Implementation of an Application to Secure Personal Data Using Enhanced DES

GRADUATE PROJECT REPORT

Submitted to the Faculty of
The School of Engineering & Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, TX

In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

by

Swetha Devana
Spring 2014

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Longzhuang Li
Committee Member

Dr. David Thomas
Committee Member
ABSTRACT

Security is one of the important features in the field of communication system, specifically on a network and the internet. Developing applications using data encryption techniques for ensuring personal data security in network communication plays a significant role in the field of cryptography. Several block cipher techniques ensure security for personal data, when shared on the internet, like Caesar Cipher, Monoalphabetic Cipher, Polyalphabetic Cipher, Columnar Transposition, Data Encryption Standard (DES), and Advanced encryption Standard (AES).

The project provides a platform for the users to upload multiple files, along with file sharing and file downloading. The concept of Enhanced DES in encrypting and decrypting the data is practiced. The contribution done in the project is modification over the traditional DES algorithm. The transposition technique is added before the DES algorithm, thereby adding layer of security, as any attack made on the cipher text needs to break the DES algorithm followed by the transposition technique, which implies double security. The proposed report concerning the features and functionality of enhances DES system in securing personal data.
# TABLE OF CONTENTS

Abstract .......................................................................................................................... ii

Table of Contents .......................................................................................................... iii

List of Figures ................................................................................................................ vi

List of Tables ................................................................................................................ viii

1. Introduction ............................................................................................................... 1
   1.1 Data Encryption Standard (DES) ......................................................................... 1
       1.1.1 Double DES .................................................................................................. 1
       1.1.2 Triple DES .................................................................................................. 3
   1.2 Different attacks on DES ....................................................................................... 4
       1.2.1 Brute Force Attacks ..................................................................................... 4
       1.2.2 Meet-in-the-Middle Attack .......................................................................... 5
       1.2.3 Linear Cryptanalysis .................................................................................... 6
       1.2.4 Differential Cryptanalysis ............................................................................ 6

2. Background and Rationale ......................................................................................... 8
   2.1 Classical Techniques .............................................................................................. 8
       2.1.1 Caesar Cipher ............................................................................................... 8
       2.1.2 Monoalphabetic Cipher ................................................................................. 8
       2.1.3 Polyalphabetic Cipher .................................................................................. 9
       2.1.4 Columnar Transposition .............................................................................. 9
   2.2 Data Encryption Standard ..................................................................................... 9
   2.3 Advanced Encryption Standard ......................................................................... 10

3. Narrative .................................................................................................................... 11
3.1 Problem Statement .................................................................11
3.2 Scope ..............................................................................11
3.3 Functionalities ...................................................................13

4. System Design and Implementation ........................................14
4.1 Framework .........................................................................14
4.2 Step-by-step process of project development .......................15
4.3 System Requirements ..........................................................16
4.4 System Architecture .........................................................17
4.5 Methodology .......................................................................17
4.6 Flow of execution ..................................................................20

5. Functionality of the application ...............................................21
5.1 Modules .............................................................................21
   5.1.1 Authentication Module ..................................................21
   5.1.2 Multi File Uploading Module ..........................................21
   5.1.3 File Downloading Module .............................................21
   5.1.4 File Sharing Module .....................................................22
   5.1.5 File Searching Module .................................................22
5.2 User Interface .......................................................................22
   5.2.1 Registration Page ..........................................................22
   5.2.2 Login Page .....................................................................23
   5.2.3 User Account View .......................................................24
   5.2.4 Single File Upload ........................................................25
   5.2.5 Multiple File Upload ....................................................25
5.2.6 File Downloading.................................................................26
5.2.7 File Deletion........................................................................26
5.2.8 Creation of new folder .......................................................27
5.2.9 Account Settings .................................................................27
5.2.10 File Sharing with Single User ...........................................28
5.2.11 File Sharing with Multiple Users .......................................29
5.2.12 Downloading encrypted and decrypted files .....................29

6. Testing and Evaluation ..............................................................32
   6.1 Test cases ...........................................................................34

7. Conclusion and Future work ....................................................45

Bibliography .............................................................................47
LIST OF FIGURES

