iJRASET

International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: IV Month of publication: April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41599

OTP with Triple DES

Ashwini Shahaji[1], Dr. A. Rengarajan[2]
[1]*Final Year MCA Student, Dept of MCA, School of CS & IT, Jain Deemed-to-be University, Bengaluru*
[2]*Professor, Dept of MCA, School of CS & IT, Jain Deemed-to-be University, Bengaluru*

Abstract: This study has been undertaken to develop a system where we can securely and efficiently share files. To maintain security between users, an authentication and authorization method is used. Users can upload files to the database. that file will be stored in the database. Generation of OTP will be done by Triple DES. The user will download the file using OTP received. After verification of OTP, the file will be downloaded to the user.

Keywords: Triple Des, Encryption, Decryption, OTP.

I. INTRODUCTION

All we are aware of methods of sharing files between users. Most of these methods include a system where there is a chance of attack. It has a chance of data leak, data misuse, bully, etc. To make the system more secure for data sharing it has to be strong to verify its audience. In case of any emergency or critical condition, the system should automatically deny to user's request. We aim to develop a system where we can share files between users securely and efficiently by maintaining confidentiality and integrity. Here, there will be an authenticated user who will log in to its system. It can upload the new file to the database which will be stored in the database. After that user can log out. It can search for the file it wants. It will request its database to download the file. The database will pass this request to the user database. The user’s database will generate an OTP (One Time Password) for the file. This OTP will be generated using Triple DES. Triple DES is an encryption algorithm that uses three keys for encryption. As it uses three keys, it provides more and better security as compared to another encryption algorithm. After generating OTP, it will send OTP to the user. The user will use that OTP to download the file. After OTP timeout, the user has to request again to download the file.

A. AIM

This project aims to protect the data from data breaches and misuse of the data. when we share files with the user that file should not be used by the unauthorized user. Here Triple-DES encrypts input data three times. The three keys are referred to as k1, k2, and k3. Thus, due to the use of 3 keys, triple-DES is more secure and is sometimes preferred over the normal DES. The system combines this with the OTP which will also be encrypted using triple DES

II. RELATED WORK

This project “Encryption and Decryption of files with an OTP using Triple DES” is implemented for a secure and safe way to access the transferring files and to provide multi-layers of security. For implementing and understanding this project, I have gone through research and survey papers dated up to 2021.

A few of the main papers which have been reviewed and studied are mentioned below.

The authors in these papers have explained the importance of a strong authentication system, which can provide multi-layers of security to the users of the system and safeguard them against unauthorized access

1) Secure File Transfer Protocol (SFTP) is an intranet-based tool that allows for more secure file transfers. Encryption is performed by the software itself in this case. As a result, the client plays no part in encryption or decoding. SFTP encrypts the file during transmission and decrypts the encrypted data at the receiving end. The ability to encrypt keys is one of the most essential features of SFTP. The file is encrypted using a private key during encrypted file transfer. The SFTP generates the private key from the client's registration information. To decode the encrypted file, The key must be communicated by the sender to the recipient. As a result, the encrypted file is sent along with the private key. Encryption is used here to protect the private key. That is, a static software key encrypts the private key. As a result, with this key, the recipient can quickly decrypt the contents. As a result, the encrypted transfer is quicker than SSH FTP. To increase the security of a file, SFTP supports file locking and unlocking procedures. Cryptography is used to do this modification will not work on locked files. Screen sharing is yet another capability of SFTP. The term "screen share" refers to when two or more people share their screens remote systems.
2) In this paper to improve the Key Schedule Method, a unique FORTIS algorithm is proposed in this research. When compared to

the present Triple-DES, the Verilog code was simulated and the Physical design was created using Cadence Design Suite, with the power and are having a negligible effect. The algorithm's power traces were acquired using ChipwhispererR -Lite (CW1173) using the CW-305 Artix-7 FPGA board as the target to determine the algorithm's strength. The identification of operations from the power trace became more difficult with the introduction of the Comparator and flexible shifter in the Key Schedule Algorithm, as a result of which the PGE values were reduced and the algorithm was harmed.

