based applications. Toubba shows that corporations that store transmit, and use consumer data must take steps to choose strong cryptographic solutions to protect this data, and to employ complementary network security procedures to maximize the overall effectiveness of the encryption product. Strong key management and granular access control are viewed as the complementary network security procedures.

Abbot (1999) argues that there are four main benefits that SET offers over SSL. First, SET provides merchants with assurance that transactions will not be fraudulently charged back. This feature will lower the merchants' costs. Second, SET affords greater privacy and makes it easier to buy online. It assures the customer that the merchant is legitimate and the credit card is safe. Third, SET allows banks and companies extend their brands to cyberspace, while still maintaining their strong position as payment systems. The lower rates of fraud when using SET make credit cards more competitive than other means of payments. Fourth, SET defines inter-functionality between all parts of the card-payment process.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

Analysis

Secure socket layer	**Secure electronic transaction**
SSL is basically an encryption mechanism for order taking, queries and other applications and available on customer's browser. It does not protect against all security hazards and is natural simple and widely used. SSL is a protocol for general purpose secure message exchange. SSL protocol may use a certificate, but the payment gateway is not available. so, the merchant need to receive both the ordering information and credit card information because the capturing process should be generated by merchant. SSl protocol has been the industry standard for securing internet communication. SSL protocol was developed by Netscape for securing online transaction.	SET is a very comprehensive protocol. It provides Privacy, integrate and authenticity. It is not used frequently due to its complexity and the need for a special card reader by the user. it may be abandons if it is not simplified. SET is tailored to the credit card payment to the merchant. A SET protocol hides the customer's credit card information from merchant and also hides the order information to banks to protect privacy called dual signature. SET protocol is a complex and more secure protocol. SET protocol was jointly developed by MasterCard and visa with the goal of securing web browsers for bank card transaction.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Issue 2, 2022

Conclusion

E-commerce is the ability to do business through the Internet. It is not just present of computers and absence of papers. It has more than this. E-commerce security is the major issue keeping many commerce organizations afraid from using Internet for their business. Secured Socket Layer (SSL) and Secured Electronic Transactions (SET) are the major popular Ecommerce security protocols. Each one of them has its domain of use, its products, its strategy, and its own encryption procedure. Doing a comparison study between SSL and SET is not an easy thing. Using SSL or SET depends on user consideration. A comparison study shows the design issue of each one, its way of securing E-commerce, authenticates parties, using key exchange, and its encryption methodologies. While there are still lots of efforts focused on E-commerce security, it is not an easy decision to use Internet to exchange critical data such as credit card number, passwords, or any sensitive private information.

References

1. Abbot. (1999). Debate for Secure E-Commerce. Performance Computing, 37-42.
2. K, T. (2006). Employing Encryption to Secure Consumer Data. Information Systems Security, 46-54.
3. S, R. (2008). Safe and secure: data encryption for embedded systems. Academic Search Premier Database, 24-33.
4. ZAnin G, D. P. (2008). Robust RSA Distributed Satures for Large Scale Long-lived adhoc networks. Journal of Computer Security, 171-196.