Figure 1  Encryption with 2DES using two keys K1 and K2 ........................................2
Figure 2. Decryption with 2DES using two keys K1 and K2 ........................................2
Figure 3. Encryption with 3DES using three keys K1,K2 and K3 .................................3
Figure 4. Decryption with 3DES using two keys K1 and K2 ......................................4
Figure 5. Architecture of the Proposed System ..............................................................17
Figure 6. Process of encrypting plain text .................................................................18
Figure 7. Process of decryption of the created plaintext .............................................19
Figure 8. Flow of execution of the Proposed System .................................................20
Figure 9. Screenshot of Registration Form .................................................................23
Figure 10. Screenshot of Login Page ........................................................................24
Figure 11. Screenshot of User Account ........................................................................24
Figure 12. Screenshot of Single File Upload ..............................................................25
Figure 13. Screenshot of Multiple File Upload ..........................................................25
Figure 14. Screenshot of File Download .....................................................................26
Figure 15. Screenshot of File Deletion .......................................................................26
Figure 16. Creation of New Folder ...........................................................................27
Figure 17. Screenshot of Account Settings .................................................................28
Figure 18. Screenshot of file sharing with a single user ............................................28
Figure 19. Screenshot of file sharing with multiple users ...........................................29
Figure 20. Screenshot to show downloading of Encrypted or Decrypted File ..........30
Figure 21. Screenshot showing the format of viewing Encrypted File .....................30
Figure 22. Screenshot to Decrypt the Encrypted file .................................................31
Figure 23. Screenshot showing the result of entering wrong input .............................34
Figure 24. Screenshot showing the link received to the user email..........................35
Figure 25. Screenshot showing successful activation..............................................35
Figure 26. Screenshot showing the result of entering wrong password ......................36
Figure 27. Screenshot showing multiple file uploads..............................................37
Figure 28. Screenshot showing successful file upload ............................................37
Figure 29. Screenshot showing files after successful upload in the user account ..........38
Figure 30. Screenshot showing file transfer to the user...........................................38
Figure 31. Screenshot showing the selected file being sent to the recipient...............39
Figure 32. Screenshot showing email received by the recipient to download the file.....39
Figure 33. Screenshot showing to enter key to decrypt the file..................................40
Figure 34. Screenshot showing links to download both encrypted and decrypted files ..41
Figure 35. Screenshot showing encrypted file format .............................................42
Figure 36. Screenshot showing decrypted file format .............................................42
Figure 37. Screenshot showing the settings of a particular file ..................................43
Figure 38. Screenshot showing search option of the file that is protected ..................44
Figure 39. Screenshot showing send request folder for the protected files ...............44
LIST OF TABLES

Table 1. Table showing Simple Columnar Transposition Technique..........................12
1. INTRODUCTION

Encryption is the process of encoding plain text into cipher text. Decryption is exactly the reverse of encryption, which decodes the given cipher text to plaintext. This is achieved based on two techniques namely symmetric-key cryptography and asymmetric-key cryptography. In symmetric-key cryptography, the users are allowed to use the same key for both encryption and decryption. And in asymmetric-key cryptography the users are provided with unique key for encryption and another key for decryption, Sombir, Sunil, & Sudhesh. (2013).

1.1 Data Encryption Standard (DES)

Data encryption standard is one of the most widely used symmetric cipher techniques. It is originated in 1977 at IBM, and then was adopted by U.S. Government in the Department of Defense. It is specified in ANSI X3.92 and X3.106 standards and also in the Federal FIPS 46 and 81 standards. DES uses a 56-bit length key on each 64-bit block of data. This process includes 16 rounds and can run on several modes. Similar to other private key cryptographic techniques, DES uses same private key for both sender and the receiver.

1.1.1 Double DES

Sombir, et.al. (2013), Double DES is also known as 2DES. It is similar to the working style of DES, but repeats same process 2 times and uses two keys, K1 and K2. When the plain text is given to 2DES, it applies K1 to produce a cipher, which acts as input for another cipher text which generated using another cipher text using K2. This mechanism is same for the decryption process. The figures below illustrate the process of encryption and decryption in 2DES.
Figure 1. Encryption using two keys $K1$ and $K2$

Plain text → Encrypt text with $K1$ → Cipher text → Encrypt cipher text with $K2$ → Cipher text

Figure 2. Decryption using two keys $K1$ and $K2$

Cipher text → Decrypt with $K2$ → Cipher text → Decrypt with $K1$ → Plain text
1.1.2 Triple DES

Triple DES implies applying DES three times. There exist two types of triple DES, one which uses three keys and the other uses two keys in the process of encryption and decryption. In the case of using three keys, the first key, K1 is used to encrypt plain text, followed by K2 and K3 keys, where all the keys are different from each other.

To decrypt the obtained cipher text, we need to perform the encryption operation on the plaintext using key K3, followed by K2 and K1 to get the final cipher text as the output. In the process of decryption, with two keys, we need to decrypt the plain text using K1 to get the cipher text, followed by K2, to obtain the output and finally decrypt the obtained result using K1 to get the encrypted plaintext.