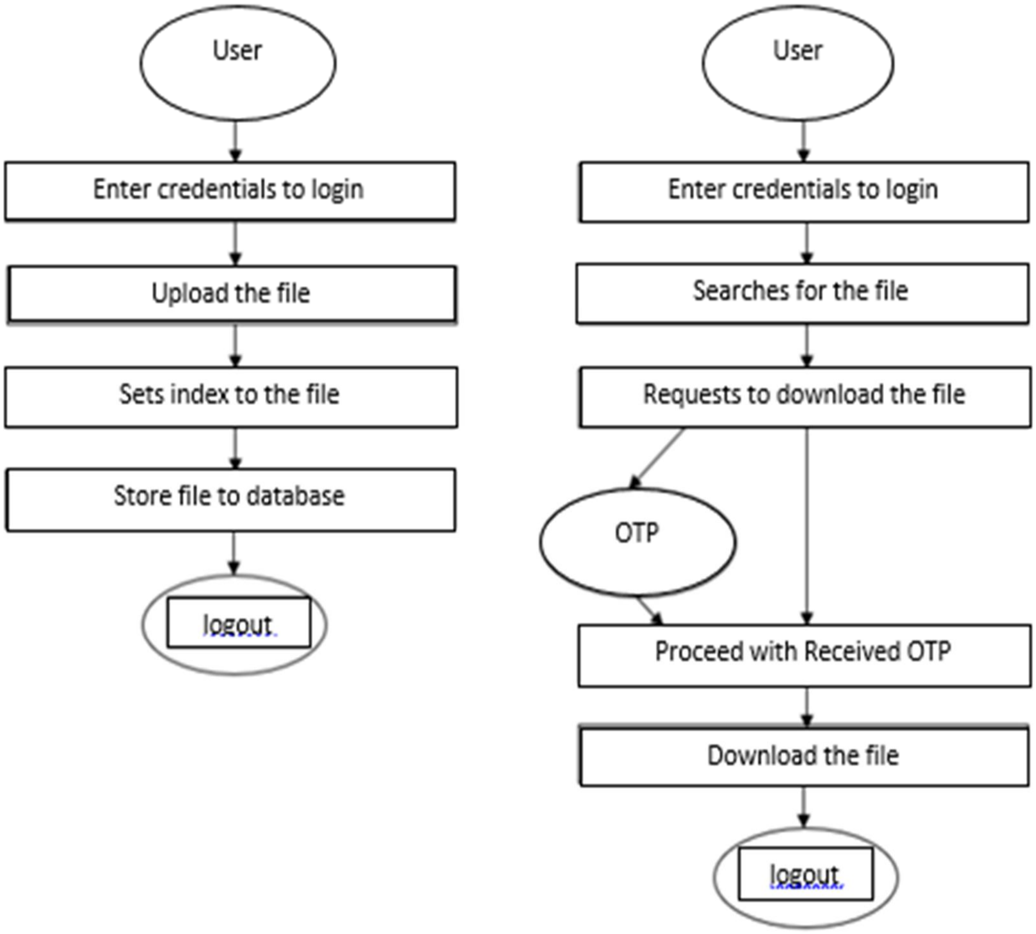
3) The AES algorithm and the chaotic sequence are used to encrypt and decrypt images in this research. The encryption and decryption processes are successfully implemented utilizing JAVA coding. To ensure the efficacy of the encryption method used, histogram analysis and adjacent pixel autocorrelation are performed on the photos. As a result, the encryption approach can withstand a variety of attacks, including brute force, cipher, and plaintext attacks.

4) The author of this research paper has proposed that this method is most effective when applied at the organizational level. Because of the Triple-DES approach employed, even if the data is hacked, the hacker will not be able to access the account. As a result, this tool is the best for security. To protect users of Gmail, Rapid Share, PayPal, eBay, and other services from being hacked. To prevent people from losing data on the internet. The use of two-factor authentication improves security.

