

# Cryptology For Security In Web Services

T R Vinod Kumar<sup>1</sup>, H.Syed Ali Fathima<sup>2</sup>

1M.TECH, DEPARTMENT OF MCA, MOTHER THERESA INSTITUTE OF COMPUTER APPLICATIONS, PALAMANER, INDIA

2ASSISTANT PROFESSOR, HEAD OF DEPARTMENT, DEPARTMENT OF MCA, MOTHER THERESA INSTITUTE OF COMPUTER APPLICATIONS, PALAMANER, INDIA

## Abstract:-

A digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Signatures must be verifiable; Cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents. The main aim of this paper is to provide a broad review of network security and cryptography, with particular regard to digital signatures. Network security and cryptography is a subject too wide ranging to coverage about how to protect information in digital form and to provide security services. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information.

## I. INTRODUCTION

Cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve. With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. Data security is the

utmost critical issue in ensuring safe transmission of information through the internet. Also network security issues are now becoming important as society is moving towards digital information age. As more and more users connect to the internet it attracts a lot of cyber-criminals. It comprises authorization of access to information in a network, controlled by the network administrator. The task of network security not only requires ensuring the security of end systems but of the entire network. In this paper, an attempt has been made to review the various Network Security and Cryptographic concepts. This paper discusses the state of the art for a broad range of cryptographic algorithms that are used in networking applications.

In Existing system, the data will be not being secure through the network because data transmission is done in unencrypted format. In Existing system, data can be accessed by the unauthorized person. The system does not provide security to the data store in database, the security is not provided throughout the server and database.

The development of this new system contains the following activities, which try to automate the entire process keeping in the view of database integration approach. In Proposed System, the data will be secure using the web technology by using https enabled; 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.

## II. MODULES

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.

### ➤ **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.

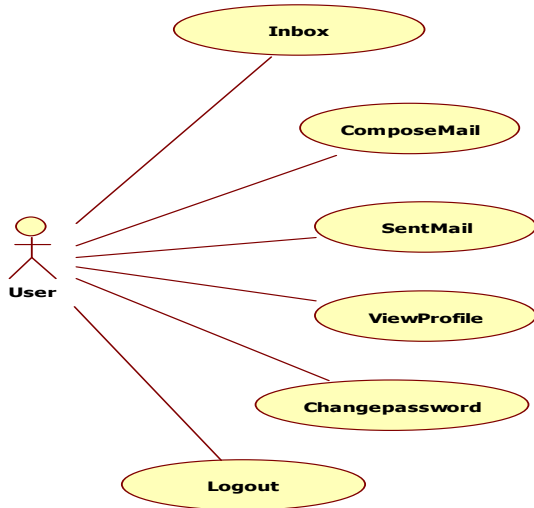
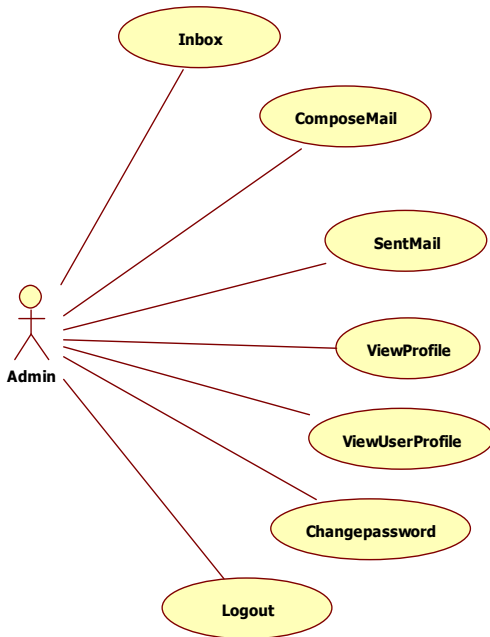
### ➤ **Image transformation:**

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.