Figure 3. Encryption with Triple DES using three keys K1, K2 and K3
1.2 Different attacks on DES

In the present scenario, as technology is advancing to major extent, computers with parallel processing has been discovered, which performs calculations and computations at a high speed. Many researchers and critics admit that the major drawback of DES is due to its fixed key size. Therefore the machines using latest technology like high computational and processing speed can break the DES security very easily. Few attacks done on DES are listed below.

1.2.1 Brute Force Attacks

Brute force attacks work very systematically by attempting every possible key. It is used frequently on the known plain text and also on cipher text-only attacks. Brute force attacks are always done successfully when given some finite key length along with
sufficient time. As the speed of the CPU of a machine increases, so does the probability of being attacked by the brute force attacks regarding the encryption algorithm also increases. Brute force attacks will always be able to find a solution. In any worst case, they involve traversing the entire search space. Encryption is the technique that converts the given plaintext to cipher text. The entire encryption process is referred to as diffusion, where the changed cipher text bit should be having 50% chances of being 1 or 0.

1.2.2 Meet-in-the-Middle Attack (MITM)

Meet-in-Middle attacks are also known as plaintext attacks. It is a generic attack that is applicable over several cryptographic systems. MITM attack can be integrated with other attacks that have been processed previously. All it needs is the potential to encrypt and decrypt along with the possession of the plain text and its corresponding cipher text. A simple idea to improve the security of the block cipher is by encrypting the given plain text a number of times, using different sequence of functions, based on which users think that this might increase the security of the encryption scheme, as it is going through number of encryptions, Ojha, et.al. (2010).

MITM attacks are used against the cryptographic algorithms that use multiple keys for encryption, like 2DES. 2DES is used in order to increase the strength of DES, as it uses key length of 112 bits and the DES uses 56 bits. MITM attack will always try to find the values of both plain text and cipher text, based on the composition of different functions like first function’s forward mapping is same as that of last function’s backward mapping which is almost like meeting in the middle of a composed function. A multi-dimensional MITM (MD-MITM) makes use of different combinations of MITM-attacks, in which meeting takes place in multiple positions in a composed function.
1.2.3 Linear Cryptanalysis

Linear cryptanalysis is also called as plaintext attack. Ojha, et.al. (2010), stated that this type of attack requires access pairs of plaintext along with cipher text in large amounts that has been encrypted with any unknown key. Linear cryptanalysis mainly takes care of the statistical analysis for each round of decryption performed on large amounts of cipher text. Cryptanalyst make the decryption process of each cipher text is done by making use of all possible sub keys in each round of the encryption process and the final result is taken into consideration by using the intermediate cipher text and counts the least result. A candidate key is selected based on the least random intermediate cipher produced by a sub key among all the cipher texts.

1.2.4 Differential Cryptanalysis

Differential cryptanalysis gathers information regarding the relationship between cipher texts that have been produced by two plaintexts related to each other. Differential cryptanalysis mainly concentrates on the statistical analysis of inputs and outputs of cryptographic algorithm. Then after, encryption of the plaintext is done by the cryptanalyst along with its XORed pair, by making use of all the possible sub keys. Then it takes the signs of non-randomness of every intermediate cipher text pair, Ojha, et.al. (2010). Therefore the sub key having the least random pattern is considered as the candidate key.

Both differential cryptanalysis and linear cryptanalysis attacks are relevant to each other. They are primarily used against iterative symmetric key block ciphers. Iterative ciphers are also known as product ciphers, which conduct several rounds for the encryption process using a sub key for every round. Feistel network used in DES is one
of the examples that include this process. Cryptanalyst observes the changes made in the intermediate cipher text done in between the rounds of encryption process, in both the attacks. These attacks are combined together and called as differential linear cryptanalysis.
2. BACKGROUND AND RATIONALE

Cryptology is the combination of cryptography and cryptanalysis into a single practice. Cryptography is considered as the art of securing the messages, followed by cryptographers. Likewise, cryptanalysis is considered as the art of breaking the secret code of the messages, followed by cryptanalysts, Bruce (1995).

2.1 Classical Techniques

The proposed algorithm has been developed based on some of the previous and most significant encryption techniques. These classical techniques provide us the benchmark of the security level for comparing it with the standard techniques. The main intention of these techniques is to provide authenticity, protection and privacy.