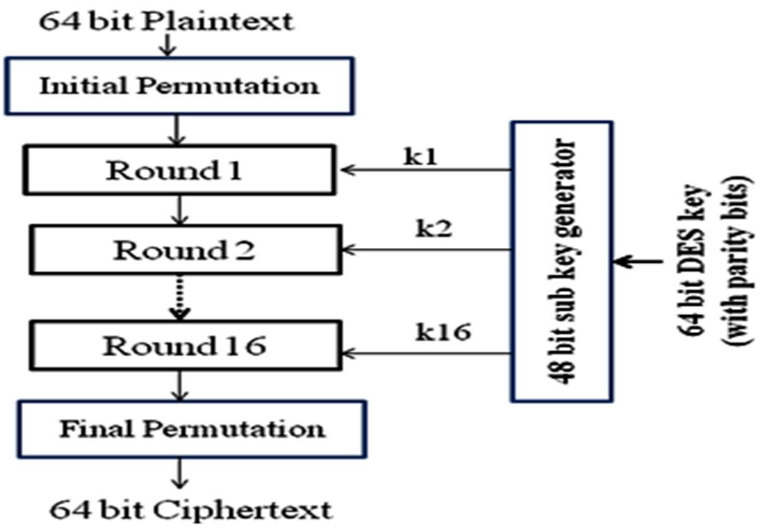
5) The authors of the research papers have proposed the accompanying data and comments demonstrate that Triple-Des delivers a higher-quality encryption procedure than des better encryption and decryption performance process. When we're in a hurry, this becomes a major flaw. Using a network to execute several processes The moment has arrived will be enhanced in the future for the Triple-DES process task would also include a higher level of assurance for all sorts of multimedia, quality and performance are essential data. The latter would entail encrypting data with a cross-platform of video and audio files, various algorithms.

III. ANALYSIS AND INTERPRETATION

A. Data Flow Diagram



B. Class Diagram



IV. SOURCE CODE

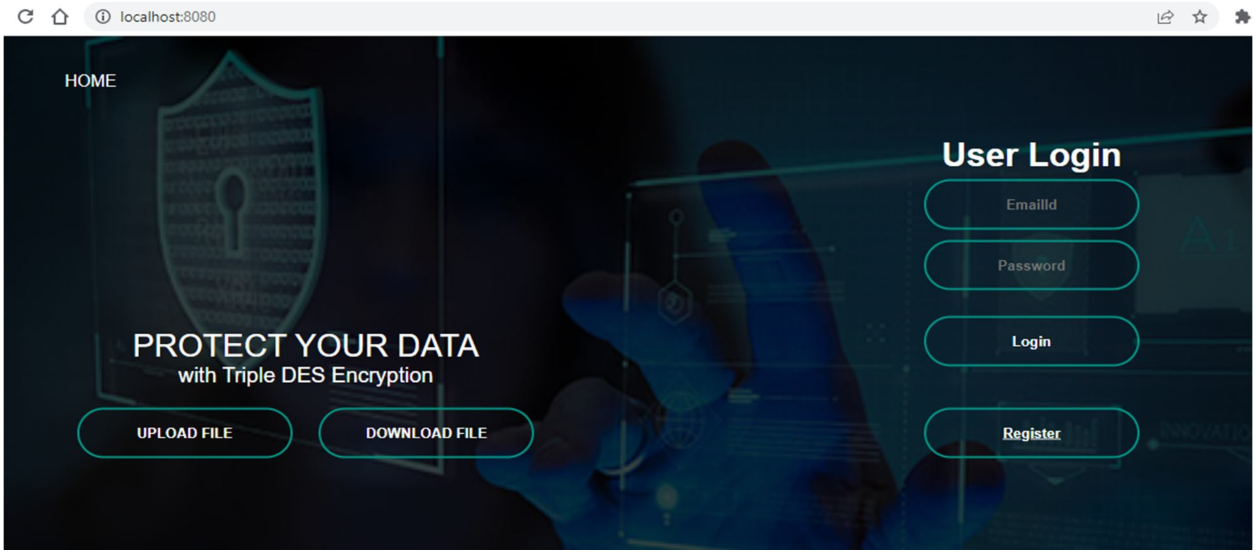
TripleDES.java.

```
package com.des.project.algo;
import javax.crypto.Cipher;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import java.nio.charset.StandardCharsets;
import java.util.Base64;
import java.util.Random;

public class TripleDES {

   private static byte[] secretKey = "9mng65v8jf4lxn93nabf981m".getBytes();
   private static byte[] iVector = "asdfghjk".getBytes();

   public static String encrypt(String secretMessage) {
      if (secretMessage == null) {
         return null;
      }
      try {
         SecretKeySpec secretKeySpec = new SecretKeySpec(secretKey, "TripleDES");
         IvParameterSpec ivSpec = new IvParameterSpec(iVector);
         Cipher encryptCipher = Cipher.getInstance("TripleDES/CBC/NoPadding");
         encryptCipher.init(Cipher.ENCRYPT_MODE, secretKeySpec, ivSpec);
         byte[] secretMessagesBytes = pad(secretMessage).getBytes(StandardCharsets.UTF_8);
         byte[] encryptedMessageBytes = encryptCipher.doFinal(secretMessagesBytes);
         String encryptedString = Base64.getEncoder().encodeToString(encryptedMessageBytes);
//          System.out.println("encrypted : " + encryptedString);
         return encryptedString;
      } catch (Exception e) {
         System.out.println(e.getMessage());
         e.printStackTrace();
```

