Web Information protection by using SSL Algorithm

Peramgani Nagasubbarayudu[1], Prof.M Kusuma[2]
[1]Peramgani Nagasubbarayudu, Dept of MCA , EAIMS, Peddulapalli, Kadapa, AP, India
[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 securable 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.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 does not provide security to the data store in database. In Existing System, the security is not provided throughout the server and database. In Proposed System, the data will be secure using the web technology by using https enabled. In Proposed System, the data will 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 super user 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.

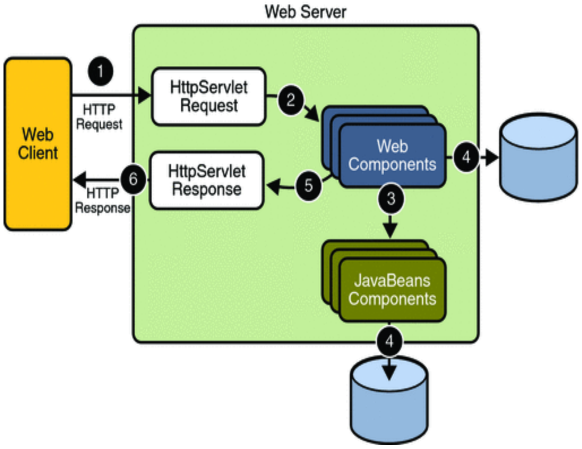
Cryptic files:

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:

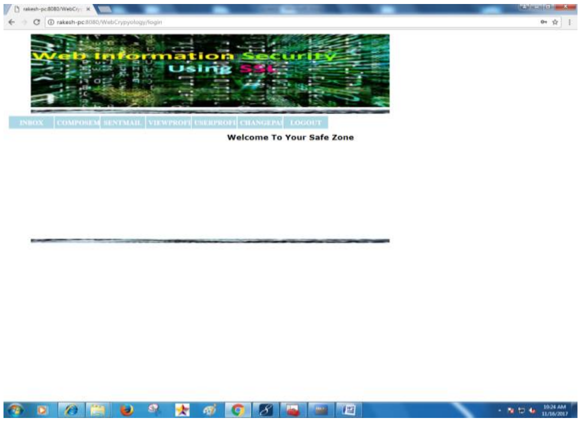


Proposed algorithm:-

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.

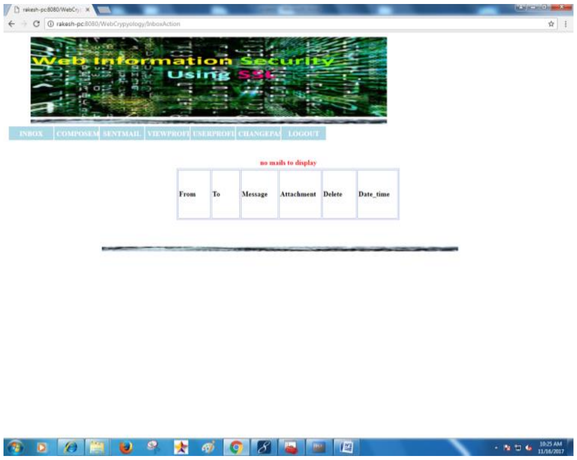
Screenshots:-

Home page:



Welcome To Your Safe Zone

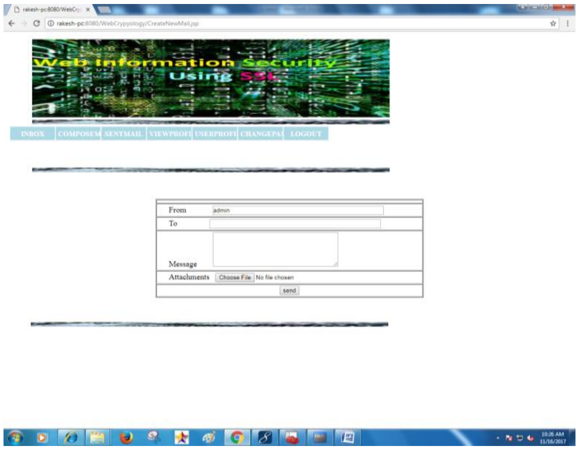
Inbox page:



no mails to display

From	To	Message	Attachment	Delete	Date_time

Compose mail:



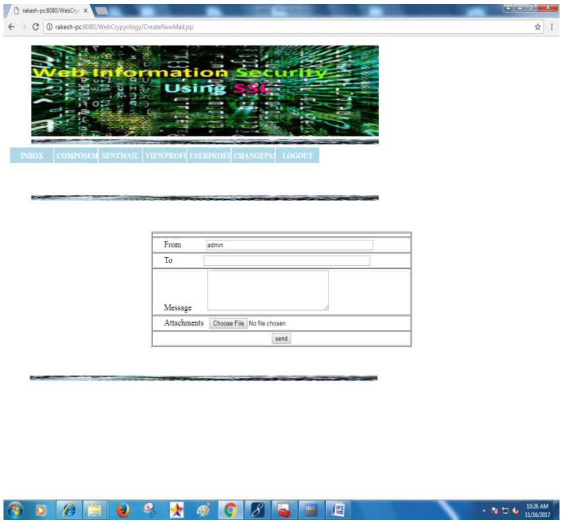
From admin

To

Message

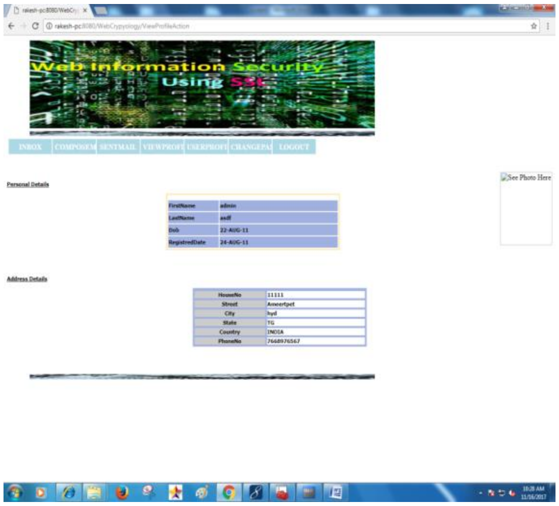
Attachments No file chosen

Sent mail:


rakesh-pc:8080/WebCrypyology/CreateNewMail.jsp
Web Information Security Using SSL
INBOX
COMPOSEM
SENTMAIL
VIEWPROFI
USERPROFI
CHANGEPA
LOGOUT
Choose File
send

From	admin
To	
Message	
Attachments	No file chosen

View profile:


rakesh-pc:8080/WebCrypyology/ViewProfileAction
Web Information Security Using SSL
INBOX
COMPOSEM
SENTMAIL
VIEWPROFI
USERPROFI
CHANGEPA
LOGOUT
See Photo Here

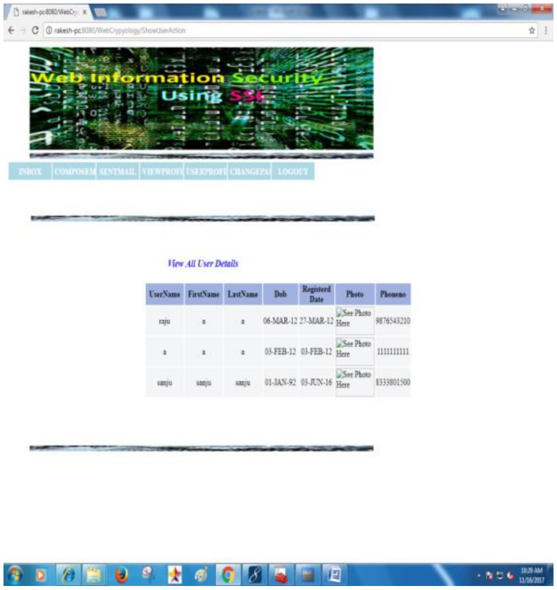
Personal Details

FirstName	admin
LastName	asdf
Dob	22-AUG-11
RegistredDate	24-AUG-11

Address Details

HouseNo	11111
Street	Ameertpet
City	hyd
State	TG
Country	INDIA
PhoneNo	7668976567