2.1.1 Caesar Cipher

Caesar cipher is one of the initial cryptography techniques used for securing the data. The mechanism followed in here is, it displaces each alphabet of the plaintext, by moving them three positions down in alphabetical order. According to Bishop (2005) and Stallings (2006), the Caesar cipher technique has the drawbacks of being easily targeted by brute force analysis, as the plaintext can be easily admitted.

2.1.2 Monoalphabetic Cipher

In this cipher technique, mapping of characters is done based on a 1:1 set. The brute force analysis is still applicable, by using the character frequency as there are basically only 25 alphabets.
2.1.3 Polyalphabetic Cipher

In this technique, each alphabet in the plaintext is correlated to one or even more alphabets in the cipher text. Stallings (2006) states that, this technique works on binary data instead of letters and the best example to explain this is the Vernam cipher which can be expressed using the expression: \( c_i = p_i (\oplus) k_i \). Here the terms \( c_i, p_i, k_i \) represents the \( i \)th binary digit of cipher text, plaintext and the key respectively. The \( (\oplus) \) represents XOR operation. Polyalphabetic cipher is a powerful as well as fast cipher technique. But still the code can be broke by using the cipher text, plaintext frequencies or sometimes both.

2.1.4 Columnar Transportation

Columnar transportation is considered as an effective cipher technique with respect to the amount of diffusion accomplished. It writes the given message into a rectangle in row by row fashion and reads it column by column. The problem with this technique is it cannot be applied in real time environment and as to make it more effective; it needs to be coupled with substitution, which needs extra runtime, Sombir, et.al. (2013).

2.2 Data Encryption Standard (DES)

The data encryption standard is a bit-oriented product, which is a combination of both substitution and transposition ciphers. It has its input, output and the key which are of 64 bits each, and are referred to as blocks, Bishop (2005). The cipher has 16 rounds each which have a separate key of 48 bits that is developed from a 64 bit key using permutations. In each round, the right half part is XORed with the left half part, with a function ‘f’.
The real strength of DES lies in this function. There are different types of DES like double DES and triple DES, which uses the standard DES algorithm for two or three times respectively. This implies that the DES is extendible for opting large key sizes. The drawback of using the traditional DES algorithm is with the fixed key size and the round numbers are applicable transferring network data, but not suitable for real time applications.

2.3 Advanced Encryption Standard (AES)

Advanced encryption standard is advancement over Data encryption standard. The needs for the usage of variable key length lead to the development of AES. Stallings (2006) mentioned that Rijndael, is an algorithm selected by the U.S National Institution of Standards and Technology (NIST), as a contender for AES. It uses keys of three different sizes 128,192 and 256 bits, along with different rounds for each size. Every round is comprised of substitutions, permutations, bit shifting and XOR additions. When compared to DES, AES works on less number of runs but has more number of operations, which it does in one round, making it inefficient from using in a network, John (2006).
3. NARRATIVE

3.1 Problem statement

The key used for encryption and decryption is considered to be the important component in Data Encryption Standard (DES). The problem arises when an attacker gets the key and tries to reveal the plaintext or any code. In the modern technology, machines with advanced computers with parallel processing have been invented, which performs calculations and computations at a very high speed. Though DES is a powerful algorithm, the advanced systems can break its security easily. So the need for improving the functioning and strength of DES has emerged. The main context is to provide security which binds authenticity, privacy and protection. This privacy issue plays a significant role when considered in network communication and also on the internet.

3.2 Scope

The main objective of this project is to provide the user a platform in the form a web application for data sharing. Here, the user has the functionalities like uploading, downloading, file searching and file sharing, file downloading and file deletion. Using this application, the user can share the data, which is available in encrypted format with a single user or with a group of people. A secret key is provided to the recipient with whom the user using this application shares the data. The recipient downloads the file using the key he receives in the email, so as to perform a secure.

DES is a powerful encryption technique that is being used and there are few drawbacks when subjected to its security factor. Therefore, the strength of DES is improved by adding a transposition technique in front of it and the total process is known
as Enhanced Data Encryption Technique (EDET), by Sombir, et.al. (2013). Performing this change in the mechanism of DES, security of the algorithm has been increased and also by employing Simple Columnar Transposition Technique with multiple rounds (SCTTMR), the security level can be increased or decreased subjected to the rounds used in the transposition technique.

The mechanism of SCTTMR can be explained by using a simple example. Consider a plaintext COME HOME TOMORROW. Now split the words in the given sentence into five columns. This can be shown using the following table.