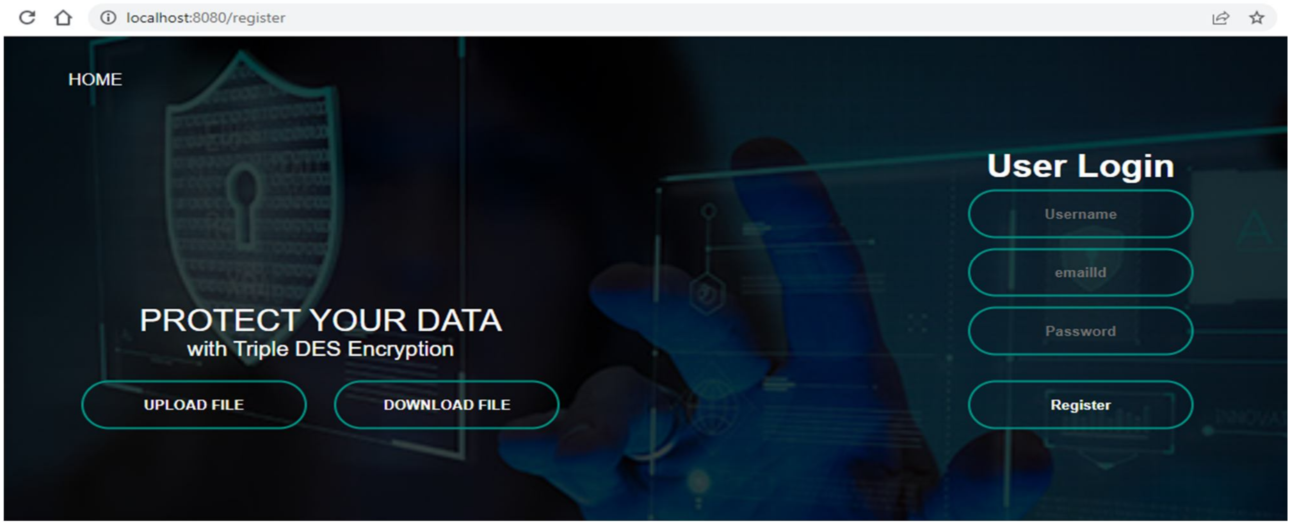
```
            return "";
        }

    }

    public static String decrypt(String encryptedString) {
        if (encryptedString == null) {
            return null;
        }
        try {
            SecretKeySpec secretKeySpec = new SecretKeySpec(secretKey, "TripleDES");
            IvParameterSpec ivSpec = new IvParameterSpec(iVector);
            Cipher decryptCipher = Cipher.getInstance("TripleDES/CBC/NoPadding");
            decryptCipher.init(Cipher.DECRYPT_MODE, secretKeySpec, ivSpec);

            byte[] bytes = Base64.getDecoder().decode(encryptedString);
            byte[] decryptedMessageBytes = decryptCipher.doFinal(bytes);
            String decryptedMessage = unPad(new String(decryptedMessageBytes, StandardCharsets.UTF_8));
//             System.out.println("decrypted : " +decryptedMessage);
            return decryptedMessage;
        }catch (Exception e) {
            System.out.println(e.getMessage());
            e.printStackTrace();
            return "";
        }

    }

    private static String pad(String str) {

        int length = str.length();
        if (length % 8 != 0) {
            int padLength = 8 - (length % 8);
            for (int i = 0; i < padLength; i++) {
                str += "~";
            }
        }
        return str;
    }
    private static String unPad(String str) {
        while(str.endsWith("~")) {
           str = str.substring(0, str.length()-1);
        }
        return str;
    }


    public  String generateString() {
        int leftLimit = 97; // letter 'a'
        int rightLimit = 122; // letter 'z'
        int targetStringLength = 10;
        Random random = new Random();

        String generatedString = random.ints(leftLimit, rightLimit + 1)
                .limit(targetStringLength)
                .collect(StringBuilder::new, StringBuilder::appendCodePoint, StringBuilder::append)
                .toString();

        return generatedString;
    }
}
```

