Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 9, September -2017

# Data Transmission Using Secure Socket Layer (SSL) Protocol in Networks

[1]Sirisha Gude, [2]Dr. R. China Appala Naidu

[1,2]*S.T.MARTIN'S,ENGINEERING,COLLEGE.*

**ABSTRACT:-***Concerning illustration associations give additional administrations,furthermore transactions online, security turns into a need. Clients require with a chance to be sure that delicate data for example, such that a credit card number is setting off to a legitimate online business.Associations need will keep client majority of the data private furthermore secure.*

*SSL certificates would be crucial part from the information encryption methodology that make web transactions secure. They need aid advanced passports that give verification should secure the secrecy and integument for website correspondence with browsers.*

*Those SSL certificate's particular occupation is will start secure sessions with those user's program through those secure sockets layer (SSL) protocol. This secure association can't a chance to be made without the SSL certificate, which digitally associate shares of the organization majority of the data with a cryptographic key.*

*At whatever association that captivates in ecommerce must have a SSL testament looking into its Web server to guarantee those security of client What's more agency information, and in addition thosesecurity from claiming fiscal transactions.*

***Keywords:*** *Secure Socket Layer,Transmission Control Protocol, Encryption.*

## 1. INTRODUCTION:

The SSL protocol might have been initially formed by Netscape, to guarantee security from claiming information transported. Also routed through HTTP, LDAP or POP3 requisition layers.SSL will be outlined to make utilization of TCP (Transmission Control Protocol)as a correspondence layer to furnish a dependable end-to-end secure also verified association between two focuses again a system. (for example

between the service client and the server). Regardless this SSL could a chance to be utilized for insurance for information for travel for particular circumstances identified with any organize service, it will be utilized basically in HTTP server and client applications. Today, practically each accessible HTTP server can support an SSL session, whilst IE or Netscape Navigator browsers pilot browsers would give for SSL-enabled customer product.

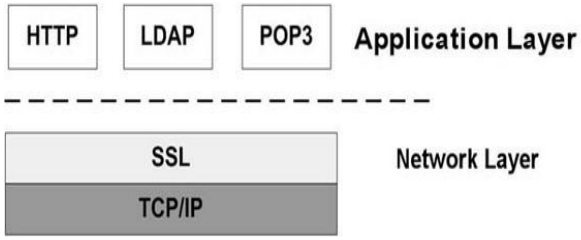



*Figure 1: SSL between application protocols and TCP/IP*

## 2. SSL objectives and architecture:

The main objectives for SSL are:

- Authenticating thecustomer furthermore server should each other: those SSL protocol helps the utilization for standard enter cryptographic strategies (public way encryption) should validate the conveying gatherings with one another.
- Guaranteeing information integrity: throughout a session, information can't be possibly eagerness or unintentionally tampered for.

@IJAERD-2017, All rights Reserved 

- Securing dataprivacy: information for transport the middle of those customer and the server must make ensured starting with interceptor. This prerequisite is necessary for both the data associated with the protocol itself (securing traffic during negotiations) and the application data that is sent during the session itself.

SSL is truth be told not an absolute protocol in any case instead a set of protocols further isolated on two layers:

1. The protocol to guarantee information security also integrity: this layer will be created of the SSL record Protocol.
2. the protocols that are designed to establish an SSL connection: three protocols are used in this layer: the SSL Handshake Protocol, the SSL ChangeCipher Spec protocol and the SSL Alert Protocol.

The SSL protocol stack is illustrated in Figure 2.