<table>
<thead>
<tr>
<th>Column1</th>
<th>Column2</th>
<th>Column3</th>
<th>Column4</th>
<th>Column5</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>O</td>
<td>M</td>
<td>E</td>
<td>H</td>
</tr>
<tr>
<td>O</td>
<td>M</td>
<td>E</td>
<td>T</td>
<td>O</td>
</tr>
<tr>
<td>M</td>
<td>O</td>
<td>R</td>
<td>R</td>
<td>O</td>
</tr>
<tr>
<td>W</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Table showing Simple Columnar Transposition Technique

In simple columnar transposition technique, the cipher text is produced by reading the text in column randomly. Therefore, the resulted cipher text is OMOETRHOOMERCOMW (when considered the column order 2, 4, 5, 3, 1).

Brute force attacks turn weak when used against the Enhanced DES because, the intruder needs to break both DES followed by Simple Columnar technique. Thus, this entire process requires extra time in hacking the algorithm. Even if the intruder has
succeeded in hacking the key of DES, he still needs to find ways to guess the random number used in the columnar approach and finally reach the plaintext.

### 3.3 Functionalities

Using the application of securing data using Enhanced DES, the user can share the data over the network and on internet, provided with functionalities like file uploading, file downloading, file sharing and file deletion process. In this application, the user can share both text and image files. When the file is uploaded and if the user is willing to share that file with a single user, then the user will be able to send that file to that particular user using the recipient’s email ID, along with the key. Then the recipient receives an email with the link to download that file that can be downloaded using the key provided.

The user has the ability to set the permissions of sharing the file with a single user or a group of users. User shares the file in encrypted format and the recipient will decrypt and downloads the file using the key provided. This helps the users in sharing data in a secure way using Enhanced DES. The features added to this application are high security, high performance and low maintenance system.
4. System Design and Implementation

The proposed system provides a platform for the users to upload multiple files, along with file sharing and file downloading options. It uses the concept of Enhanced DES in encrypting and decrypting the while sharing file. This method is a modification of the traditional DES algorithm, where the transposition technique is added before the DES algorithm, thereby increasing its security, as any attack made on the cipher text needs to break the DES algorithm followed by the transposition technique, which implies double security.

Evaluation strategy is performed by creating a File Sharing System in which each user acts as a peer. Every user can upload a file and obtain maximum reputation. Incentives are given to those peer’s which have maximum reputation. File security is being provided to filter every malicious peer. Each peer can decide its allocation frame and Access Rights to share its resources with other neighbor peers. In our proposed system, we provide efficiency and fairness among rational users.

4.1 Framework

The plain text is converted to the cipher text using the SCTTMR, and the number of rounds is decided, based on what level of security the message should be provided with. After processing the output using the SCTTMR, the format of the output is changed to bit level as Enhanced DES works on bit level similar to the traditional DES. The hexadecimal bit level data is converted into hexadecimal byte level to reduce the size of the file, which helps in increasing the performance.
4.2 Step-by-step process of project development

The following describes a brief overview of the step by step process of securing personal data using enhanced data encryption standard:

1. Understanding the mechanism of existing Data encryption techniques that are incorporated in securing personal data.

2. Developing designs of web based encryption and decryption technique using Enhanced DES feature to secure the user uploaded data, which are in the form of text and image files.

3. The proposed web application is built on MVC architecture and is developed on Java 2 Enterprise edition technology, in which the data is collected from the user and processed through servlets and JSPs.

4. MySql enterprise data software is used in this application for building the data tables, which is hosted on WAMP server. These data tables are used to store user authentication details, user uploaded information and user sharing information.

5. User encrypted files are stored in a separate folder on the server and all these files are can be downloaded on the respective local machines of other users, when shared with them.

6. Encryption and decryption techniques are created based on the enhanced DES technique, where the security packages provided by Java are used for Secret key factory classes and also for the generation of secret keys.

7. Deployment and execution are done on the local host using WampServer.
4.3 System Requirements

The following are the basic resources required in for developing and executing the project:

**Hardware Requirements**

Processor Type : Pentium –IV or above
Speed : 2.4 GHZ
Ram : 2 GB MB RAM
Hard disk : 40 GB HD

**Software Requirements**

Operating System : Win xp/Windows 7
Programming Package : JAVA / J2EE
Tools : Eclipse.
SDK : JDK1.5.0
Backend : MySql
Server : Tomcat6.0
4.4 System Architecture

The following figure represents the architecture of Securing personal data using enhanced DES, which is a modification of the traditional DES, by developing an web application. The modules of the web application are also represented in the architecture diagram.