V. RESULTS AND DISCUSSIONS

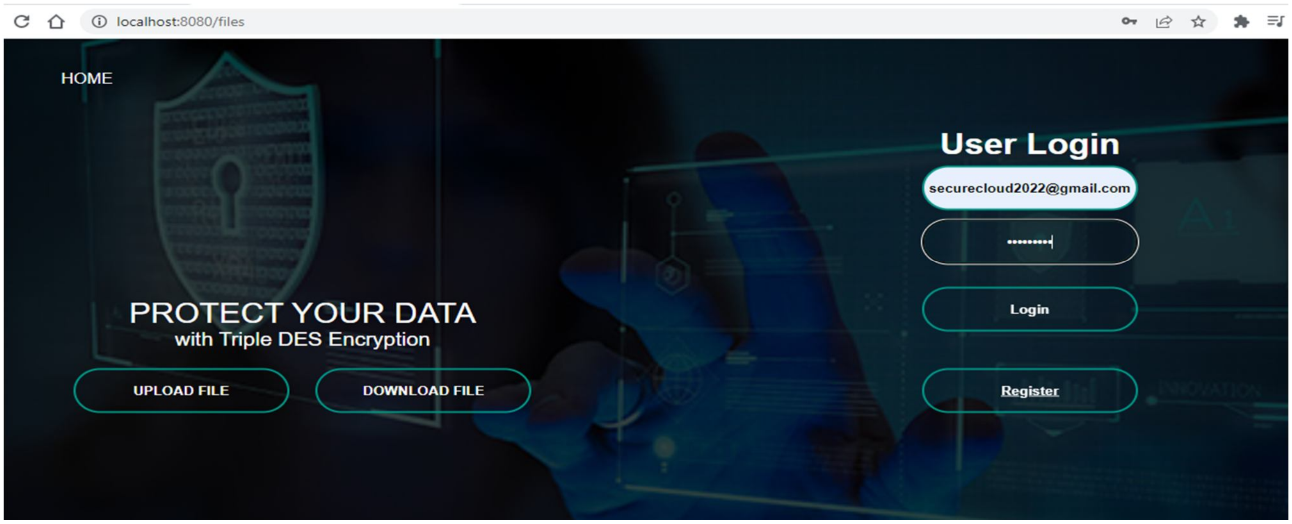
A. Homepage



B. Register



C. Login

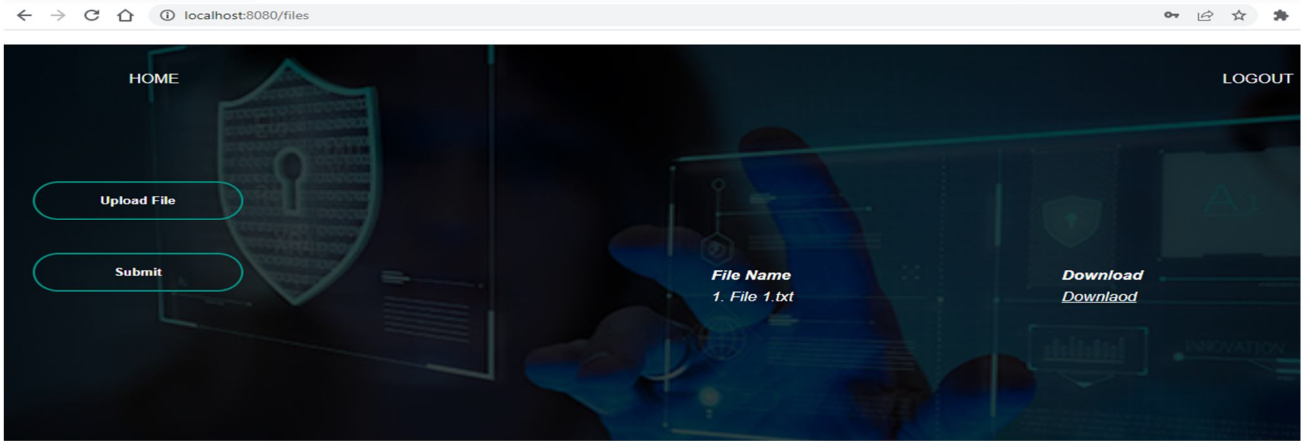


PROTECT YOUR DATA
with Triple DES Encryption

securecloud2022@gmail.com

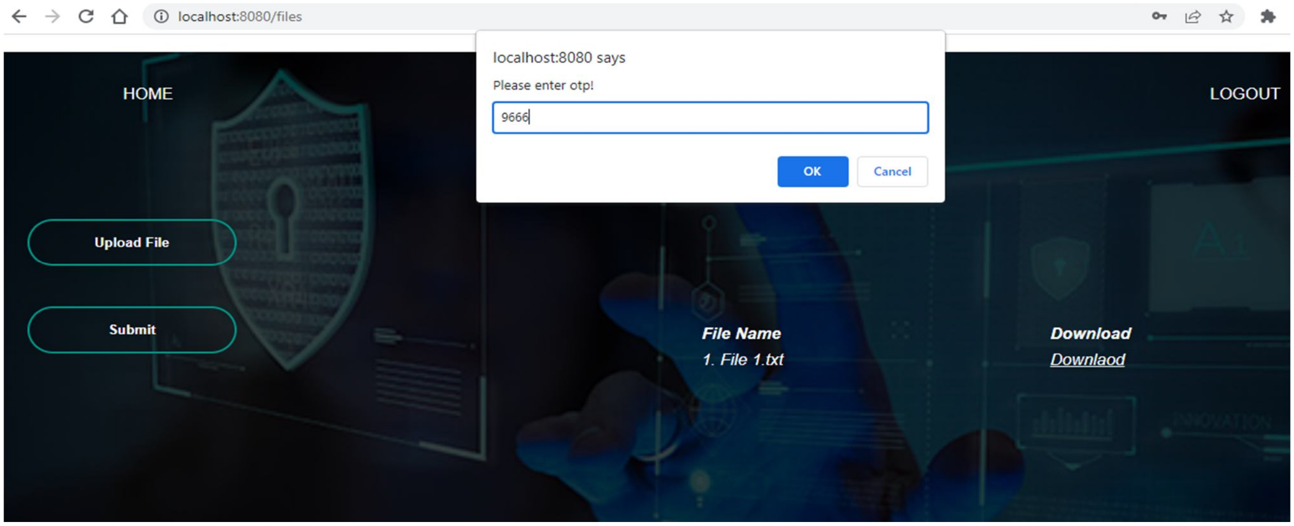
••••••••••

D. Files



File Name	*Download*
1. File 1.txt	*Downlaod*

E. OTP



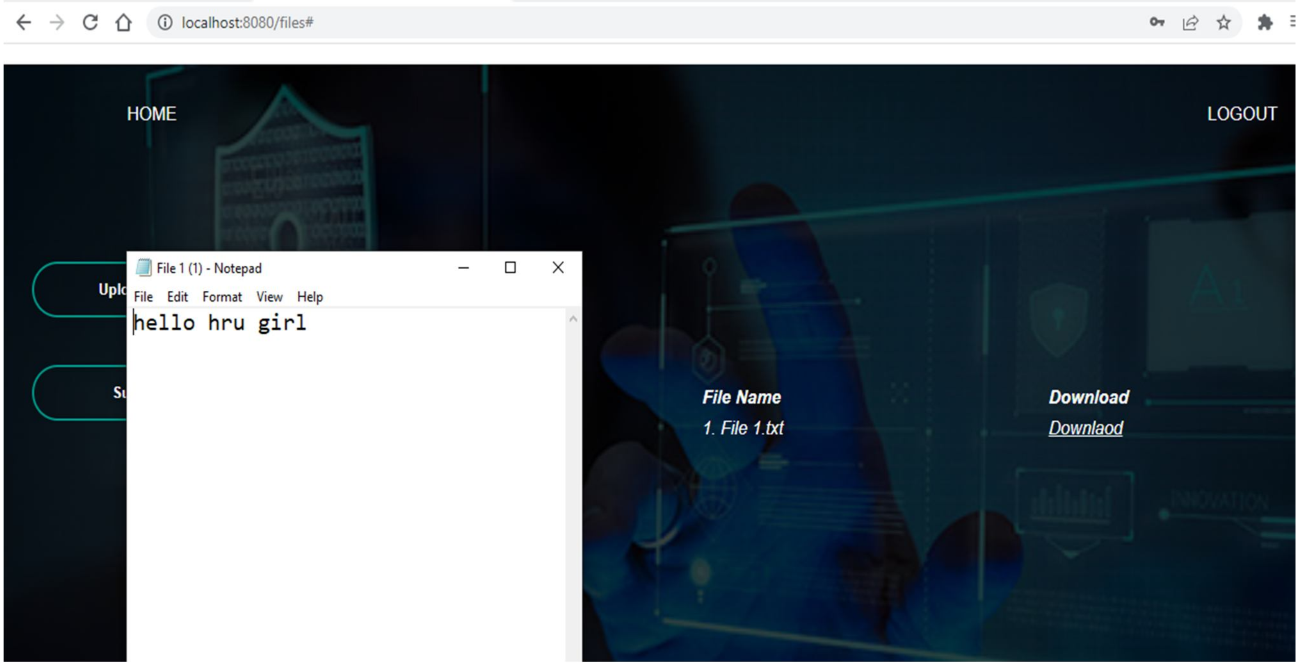
localhost:8080 says

Please enter otp!

9666

File Name	*Download*
1. File 1.txt	*Downlaod*

F. Download File



hello hru girl

File Name	Download
1. File 1.txt	Downlaod

VI. CONCLUSION

The paper is being written to provide a piece of project information on the triple Data Encryption standard for file encryption. The triple data encryption standard is an improved version of the data encryption method that performs all decryption and encryption processes three times instead of only once. It has been determined that a significant number of resources will be necessary to continue with the experimental analysis and settings for implementing the triple Data Encryption standard. However, due to its linear cryptanalysis, the implementation of the triple Data Encryption standard technique may encounter difficulties.

REFERENCES

[1] Journal for Research| Volume 02| Issue 02 | April 2016 ISSN: 2395-7549 All rights reserved by www.journalforresearch.org 8 Securing Digital Images using Watermarking Technique and Triple DES Algorithm M.R.M Veeramanickam Varsha Khenat, Puja Dhalpe Navin Dube.

