IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115115

Secure Socket Layer in the Network and Web Security

RAM AGASHE[1], AKASH PAUL[2], UDAY AWARE[3], CHINMAY KHOPKAR[4], VRUSHABH GIRI[5]

Students, Department of Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur, India

Abstract: The Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet. In order to electronically exchange information between network users in the web of data, different software such as outlook is presented. So, the traffic of users on a site or even the floors of a building can be decreased as a result of applying a secure and reliable data sharing software. It is essential to provide a fast, secure and reliable network system in the data sharing webs to create an advanced communication systems in the users of network. In the present research work, different encoding methods and algorithms in data sharing systems is studied in order to increase security of data sharing systems by preventing the access of hackers to the transferred data. To increase security in the networks, the possibility of textual conversation between customers of a local network is studied. Application of the encryption and decryption algorithms is studied in order to increase security in networks by preventing hackers from infiltrating. As a result, a reliable and secure communication system between members of a network can be provided by preventing additional traffic in the website environment in order to increase speed, accuracy and security in the network and web systems of data sharing.

INTRODUCTION

SSL (Secure Sockets Layer) is a protocol that provides a secure channel between two machines, and facilities for protecting data in transit and identifying the machine with which you are communicating. Software such as Outlook Software was introduced to provide electronic exchange information between users on the web. The need to use these new connections reduces user congestion on the site or even under the site. In the meantime, such examples as face, safety, and honesty are of utmost importance. Security and reliability are important issues for messages sent to the site with minimal error.Encryption is the science of codes and codes. It is an ancient art and has been used for centuries to protect messages between administrators, spies, loved ones, and others in order to keep their messages private. When working with data security, it is important to verify the identity of the sender and recipient of the message. Also, it is necessary to make sure that the content of the message does not change in the data transfer system.These three issues, privacy, authentication, and understanding, are the basis for modern data security and can be used for encryption.

In this paper, various encryption algorithms have been introduced to prevent hackers from entering. The aim is to provide a complete and consistent defencemodel that can be used according to the capabilities of the organisation. The use of Secure Sockets Layer (SSL) is increasing the security of web data sharing is being studied and an improved secure data sharing system is also being developed. As a result, the security and reliability of network systems can be increased to maximise the benefits of information technology in human life.
A review of research activities is presented in Phase II. The use of SSL on network and web security is presented in Section II. The advanced software for research is introduced in Phase IV. Finally, the results obtained are presented in Section V.

OBJECTIVES AND SCOPE

This report is intended to serve as a starting point for learning the basics of how SSL works. Information on how SSL termination devices are used in the Web server environment is also included. Because this report is intended for a technical audience, a basic understanding of network infrastructure and security concepts is considered. The SSL protocol is primarily intended for students who will be learning network security and for those conducting privacy protocol analysis. The spec is written with this in mind, and is intended to reflect the needs of the two groups. For that reason, this document is intended to provide specific details of the service description and description of the interface included in the report body. Secure Socket Layer (SSL) is an effective way to protect data sent through a local or wide network. Works by encrypting data sent over the network, It can be configured on both wireless and wireless networks and will work with other security features such as WPA keys and firewalls.To provide public key-based authentication, secure session key

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115115

installation, and symmetric key based on traffic secrecy, Secure Sockets Layer Security / SSL / TLS Security--1-enabled applications. Secure communication using DNA cryptography with SSL protocol on wireless nerve networks introduced [2] to provide a secure channel with secure information exchange on wireless nerve networks. To provide an improved Network Security Processor on the data web, the design of the A Gbps IPSec SSL security processor is investigated by [3]. The application of the Java Secure Socket Extension API was introduced by [4] to prevent security risks to software development programs. SSL certificate authentication is under investigation [5] to verify SSL certificates using the automatic learning concepts (LA). To increase security on data sharing systems on networks, the most recent SSL security attacks are analysed by [6]. Designing and implementing an effective network security processor introduced by [7] to develop network security processors (NSPs) in data sharing systems. An integrated approach to ensuring data security on cloud computing is introduced by [8] to increase security on data sharing networks.