![Architecture Diagram]

Figure 5. Architecture of the proposed system

4.5 Methodology

The purpose of this application is to transform existing DES technique into enhanced DES apparently improving the performance and the quality of DES. This application allows users to upload the file that has to be shared to other users in a secure way while encrypting the file through Enhanced DES technique. The modified technique not only increases the performance of DES but also protects against traditional attacks where cipher key breaking takes place.
DES is a very powerful encryption algorithm but in today’s world of parallel processors and advanced computer machines DES security can be broken easily. The enhancement of DES is implemented with the help of Simple Columnar Transportation Technique with Multiple Rounds (SCTTMR). The process start with inputting a plain text then applying SCTTMR technique over it where text are replaced randomly on the basis of columns and then DES algorithm is applied over the plain text with hexadecimal secret key producing a cipher text with help of inbuilt java security features to provide high encryption.

Once a file is encrypted and shared with corresponding user in the application, a mail will be triggered where shared user will be provided with link to application along with secret key to download the encrypted file. The newly encrypted file will be downloaded from the system and if the user wants to decrypt it the below procedure of Decryption is followed to get the general content.

4.6 Flow of execution

The following figure represents the flow of execution of Application of enhanced DES for securing personal data. All the decision making that is involved in the project is also clearly depicted.

Figure 8. Flow of execution of the Proposed System
5. FUNCTIONALITY OF THE APPLICATION

Overall functionality of Application for securing personal data using enhanced DES is divided into the number of features that are implemented. Modular approach for development process is observed and implementation of each feature is considered as a module. There are different modules each for user authentication process, multi file uploading, file sharing, file downloading and file searching.

5.1 Modules

5.1.1 Authentication Module

The Authentication module provides the authentication based on the security measurements of the system. It provides a login for the existing users and also registration of new users. Anyone who registers for a new account should provide all their details and they will be receiving a confirmation link to their email. Every user using the system will be authenticated and they should login to access the system. Finally the user will be given work place to organize his files in the system’s database.

5.1.2 Multi File Uploading Module

The Multi File Uploading module allows user to upload multiple files at a time by overcoming the time factor. Users who use large amount of storage space will be convenient using this system. User can verify different uploaded files that are stored in the system’s database. This helps the user to save his time by uploading more than one file at a time.

5.1.3 File downloading Module

The File Downloading module facilitates the user for downloading the files from the database of the server. The user should provide the secrete key before he downloads
the file, which is given to the user at the time of registering for the user account. The key is sent to the user’s mail at the time of registration process. This is an essential process for transporting the documents.

5.1.4 File Sharing Module

The File Sharing module facilitates the process of sharing the files to trustworthy people by a user. The owner of a particular file can share the file with others if needed. These people should be accepted by the user and should be authorized users for using the files.

5.1.5 File Searching Module

The File Searching module provides the user with a functionality of file searching. The feature of uploading multiple files is provided for the user where the user can search any specific file at that particular instance of time.

5.2 User Interface

5.2.1 Registration Page

The administrator or any user can register themselves by filling the form and clicking on the register button. The process followed here is when the user clicks the register button, he gets a form to fill along with a submit button. After validating the form by checking the empty fields and the validating the user name and password. If all the details are valid, then a unique ID is generated and a link is sent to the email address. Else an error message is shown if the form is left incomplete.
5.2.2 Login Page

After activating the link received by the user in his email, the user will be ready to access his account. In the home page, the user can find a button by name login. Here the user enters his valid authentication details of his username and password. If the details given by the user are valid (this is verified using authentication process), then the user will be taken to his account and can be able to access various features of the system. Else an error message is popped by asking the user to enter valid username or password.
5.2.3 User account view

The user is directed to his account, where he can see all the files he has uploaded in the system. The user has the functions like file sharing, settings, along with file download and deletion option. Here the user has the option to create sub folder in his application. Single file and multiple file upload is also available for the user’s convenience.
5.2.4 Single file upload

The following screenshot shows the scenario of single file upload, where the user can upload a single file.

![Screenshot of single file upload](image1.png)

Figure 12: Screenshot of single file upload

5.2.5 Multiple file upload

The following screenshot describes the scenario of multiple file uploads. The user can upload multiple files at a time by saving his time.

![Screenshot of multiple file upload](image2.png)

Figure 13: Screenshot of multiple file upload
5.2.6 File downloading

The user can download the file he is willing to using this function on to his system.

![Figure 14: Screenshot of file download](image)

5.2.7 File deletion

The user can delete any particular file he has uploaded in the system using this functionality.

![Figure 15: Screenshot of file deletion](image)
5.2.8 Creation of new folder

The user is provided with the functionality of creating sub folders in his system. This may help the user in uploading files which may belong to a particular part of his work by differentiating between the folders he has on the system.