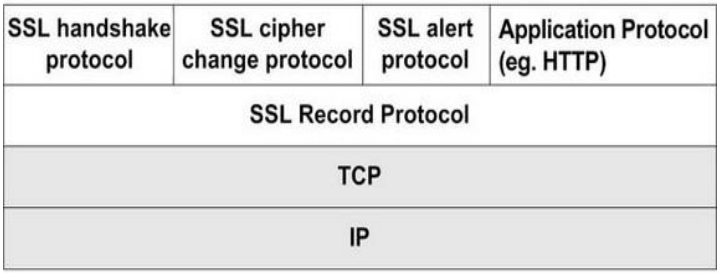


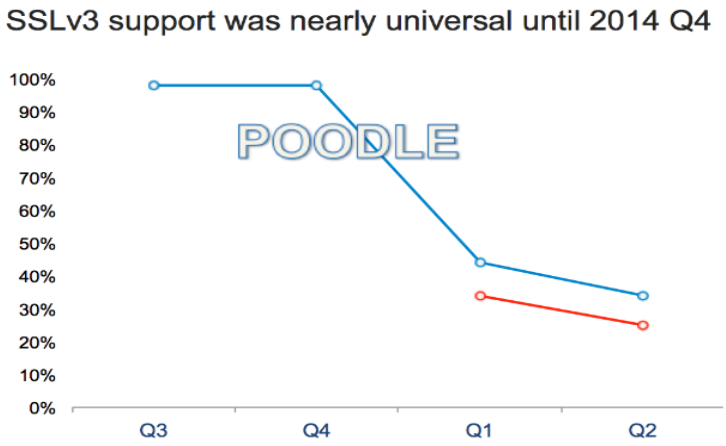

*Figure 2: The SSL protocol stack*

***SSL Record Protocol***: Those SSL record protocol may be answerable for information encryption and integument.As can be seen in Figure 2, it will be likewise utilized will embody information sent toward other SSL protocols, and accordingly it may be additionally included in the tasks connected with the SSL weigh information. The other three protocols cover the areas of session management, cryptographic parameter management and transfer of SSL messages between the client and the server.

***Alert Protocol:***The Alert Protocol is utilized by gatherings to pass on session messages related with information trade and working of the convention. Each message in the ready convention comprises of two bytes. The first byte dependably takes an esteem, "warning" and second that decides the seriousness of the message sent.

***ChangeCipher Spec protocol:***This convention is the least complex SSL convention. It comprises of a solitary message that conveys the value of 1. The sole reason for this message is to cause the pending session state to be built up as a settled state.
***Handshake protocol:***The handshake constitutes the most complex piece of the SSL convention. It is utilized to start a session between the server and the customer.

***SSL Versions***:SSLv2 and SSLv3 are the 2 versions of this protocol (SSLv1 was never publicly released).




@IJAERD-2017, All rights Reserved 

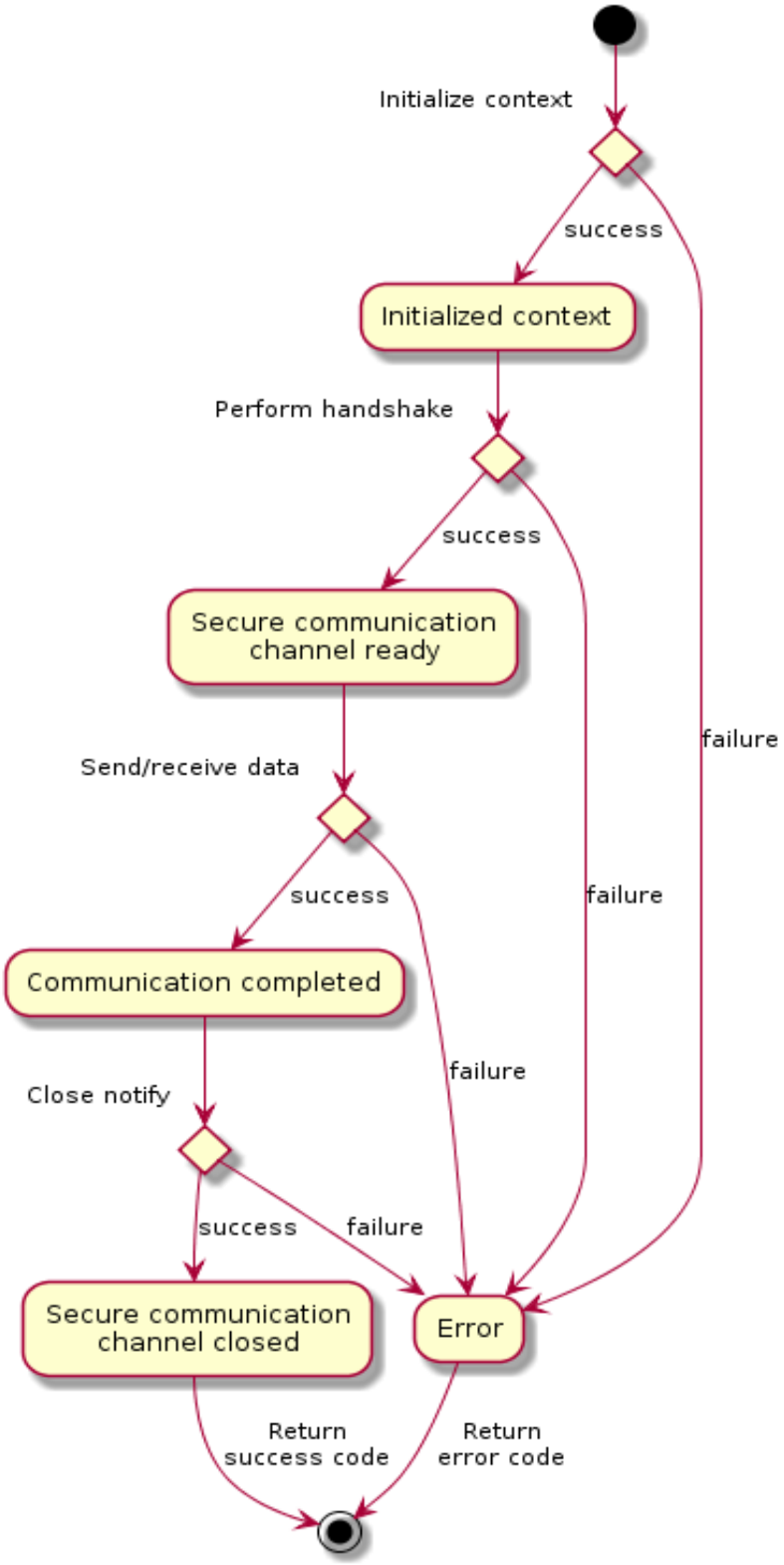
After SSLv3, SSL was renamed to TLS (Transport Layer Security). When thePOODLE vulnerabilitycame out in 2014, it was hailed as the death knell for SSL version 3. In the quarter just prior to POODLE, 98% of Internet sites supported SSLv3, but a year later that support had dropped to just 33%.

***Key exchange or key agreement***: Prior to a customer and server can start to trade data ensured by TLS, they should safely trade or concur upon an encryption key and a cipher to use when encrypting data. Among the methods used for key exchange/agreement are: public and private keys generated with RSA.

| Key exchange/agreement and authentication | | | |
|---|---|---|---|
| **Algorithm** | **SSL 2.0** | **SSL 3.0** | **TLS** |
| RSA | Yes | Yes | Yes |
| DH-RSA | No | Yes | Yes |
| DHE-RSA (forward secrecy) | No | Yes | Yes |
| ECDH-RSA | No | No | Yes |
| ECDHE-RSA (forward secrecy) | No | No | Yes |
| DH-DSS | No | Yes | Yes |
| DHE-DSS (forward secrecy) | No | Yes | Yes |
| ECDH-ECDSA | No | No | Yes |
| ECDHE-ECDSA (forward secrecy) | No | No | Yes |
| PSK | No | No | Yes |
| PSK-RSA | No | No | Yes |
| DHE-PSK (forward secrecy) | No | No | Yes |
| ECDHE-PSK (forward secrecy) | No | No | Yes |
| SRP | No | No | Yes |
| SRP-DSS | No | No | Yes |
| SRP-RSA | No | No | Yes |
| Kerberos | No | No | Yes |

The underneath segment contains an abnormal state perspective of the inner state. Particularly the inside state for a SSL/TLS handshake.

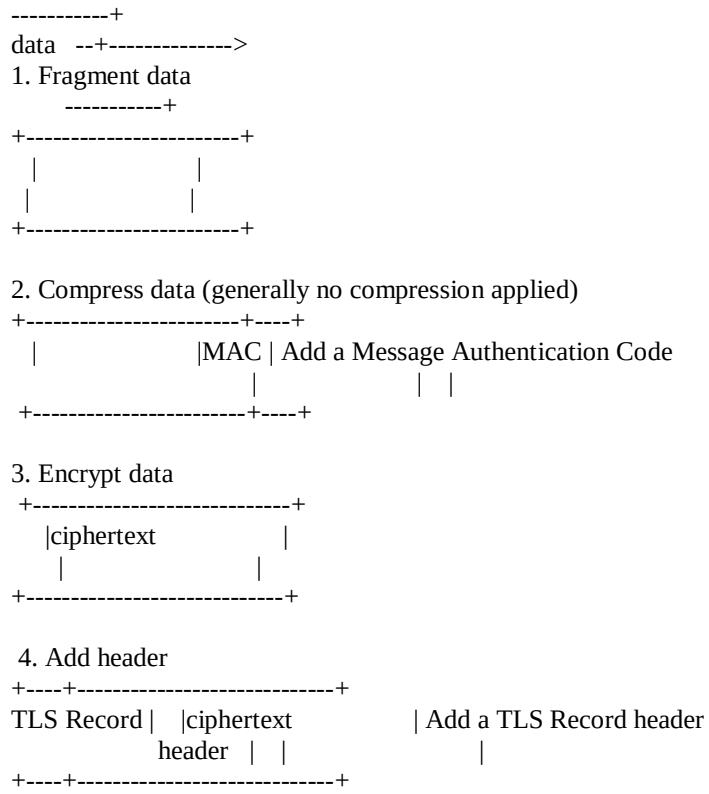
@IJAERD-2017, All rights Reserved 




**3. Traffic Analysis of an SSL/TLS Session:**

Here we will clarify what occurs at the convention level when we utilize SSL/TLS. With the end goal of this investigation we will be utilizing a non-blocking execution of a TCP client and server based on OpenSSL:

The following diagram depicts the process of building an SSL Record.




The first step in the planning of transmission of the application information comprises in its discontinuity i.e. separating the information stream to be transmitted into 16Kb (or littler) information pieces took after by the procedure of their transformation in a record. These information sections might be additionally packed, in spite of the fact that the SSL 3.0 convention determination incorporates no pressure convention, in this manner at display, no information pressure is utilized.
The record header that is added to every datum parcel contains two rudimentary snippets of data, to be specific the length of the record and the length of the information piece added to the first information.

In the subsequent stage, the record information developed comprises of the accompanying components:

- primary data,
- some padding to complete the datagram as required,
- MAC value.

MAC is responsible of the integrity of the message included into the transmitted record. MAC = Hash function [secret key, primary data, padding, sequence number].
A secret key in creation of MAC is either a client write MAC secret or a server write MAC secret respectively, it relies upon which party readies the bundle. In the wake of accepting the bundle, the getting party registers its own estimation of the MAC and contrasts it and that got. On the off chance that the two esteems coordinate, this implies information has not been changed amid the transmission over the system. Next, the information in addition to the MAC are scrambled utilizing a preset symmetric encryption calculation. This readied information is joined with the accompanying header fields:

- Content type:distinguisheswhat payload is conveyed by the bundle to figure out which higher conventions are to be utilized for preparing of information incorporated into thepacket.
- Major version: establishes the main portion of the protocol version to be used. For SSL 3.0, the value is 3,
- Minor version: establishes the additional portion of the used version of the protocol. For SSL 3.0 the value is 0.

@IJAERD-2017, All rights Reserved 

The entire process of preparation of the packet to be sent is illustrated in Figure 3.