SSL APPLICATIONS

SSL was originally created to protect web traffic information, especially data transmitted between web browsers and servers. For example, if you are using Internet Banking and you see https: // and a small lock in the lower right corner of a web browser, you are using SSL. It then grew to work with other applications such as telnet, printers and FTP software to become an international Internet security solution. Its original design objectives are still used today by many online retailers and banks to protect sensitive data, such as credit card numbers, customer records etc. SSL uses the highest encryption standards and is trusted by banks around the world as it is less likely to be breached. According to VeriSignTM, the leading SSL Certificate Authority (CA) 1 online, it will take a 'lifetime' attacker to break a standard encrypted SSL document. SSL is a standard, registered technology for secure communication between a web server and an Internet browser or mail server and mail client (e.g., Outlook). This secure connection protects all information we transmit between the web server and the Internet browser (user) to keep it confidential and secure. SSL is an industry standard and is used by millions of websites worldwide to ensure data security. SSL is the solution to secure communication between a server and a service provider, provided by Netscape. In fact, SSL is a lower protocol than the application layer (TCP / IP layer 4 in the TCP / IP model). The advantage of using this protocol is its embedded use security features to protect secure application layer protocols such as HTTP and HTTPS. Based on that, cryptographic algorithms are used in plain text that must pass through an unprotected communication channel such as the Internet, and ensure that the data is kept confidential throughout the transmission channel. An SSL certificate is required for a website to have a secure SSL connection. The connection between a web browser and a web server using SSL is shown in Fig-1 [9] To create security on websites, the security level of https is provided using a server identification system. The public key of the server is sent to the browser to protect your website content. Then, it is controlled by the browser to check the validity of the certificate used. Therefore, verification and verification of the supposed certificate is authorised by the browser in order to obtain a response from the key used in the website server [9]. For authenticated clients and servers, SSL works to authenticate clients and servers using digital certificates, and encryption / decryption using specific keys that need to be verified at the Cortication Authority (CA) certification centre. The function of the CA is to identify the parties to the relationship, addresses, bank accounts and the date of expiry of the certificate, and to determine the identity documents based on them. By using the advanced feature in SSL, the user is verified by server authentication. SSL-based software on the receiving side (for example, a web browser such as Internet Explorer) for standard key-based encryption and comparison of public server keys (such as a web service provider like IIS) can be used. to identify a user on a website. Then, the user can enter his or her details such as credit card numbers or passwords with a high level of security and reliability. The SSL system can use a combination of symmetrical and asymmetric encryption. Symmetric key encryption is faster than public key encryption, and on the other hand, public key encryption provides more robust authentication techniques. A secure SSL connection such as the "SSL Handshake" is generated when users attempt to access secure website content. The process and keys produced in the security functions are not visible to the user. In order to encrypt all transferred data, anything encrypted with the public key can be encrypted with a secret encryption, and vice versa [9].

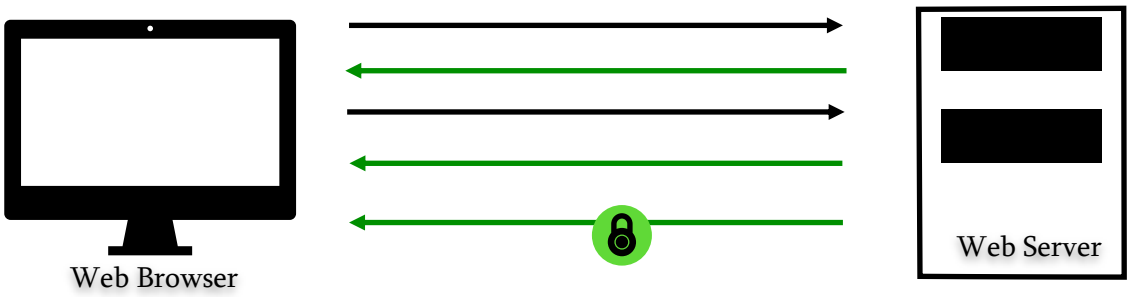

Fig.1 The connection between the web browser and WebServer using the SSL system [9]

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115115

FAMILY TREE OF SSL

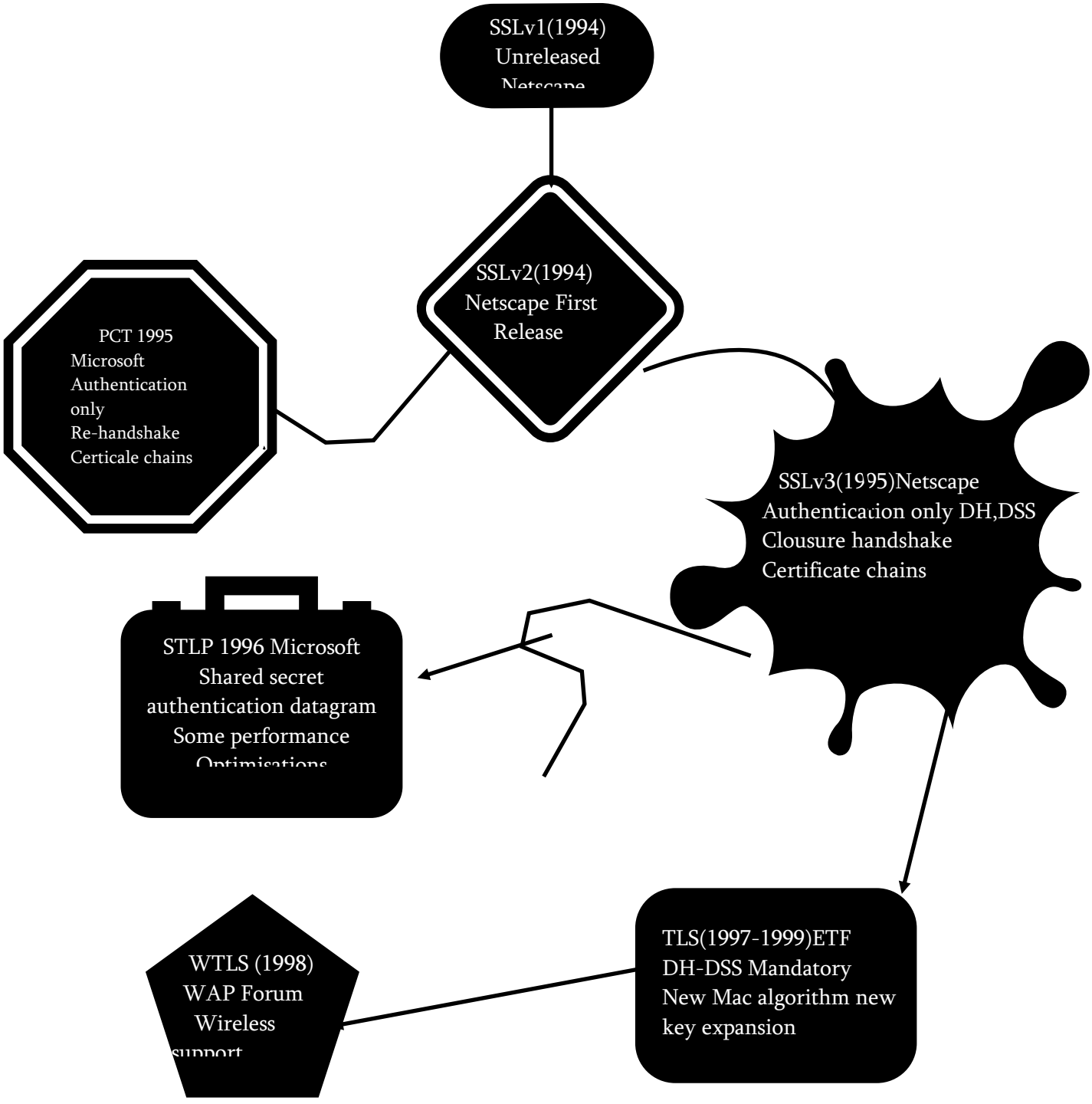

Fig.2 The main dialogue box of the developed software

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115115

CONCLUSION

Improved data sharing systems have recently been introduced due to the need for information exchange between data websites. In this study, various encryption algorithms were introduced to prevent hackers from entering. The purpose of the current research work is to provide a complete and consistent defence model that can be used within the organisations capabilities. Advanced research software is introduced and the program algorithm is explained. By connecting between two computers, the user can consider features such as sending various files and voice and voicemail calls, etc., in addition to text chat. Therefore, an improved secure communication system on data websites can be provided using an advanced research system. The results obtained proved the reliability and power of advanced software for research that can be used online (Like yahoo messenger software). The Secure Sockets Layer (SSL) protocol uses a combination of public key and symmetric key encryption. Symmetric key encryption is much faster than public key encryption; However, encryption for public keys provides better authentication strategies. An SSL session always starts with an exchange of messages called an SSL handshake. Handshake allows the server to authenticate to the client using public key strategies, and then allows the client and server to work together to create symmetric keys for faster encryption, encryption, and interruption detection during the next session. Voluntarily, shaking hands also allows the client to authenticate themselves on the server.

In creating security patterns, balance between the user and the security system is very important. In addition, the process of changing and updating security technologies should be expectations in line with new standards and threats. Consumers of the security system are still struggling with many security issues. Some organisations purchase expensive security equipment to ensure their security on the data web, which is beyond the scope of the organisation. Over-protection system organisation is a waste of money. Also, a flawed defence system will have little effect on the organisation's performance, and it is a waste of time and energy.

As a result, it is important to provide an improved communication system on the data web by taking into account the needs and threats to maximise the benefits of information technology in human life.

FUTURE SCOPE

SSL is essential for Web security. Provides a strong sense of privacy, message integrity, and server authentication for users. At the moment, SSL / TLS is not only the basis of E-commerce but also of any secure information exchange across the internet that is closely linked to consumer confidence in SSL performance across the net. In the future, SSL termination devices will be able to handle additional transactions at a faster rate. Key encryption and the cipher suites used will also continue to appear to ensure the security of sensitive information on the web. In this way, e-commerce will be able to continue to grow in popularity as users grow more privacy in online shopping and banking, and embrace new online apps.In future work, other counters such as network usage and congestion measure, CPU performance counters such as processor time of thread and user time of thread can be incorporated in the study and analysed using different workload sizes. Other Operating System Environments such as Linux can be used in the study with perf tool. The study can also be advanced by analysing real life SSL applications such as e-commerce applications.

REFERENCES

[1] Himanshu V Taiwade,., and Premchand B. Ambhore. "Amalgamation of Blockchain Technology and Cloud Computing for a Secure and More Adaptable Cloud." In Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0, pp. 87-102. CRC Press, 2021

[2] M.L. Das, N. Samdaria, “On the security of SSL/TLS-enabled applications” Appl. Comput. Inform. 2014, 10(1-2), pp.68-81.

[3] S. Upadhyaya, “Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks” Proced. Comput. Sci. 2015, 70, pp.808-813.

[4] H.Wang, G. Bai, and H. Chen, “A gbps ipsec ssl security processor design and implementation in an fpga prototyping platform” J. Signal Process. Syst. 2010, 58(3), pp.311-324.

[5] C. Wijayarathna, N.A.G. Arachchilage, “Why Johnny can’t develop a secure application? A usability analysis of Java Secure Socket Extension API” Comput. Secur. 2019, 80, pp.54-73.

[6] P.V Krishna, S.Misra, D. Joshi, A. Gupta and M.S. Obaidat, “Secure socket layer certificate verification: a learning automata approach” Secur. Commun. Networ. 2014, 7(11), pp.1712-1718.

[7] W.El-Hajj, “The most recent SSL security attacks: origins, implementation, evaluation, and suggested countermeasures” Secur. Commun. Networ. 2012, 5(1), pp.113-124.

[8] H. Wang, G. Bai and H. Chen, “Design and implementation of a high performance network security processor” Int. J. Electron. 2010, 97(3), pp.309-325.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115115

[9] S.K. Sood, "A combined approach to ensure data security in cloud computing" J. Networ. Comput. Appl., 2012, 35(6), pp.1831-1838.
[10].Owasp.org. (2016). Category:Attack - OWASP. [online] Available at: https://www.owasp.org/index.php/Category:Attack [Accessed 14 Apr. 2016].
[11]. Thomas Østdahl, "Security Issues with Content Management Systems (CMSs) on the Cloud", 2011
[12]. IMPERVA, 2015 Web Application Attack Report (WAAR) 6th edition, 2015.
[13]. Issues List. (2016). Joomla! Issue Tracker - CMS. [online] Available at: https://issues.joomla.org [Accessed 2 Feb. 2016]
[14]. Sirinam, Payap, et al. "Deep fingerprinting: Undermining website fingerprinting defenses with deep learning." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018.
[15]. Hadsell, Raia, Sumit Chopra, and Yann LeCun. "Dimensionality reduction by learning an invariant mapping." 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06). Vol. 2. IEEE, 2006