![Screenshot of creating new folder](https://example.com/screenshot.png)

Figure 16: Screenshot of creating new folder

5.2.9 Account Setting

The user has been provided with the setting option in the application, where he has the functionalities like changing his password, editing account setting, changing access rights, along with changing user profile details, comments and communication. This helps the user to update any of the information mentioned about at any particular instance of time.
5.2.10 File sharing with single user

This screen describes the process of the user sharing his file with a single user.
5.2.11 File sharing with multiple users

The user has also been provided with the functionality of sharing the same file with multiple users at a time.

![Screenshot of file sharing with multiple users](image)

Figure 19: Screenshot of file sharing with multiple users

5.2.12 Downloading Encrypted and Decrypted file

After sharing the file with a particular user or a group of users, the recipient will receive an email from the user who is willing to share the file. This email contains the secret key along with the link to download the file from which the recipient can download both the encrypted and decrypted file. When the user downloads the encrypted file, he cannot see any content in it. Downloading the decrypted file by using the key will help the user to view the original format of the file he received.
User can decrypted the downloaded encrypted file by using the key he has been provided with in the email.
Figure 22: Screenshot to decrypt the encrypted file
6. TESTING AND EVALUATION

Testing is the process used to check the errors in the program. It is considered as the major quality measure which is employed in software development. During testing, the program is executed with a set of test cases and the output of the program for the test cases is evaluated to determine if the program is performing as it is expected to perform.

Testing is vital to the success of the system. System testing makes a logical assumption that if all parts of the system are correct, the goal will be achieved successfully. In the testing process we test the actual system in an organization and gather errors from the new system by taking the initiative to correct them. System testing is the stage of implementation, which is aimed to ensure that the system works accurately and efficiently. The front-end and back-end connectivity are tested to be sure that the new system operates in full efficiency.

The process of testing considered as a significant one as it uncovers errors from system. For achieving this process proper input data is given to the system. So the user should have more awareness to give input data. It is important to give correct inputs for efficient testing. Inadequate or non-testing lead to errors that may appear few months later. The following problems can generate inadequate testing scenarios.

- Time delay arises between the cause and appearance of the problem.
- The effect of the system errors can be observed on the files and records within the system.

The testing process focuses on logical intervals of the software ensuring that all the statements have been tested on the function intervals, where tests are conducted to uncover errors and ensure that the defined inputs will produce actual results that agree
with the required results. Testing has to be done using the two common steps Unit testing and Integration testing.

**Unit testing**

Unit testing is also referred to as module testing. In unit testing, all the individual units of the project are tested so as to verify the functionality of each unit to see if it provides the output as expected or not. Each module of the application is tested separately to test for the expected output.

**Integration Testing**

Testing each module individually will not be sufficient in some cases, where the functionality of one unit causes hindrance to the functionality of other module. Therefore, testing is performed after making all the modules of the application work after integrating them together.
6.1 Test cases

In the project system testing is done by making the procedure level testing first. This is done by giving improper inputs; the errors occurred are noted and eliminated. This is the final step in system life cycle. Here we implement the tested error-free system into real-life environment and make necessary changes, which runs in an online fashion. The following are the test cases used to test the working of the proposed project.

**Test case 1:** Verifying the user registers successfully.

The user will be provided a link with the name `register` on the top right of the homepage. Then a new window with the registration form is given to the user. The user need to fill up all the details required in the fields given. If any of the input details are not given and user tries to click on register button, then the system will not allow further registering process.

![Figure 23: Screenshot showing the result of entering wrong input](image-url)
**Test case 2:** Verifying the link received to the user upon successful registration.

The user will be receiving an email with the activation link and the user credentials. On clicking the link, the user will be redirected to the page asking him to click on the activate button to complete his activation process.

![Figure 24: Screenshot showing link received to the user email](image1)

![Figure 25: Screenshot showing successful activation](image2)
**Test case 3:** Verifying the password changing functionality.

If the user wants to change his current password, he can change it by using the settings option in the system. The user should first provide the existing password and then he need to give the password to which he likes to change his password to and he has to re-enter the same password again. If the user enters the password wrongly for the second time, error saying mismatch password is given.