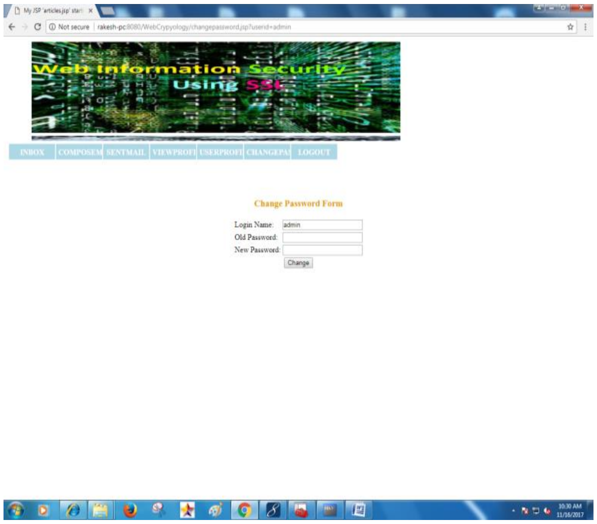
View user profiles:


rakesh-pc:8080/WebCrypyology/ShowUserAction
Web Information Security Using SSL
INBOX
COMPOSEM
SENTMAIL
VIEWPROFI
USERPROFI
CHANGEPA
LOGOUT

View All User Details

UserName	FirstName	LastName	Dob	Registerd Date	Photo	Phoneno
raju	a	a	06-MAR-12	27-MAR-12	See Photo Here	9876543210
a	a	a	03-FEB-12	03-FEB-12	See Photo Here	1111111111
sanju	sanju	sanju	01-JAN-92	03-JUN-16	See Photo Here	8333801500

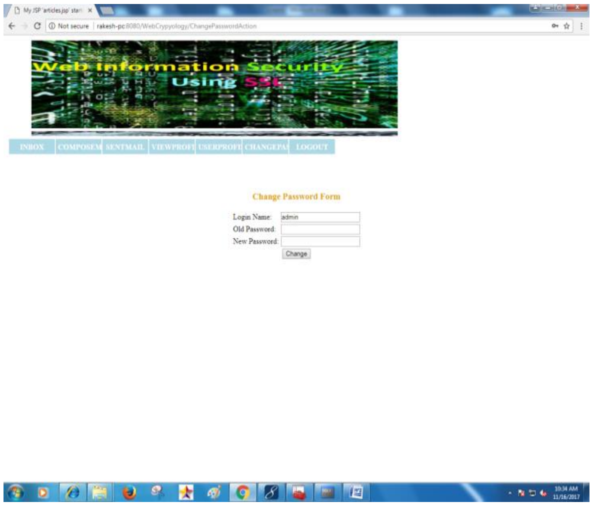
Change password:


rakesh-pc:8080/WebCrypyology/changepassword.jsp?userid=admin
Web Information Security Using SSL
INBOX
COMPOSEM
SENTMAIL
VIEWPROFI
USERPROFI
CHANGEPA
LOGOUT
Change

Change Password Form

Login Name: admin
Old Password:
New Password:

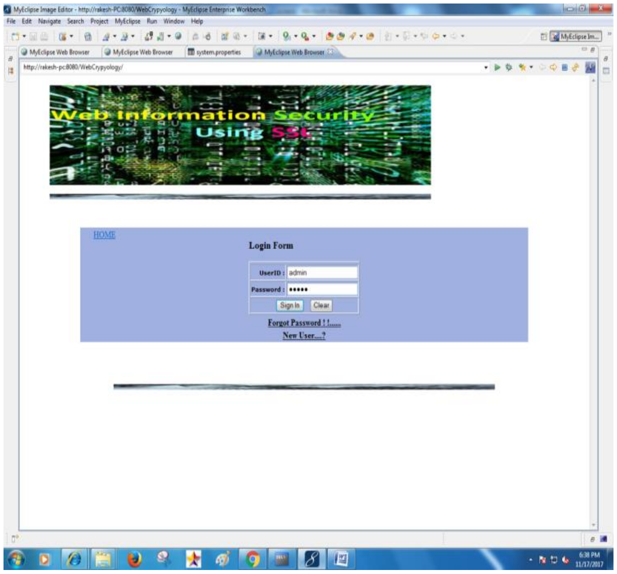
After change the password:


rakesh-pc:8080/WebCrypyology/ChangePasswordAction
Web Information Security Using SSL
INBOX
COMPOSEM
SENTMAIL
VIEWPROFI
USERPROFI
CHANGEPA
LOGOUT
Change

Change Password Form

Login Name: admin
Old Password:
New Password:

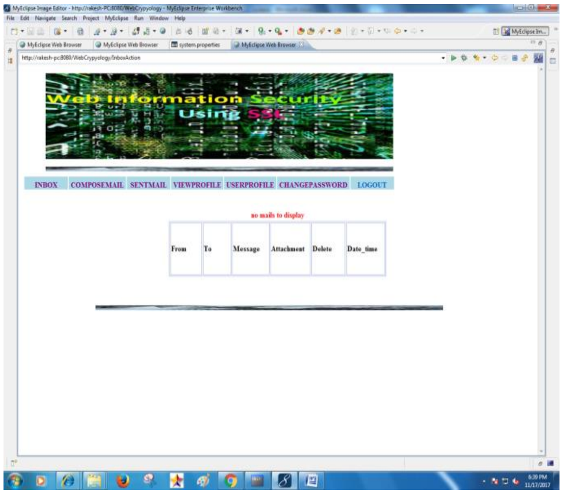
Admin login page:-


MyEclipse Image Editor - http://rakesh-PC:8080/WebCrypyology - MyEclipse Enterprise Workbench
File Edit Navigate Search Project MyEclipse Run Window Help
MyEclipse Web Browser
MyEclipse Web Browser
system.properties
MyEclipse Web Browser
http://rakesh-pc:8080/WebCrypyology/
Web Information Security Using SSL
HOME
Sign In
Clear
Forgot Password ! !......
New User....?

Login Form

UserID : admin
Password : •••••

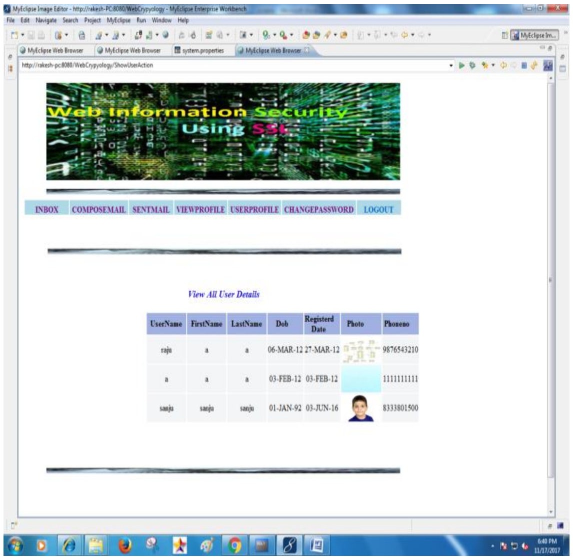
View mails:-



no mails to display

From	To	Message	Attachment	Delete	Date_time

View all users' details:-



View All User Details

UserName	FirstName	LastName	Dob	Registerd Date	Photo	Phoneno
raju	a	a	06-MAR-12	27-MAR-12		9876543210
a	a	a	03-FEB-12	03-FEB-12		1111111111
sanju	sanju	sanju	01-JAN-92	03-JUN-16		8333801500

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

[1] Kartikey Agarwal and Dr. Sanjay Kumar Dubey, "Network Security: Attacks and Defence."

[2] Mr. Pradeep Kumar Panwar and Mr. Devendra Kumar," Security through SSL ." in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012.

[3] Confidentiality integrity and availability CIA http://whatis.techtarget.com/definition.

[4] Encryption and secret key cryptography cryptography/www.wikipedia.org.

[5] Network Security: History, Importance, and Future by University of Florida Department of Electrical and Computer Engineering Bhavya Daya.

[6] Mohammed A. Alnatheer , " Secure Socket Layer (SSL) Impact on Web Server Performance ." in Journal of Advances in Computer Networks, Vol. 2, No. 3, Sept 2014.

[7] K. Kant, R. Iyer, and P. Mohapatra, "Architectural impact of secure socket layer on internet servers: A Retrospect" in Proc. International Conference on Computer Design.

[8] K. Kant, R. Iyer, and P. Mohapatra "Architectural impact of secure socket layer on internet servers" in Int. Conf. on Computer Design, pp. 7-14, 2000.

[9] SSL Certificate Explained by Scion Solutions Ltd.

[10] SSL Information Center/What is an SSL Certificatehttps://www.globalsign.com/en-in.

[11] MS.Bhiogade Patni Computer Services, Secure Socket Layer InSITE - "Where Parallels Intersect" June 2002.