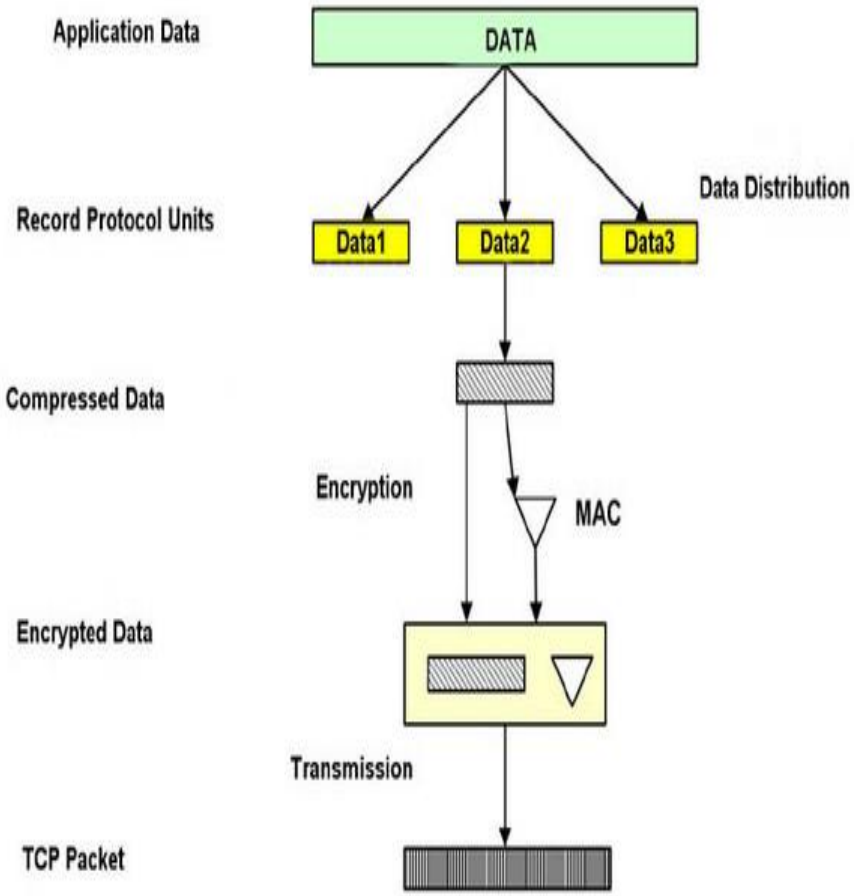



*Figure 3: Creating a packet under SSL record protocol*

**4. CONCLUSION:**

SSL is utilized as a part of many administrations however generally SSL ensures the HTTP correspondence channel over the Internet and thusly the SSL convention is seen frequently as related just with WWW pages. As it has been as of now said, the SSL convention can be utilized to secure the transmission for any TCP/IP benefit. The second in all likelihood use of this convention is related with email sending and getting. Concerning Windows NT/2000/XP applications, SSL is basically utilized as a part of the arrangement of HTTP and SMTP server benefits that work in conjunction with IIS. These servers enable a suitable demand to be produced by acquiring the certificate from one of the trusted CAs such as VeriSign.

**REFERENCES:**

[1] A Santhoshi, Dr.R.ChinaAppala Naidu, E. Sowmya and K Meghana " A Modern Approach for Data Transformation in networks with new methodology" International Journal of innovative research in Computer and communication Engineering, ISSN (online) :2320-9801, ISSN (print) :2320-9798, Volume 3, Issue 9, pp.8964-8969, September 2015.

[2] A. Freier, P. Karlton, P. Kocher "The Secure Sockets Layer (SSL) Protocol Version 3.0", August 2011.

[3] EkkuluriRamlal and R.ChinaAppala Naidu "Encrypted: A Secure File Transfer Application" International Journal of Advanced and Innovative Research ISSN: 2278-7844, Vol 4, Issue 6, Pp.143-147, 2015.

[4] Y. Wang, S. Wenger, J. Wen, and A. K. Katsaggelos, ―Real-time communications over unreliable networks,‖ IEEE Signal Process. Mag., vol. 17, no. 4, pp. 61–82, Jul. 2000

[5] Krishna Kant, Ravi Iyer and PrasantMahapatra, " ArchitecturalImpact of Secure Socket Layer on Internet Servers", Sep. 2000.

[6]S.Rekha and R.ChinaAppala Naidu "Implementation of Spontaneous Wireless Ad-hoc Network for Secure Data Transmission" International Journal of Scientific Engineering and Technology Research, ISSN: 2319-8885, Vol 4, Issue 14, Pp.2591-2595, June-2015.

[7] T. Dierks, E. Rescorla "The Transport Layer Security (TLS)Protocol, Version 1.2", August 2008.

[8] S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H., "An Architecture for a Secure Service DiscoveryService," Proc. ACM/IEEE MobiCom, Aug. 1999.

[9] S.Soumya and R.ChinaAppala Naidu" A Secure way for Privacy Prescribed Profile Matching in Mobile Social Networks" International Journal Of Eminent Engineering Technologies, Vol 2, Issue 4, Pp.88-95, June-2015.

[10] Thomas Y. C. Woo, RaghuramBindignavle, Shaowen Su andSimon S. Lam, "SNP: An interface for secure network programming proceedings USENIX Summer Technical Conference", June 1994.

@IJAERD-2017, All rights Reserved 