Figure 26: Screenshot showing the result of entering wrong password on the second time

**Test case 4:** Verifying if the user can upload multiple files into the system at a time.

In the proposed system, the user has the functionality to upload multiple file, in the system at a time, which helps the user to save his time by uploading more than one file at a time. User can verify different uploaded files that are stored in the systems database. Users who use large amount of storage space will be convenient using this system.
Figure 27: Screenshot showing multiple file uploads

Figure 28: Screenshot showing successful file upload
Test case 5: Verifying the sharing option with another user

The user can share the files which he has on the system by using the share option. The user needs to select the file which he is willing to share and a new window will be opened, in which the user has the option to generate the key, followed by which he needs to give a name to the file along with the recipient's email address.
The user will be getting an email with the link and the secret key to download the file. The following screenshot explains this scenario.

![Screenshot showing the selected file being sent to the recipient](image1)

Figure 31: Screenshot showing the selected file being sent to the recipient

![Screenshot showing email received by the recipient to download the file](image2)

Figure 32: Screenshot showing email received by the recipient to download the file
Test case 6: Verifying the link received by the recipient to download files

After receiving the email along with the link and the key, when the user clicks on the link, he will be redirected to the application where he can download both the encrypted and decrypted files. As the main intention of the proposed project is to show the encryption and decryption of the files, we need to download the encrypted file and decrypt the saved encrypted file using the key provided in the mail.

Figure 33: Screenshot showing to enter key to decrypt the file

After entering the secret key value in the given field, the user will be able to download the file he has been shared with. To show the mechanism running in the project, the user needs to download the encrypted file first.
Test case 7: Verifying the downloading process of encrypted and decrypted files

When the user clicks on the option *click here to download encrypted file*, the file gets downloaded and will be saved to the users system. Followed by this when the user clicks the option *click here to decrypt to het in normal format*, the user will be asked to enter the secret key, followed by which he will be asked to choose the file he want to decrypt and finally click on the decrypt process to get the file in its original format.
**Test case 8:** Verifying the file formats of both encrypted and decrypted file

When the user tries to access the encrypted file after downloading it, he cannot see the content in it. He needs to decrypt the file so as to have the original file format.

![Image of encrypted file format](image1)

*Figure 35: Screenshot showing encrypted file format*

![Image of decrypted file format](image2)

*Figure 36: Screenshot showing decrypted file format*
**Test case 9**: To verify settings of the file that is being shared in the system

The user can change the settings of the file he saved on the system. He can set the file setting to either as public or protected. When selected *public*, everyone who is having access to the application can view that particular file and when given *protected*, other users cannot see that file in the application.

![Screenshot showing the settings of a particular file](image)

Figure 37: Screenshot showing the settings of a particular file

After setting the file to protected view, other users when try to search that file, they can only see the file name in the system and they need to send request to access that folder to the user who is having that file.
Figure 38: Screenshot showing searching option of the file that is protected

Figure 39: Screenshot showing to send request folder option for the protected file
7. CONCLUSIONS AND FUTURE WORK

The scope of the proposed project is to provide the user a platform for uploading, sharing and downloading his files in network communication using a web application. The system provides the user to apply this work to text, image files. The main intention is to provide the user a high secured, high performance and low maintenance system. This process uses the Enhanced DES algorithm, which removes the defects caused by traditional DES encryption technique, by enhancing its features using Simple Columnar Transposition Technique Using Multiple Rounds in the process of encryption and decryption and the security keys are used from the hexadecimal structures, which further helps in reducing the size of the data in the system.

The proposed web application is tested considering various scenarios and also the type of inputs given by the user. This testing process is done in order to verify all the features working in this application. Different features are implemented as modules and every module is tested to get the expected working. Results of the proposed application for securing personal data using enhanced DES show that this application works successfully in sharing the data with others in a secured way. The main intention is to provide the users a web application of high performance, high secured and low maintenance system.

There is huge scope for enhancement possible in this project. The strength of the resulted encryption standard is not tested. The evaluation process can be done in the future enhancements, where different password cracking tools can be used to verify the complexity issues. Many new features can be added to the current version of the application like supporting video files, which is performed in this project based on time
and complexity issues. This application can be used in educational institutions, business organizations and in all other fields where file sharing is done, so as to provide a high security to the files that are being shared on the network.
BIBLIOGRAPHY

Alani, M.M. (2010). A DES96 - improved DES security. 7th International Multi-


Coppersmith, D. (1994). The Data Encryption Standard (DES) and Its strength Against
attacks, IBM J. RES. Develop, 3.


ASIA CCS ’07: Proceedings of the 2nd ACM symposium on Information, computer
and communications security, 350-352.

and network security. Information Communication and Embedded Systems
(ICICES), 2013 International Conference on, 346,351.

Theoretical and Advanced Information Technology.

information and communication technologies, 84-89.

Approach to Enhance the Security of Data Encryption Scheme. International Journal