UML diagrams:-

Administrator Use Case Diagram

User Use case Diagram:-



Screen shots:-

User login page

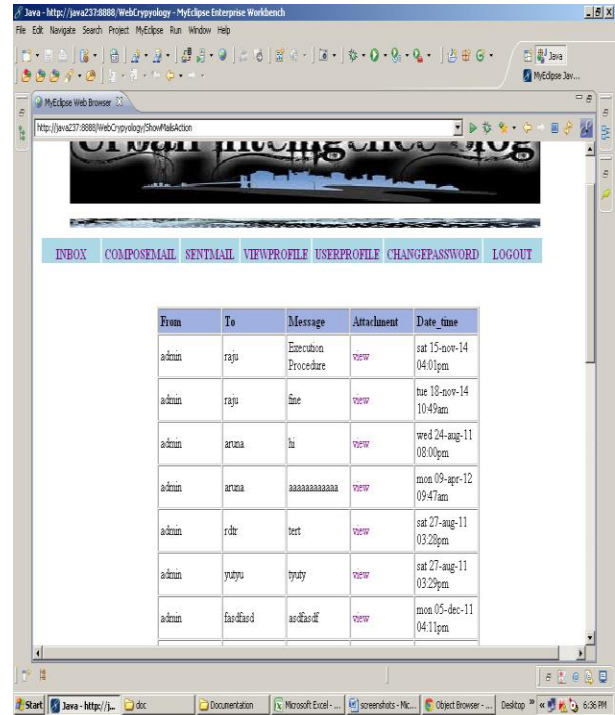
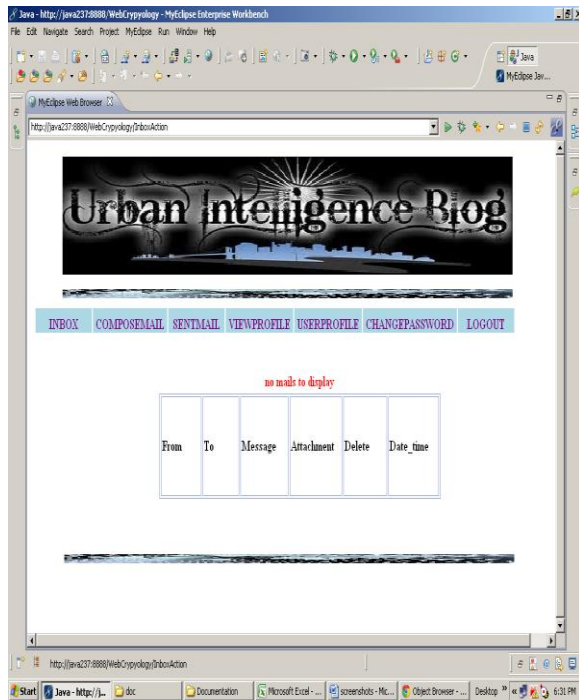


User home page



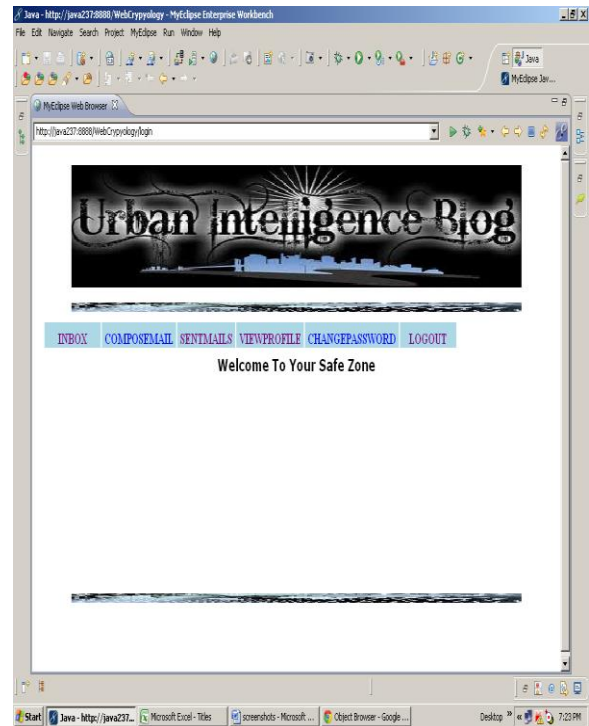
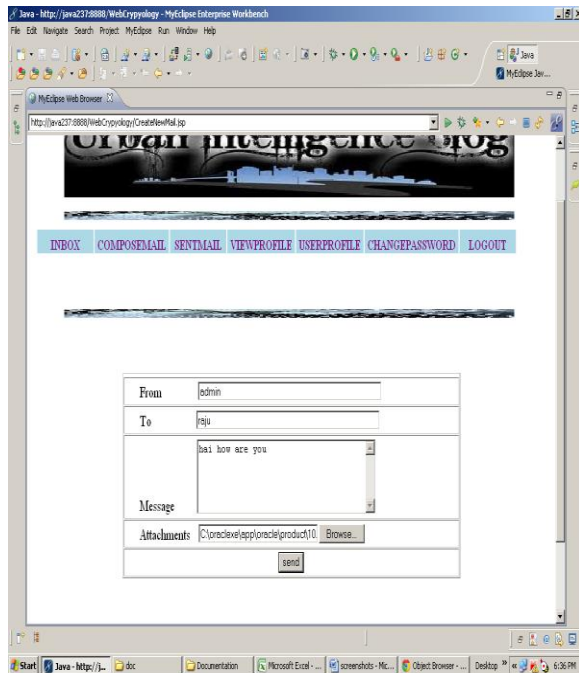
View all files

View inbox details

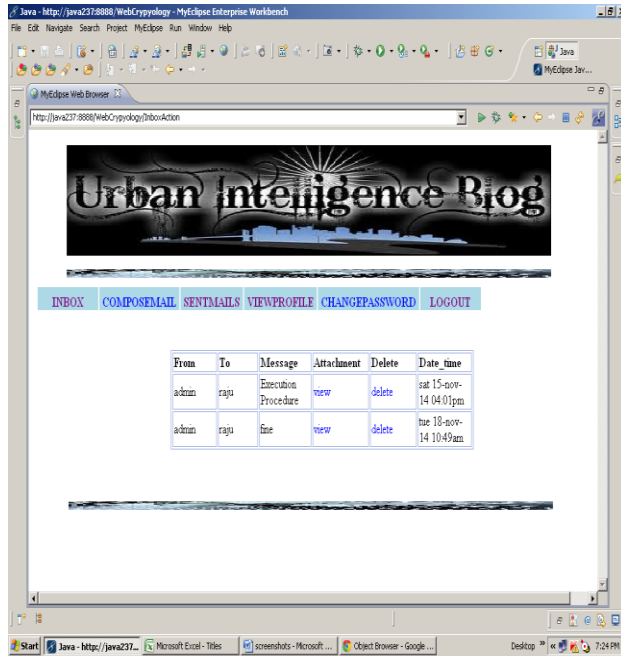


Admin home page

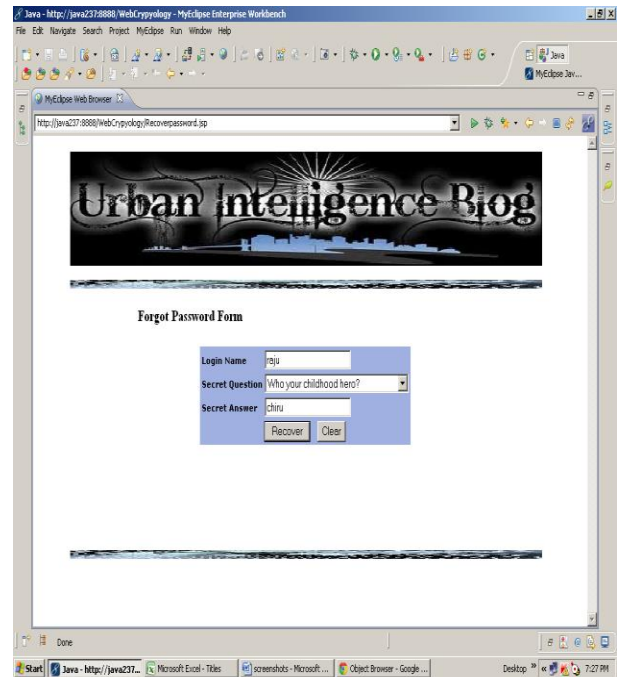
Compose a mail



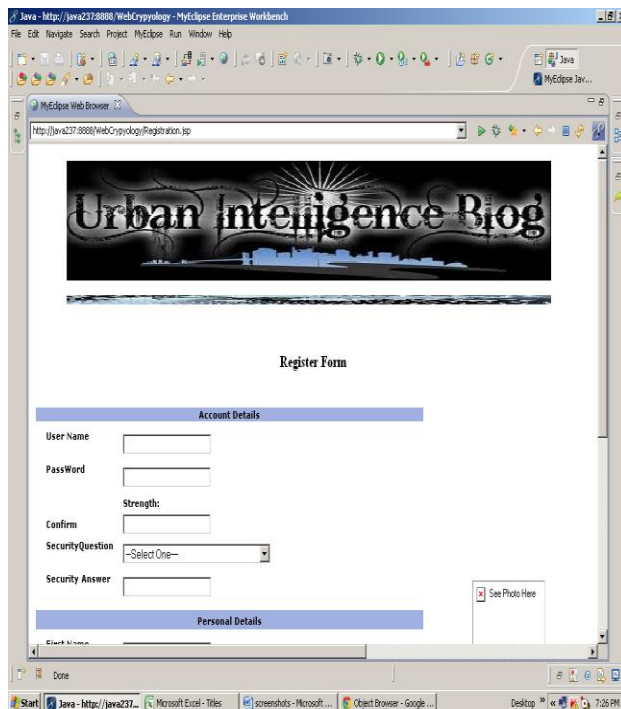
View inbox details



Change password



User registration form



III. CONCLUSION

This application A Cryptology-based Approach for Web Information Security is to send the confidential details and related confidential files and documents to their recipients in a securable way. Crypto log will use the numerous kinds of algorithms to generate the encrypted strings, files and decrypted strings, files. This application software has been computed successfully and was also tested successfully by taking “test cases”. It is user friendly, and has required options, which can be utilized by the user to perform the desired operations. Finally this application provides high security in data sharing.

#### IV. BIBLIOGRAPHY

- (1) Java Complete Reference by Herbert Shield
- (2) Database Programming with JDBC and Java by George Reese
- (3) Java and XML By Brett McLaughlin
- (4) Wiki pedía, URL: <http://www.wikipedia.org>.
- (5) Answers.com, Online Dictionary, Encyclopedia and much more, URL: <http://www.answers.com>
- (6) Google, URL: <http://www.google.co.in>
- (7)Project Management URL: <http://www.startwright.com/project.htm>