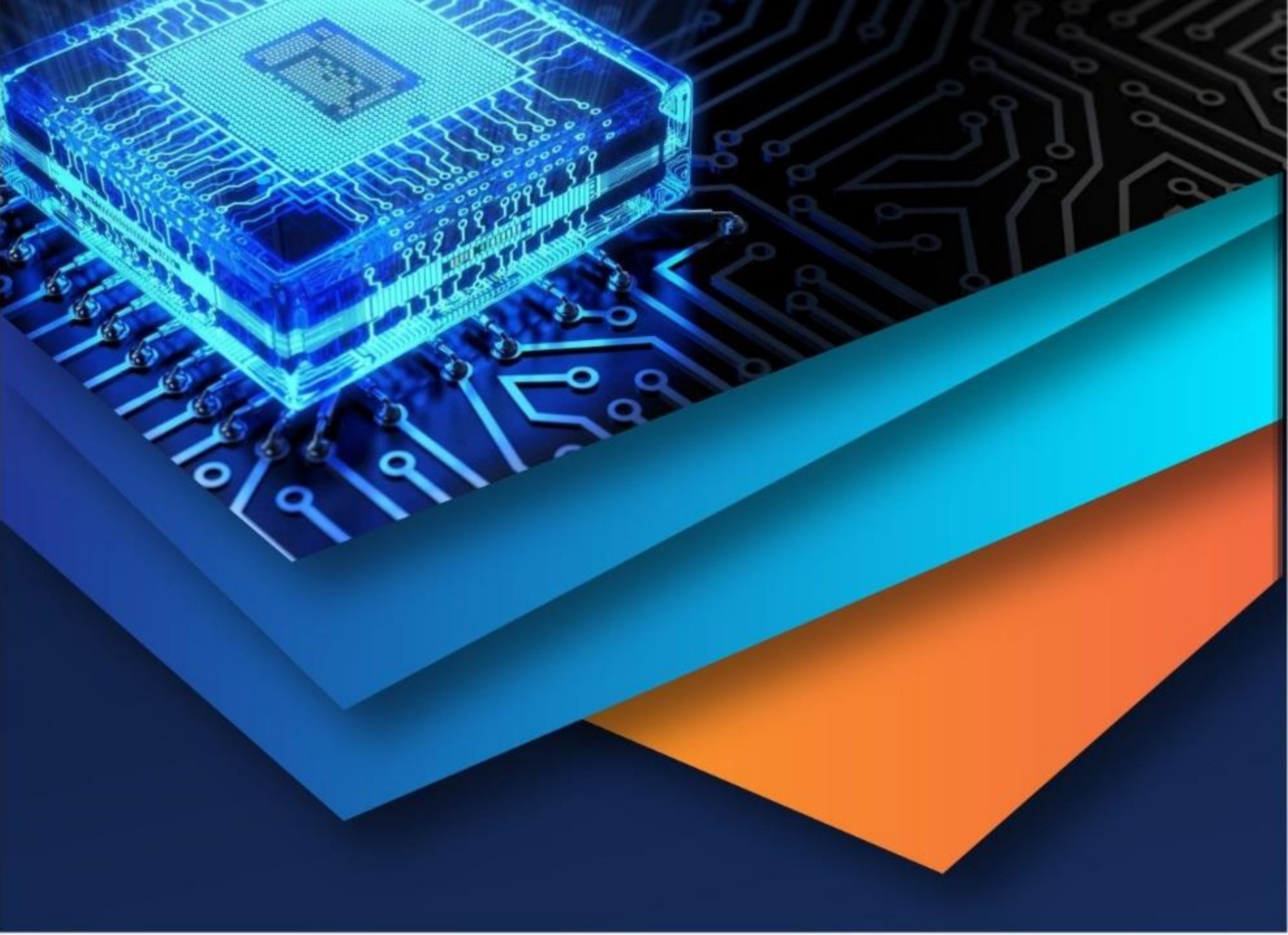
[2] International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014 Licensed Under Creative Commons Attribution CC BY Data Encryption and Decryption by Using Triple-DES and Performance Analysis of Crypto System Karthik. S, Muruganandam. A

[3] International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014 38 Image Encryption using Simplified Data Encryption Standard (S-DES) Sanjay Kumar, Sandeep Srivastava

[4] Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-5, 2017 ISSN: 2454-1362, http://www.onlinejournal.in Imperial Journal of Interdisciplinary Research (IJIR) Page 969 Image Encryption using Triple-DES Algorithm Anup R1 & Suchithra R2

[5] International Journal of Computer Applications (0975 – 8887) Volume 165 – No.8, May 2017 1 Secure Message Transfer using Triple-DES Somya Garg

[6] Computer Tarun Garg Bhawna Mallick.dcwlq



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY