Web Information protection by using SSL Algorithm

Peramgani Nagasubbarayudu\textsuperscript{1}, Prof.M Kusuma\textsuperscript{2}

\textsuperscript{1}Peramgani Nagasubbarayudu, Dept of MCA, EAIMS, Peddulapalli, Kadapa, AP, India
\textsuperscript{2}Professor, Dept of MCA, EAIMS, Tirupati, AP, India

Abstract- The main objective of this project is to send the confidential details and related confidential files and documents to their recipients in a secure way. Cryptolog for Security will use the numerous kinds of algorithms to generate the encrypted strings, files and decrypted strings, files. The Secure Sockets Layer (SSL) is a common Encryption protocol used in Cryptolog. When you see a URL in your Web browser that starts with "https" instead of "http", it is a secure connection that is using SSL. Some methods of cryptography used a "secret key" to allow the recipient to decrypt the message. The most common secret key cryptosystem is the Data Encryption Standard (DES), or the more secure Triple-DES which encrypts the data three times.

Index Terms- SSL algorithm, cryptography, Encryption, Decryption.

INTRODUCTION

Originally developed by Netscape Communications to allow secure access of a browser to a Web server, Secure Sockets Layer (SSL) has become the accepted standard for Web security.\textsuperscript{1} The first version of SSL was never released because of problems regarding protection of credit card transactions on the Web. In 1994, Netscape created SSLv2, which made it possible to keep credit card numbers confidential and also authenticate the Web server with the use of encryption and digital certificates. In 1995, Netscape strengthened the cryptographic algorithms and resolved many of the security problems in SSLv2 with the release of SSLv3. SSLv3 now support more security algorithms than SSLv2. In Existing system, the data will be secure through the network because data transmission is done in encrypted format. In Existing system, data will not be accessed through the authorized person. The system provides security to the data store in the database. In Proposed System, the security is provided throughout the server and database by disabling the cookies etc. The main role of SSL is to provide security for Web traffic. Security includes confidentiality, message integrity, and authentication. SSL achieves these elements of security through the use of cryptography, digital signatures, and certificates. Cryptography SSL protects confidential information through the use of cryptography. Sensitive data is encrypted across public networks to achieve a level of confidentiality. There are two types of data encryption: symmetric cryptography and asymmetric cryptography (refer to Table 1). Symmetric cryptography uses the same key for encryption and decryption. An example of symmetric cryptography is a decoder ring. Alice has a ring and Bob has the same ring. Alice can encode messages to Bob using her ring as the cipher. Bob can then decode the sent message using his ring. In cryptography, the “decoder ring” is considered a preshared key. The key is agreed upon by both sides and can remain static. Both sides must know each other already and have agreed upon what key to use for the encryption and decryption of messages. Remember that the same key is used for encoding as well as decoding messages—thus the term symmetric cryptography.

The Cryptology has been divided into 5 different modules:
1. Administrator
2. User
3. Cryptic messages
4. Cryptic files
5. Image transformation

Administrator: Administrator is a superuser in the system. He will monitor all the users’ activities in the system. He has privileges to do anything at any point of time. He is responsible for providing secure mechanism for the
user of the system to send their confidential data in a secure way. (Not visible)

User:
User will register in to site and send his confidential data in a secured way by using Crypto log technology facility provided in the application.

Cryptic messages:
In this module user will send his confidential messages in an encryption format so that receiver will receive the data and he will decrypt to get original data. So that data will transmitted in a secure way.

Cryptic files:
In this module user will send data file in an encryption format so that receiver will receive the data and he will decrypt to get original data. Application provides a facility to send files in a secured way.

Image transformation:
In this module user will transmit data in the form of image and he can encrypt the image and transform to receiver. Receiver will receive the data and he will decrypt to get original data. By using this application user can send images also in a secured way.

Architecture Diagram:

Proposed algorithm:-
SSL protocol uses a combination of public-key and symmetric-key encryption to secure a connection between two machines that can be a Web or mail server and a client machine, communicating over the Internet or an internal network. SSL runs on the transport layer and the network layer. These layers are responsible for the transportation of data between the processes and the routing of network traffic between the processes and the routing of network traffic. SSL basically consists of two phases: handshake phase and data transfer phase.

Screenshots:-
Home page:

Inbox page:

Compose mail:
Sent mail:

Change password:

View profile:

After change the password:

View user profiles:

Admin login page:
CONCLUSION

The main objective of this project is to send the confidential details and connected confidential files and documents to their recipients in a very securable approach. Cryptolog for Security can use the many sorts of algorithms to get the encrypted strings, files and decrypted strings, files. The Secure Sockets Layer (SSL) may be a common coding protocol employed in Cryptolog, the info are going to be secure victimization the online technology by victimization https enabled. In projected System, the info is going to be accessed through the approved person. The system provides security to the info store within the info. In projected System, the protection is provided throughout the server and info by disabling

REFERENCES