United International University

Mid Progress Report

CSE 4531: Computer Security

A Secure Messaging Platform for Image, Audio, Text and Document Communication

Submitted to:

Prof. Dr. Mohammad Shahriar Rahman

Submitted by:

Shifa Chowdhury Iwase	**ID: 011183003**
Juairia	**ID: 011191002**
Md. Eram Bin Tanbir	**ID: 011191182**
Md. Anisur Rahman	**ID: 011191191**
Niful Islam	**ID: 011201057**

Section: A

Date of Submission:

7 December, 2022

Abstract:

Chat is the term that refers to the process of communicating, exchanging messages, and engaging with others over the computer network where the participant can share text messages, images, audio, and different kinds of documents. With the increasing amount of usage of different chatting software, privacy has become a burning issue among users. There is a need to ensure the security of the system. A secure chatting environment indicates that no unauthorized user has access to the information exchanges between or among the participants. In this project, we propose to design a chat application to ensure the privacy of the messages. For this purpose, we follow some cryptography algorithms like RSA(Rivest-Shamir-Adleman), Digital Signature, etc. The system provides a secure platform for sharing text, images, audio, and different documents securely. In addition, to implement the project we adapt the Django framework.

Introduction:

With the expansion and accessibility of internet connectivity, much of our interaction has been done through the screen of our PC monitors or even our smartphones. Each day, hundreds of millions of internet or smartphone users utilize messaging applications, where the facilities are free to use and install. WhatsApp, Viber, Telegram, and other programs have been shown to be more reliable than traditional phone calls. Although these platforms have tempting built-in features for users, they frequently neglect security concerns when utilizing them. As per a report issued by the Electronic Frontier Foundation (EFF), the majority of these chat applications do not guarantee enough security for their users [1].

In today’s modern internet world, governments and malicious hackers are constantly interested in hacking servers and disclosing sensitive information about users on messaging platforms. Although a huge number of chatting applications advertise to provide security, confidentiality, and integrity of the user's information, a hacking instance reveals that these statements are baseless These hacked data can be used to track users' every move, to discover our profiles, and to plan and perform customized attacks such as phishing, as well as kidnappings or deceits.

Cybersecurity in message applications is critical since it protects all forms of data from theft and loss. This includes sensitive data, personally identifiable information (PII), personal information, data, and government and business information systems. If cyber security experts did not work relentlessly to prevent denial-of-service attacks, messaging platforms would be almost impossible to use. Ensuring security in the chatting application can help with data privacy, preventing text and audio message leakage, image authority confirmation, and other services. It makes the overall system reliable and safe.

The purpose of this project is to create a secure chat application that uses cryptographic techniques to safeguard the security of its users. End-to-end encryption is ensured in our system by generating a shared key between users that will be used as a key for the encryption methods, ensuring the confidentiality of data being sent, such as text, image, audio, and document. Our proposed project also ensures that no data is altered while being transferred between entities, hence ensuring data integrity. The system's efficient functioning has also been considered for smoother and more effective communications.

Literature Review:

In 2019, Botha et. al. [2] have evaluated the best and purportedly most secure messaging platforms based on the apps' built-in security and privacy protections, as well as the location and future accessibility of stored data. It has been discovered that the most secure free apps include Signal, Telegram, WhatsApp, and Viber, according to a study of the security characteristics of several Apps. With a variety of extra capabilities to conceal and disguise the user's information, CoverMe offers elevated security and privacy. WeChat, Google Hangouts, and Slack are the least secure apps, mostly because they don't use end-to-end encryption. WeChat has serious privacy problems, and the best course of action is to uninstall the app from your phone. Also noted for severe security and privacy issues was Google Hangouts.
In the article [3], authors have implemented the ECC algorithm to secure text messages sent over a smartphone's messaging app, that comes with end to end encryption. This study have established the ECC algorithm's applicability and demonstrates its competitive performance in terms of speed and accuracy. To achieve better outcomes, the ECC application in the Android app still needs to be adjusted and it has been found that in the future, ECC method optimization can be used in both the encryption of photos and videos as well as other applications.
The authors of the study [4] have proposed a method that enables the maintenance of personal information privacy while granting access to useful data, and the system archyevufe is built to use blockchain as a software component for transmitting messages safely and anonymously

Tools And Validation:

Tools and Software:

- Python

- NumPy

- TensorFlow
- Rivest-Shamir-Adleman encryption (RSA) algorithm for encryption and decryption.
- Django Framework

Justification Behind those Tools and Software:

Python: Python is widely used for developing websites and software, task automation, data analysis, and data visualization. We have used python because it has some built-in function which will give us some extra advantages so that we can implement the feature properly and most of the deep learning libraries are easily available in python.

TensorFlow: TensorFlow helps us to implement best practices for data automation, model tracking, performance monitoring, and model retraining. Besides, the community of TensorFlow is very wide compared to pytorch.

Rivest-Shamir-Adleman encryption (RSA) Algorithm: RSA algorithm is an asymmetric cryptography algorithm. It works on two different keys. (I) Public Keys (II) Private Keys. Here the Public key is given to everyone and the private key is kept secret. As the private key is only to the receiver so the data is kept secret here.

Django Framework: If we talk from a security perspective, Django offers us a highly secured approach to develop web applications as it prevents attacks like XSS (Cross-Site Scripting), CSRF (Cross-Site Request Foregery), SQL Injection etc.

Plan and Design:

According to the gantt chart we have made the platform completely. We individually is doing different different part like sending text, images, audio, document. Image encryption is fully done. Text, audio and document is in progress. Text, document and audio is tested on our each local machine. Integration with the main chatting flatform is yet to be done. The project was distributed in the following manner:

Name	**Task**
Md.Eram Bin Tanbir	Text encryption Text decryption Calculating hash value for plain text Verifying hash with decrypted text
Niful Islam	Autoencoder construction

	Creating hidden watermarking system
Juairia	Messaging platform creation Handling frequent cyber attacks
Md. Anisur Rahman	Audio encryption Audio decryption Literature Review Write Abstract and Conclusion
Shifa Chowdhury Iwase	Document encryption Document decryption Literature Review Write Introduction Literature Review

Progress:

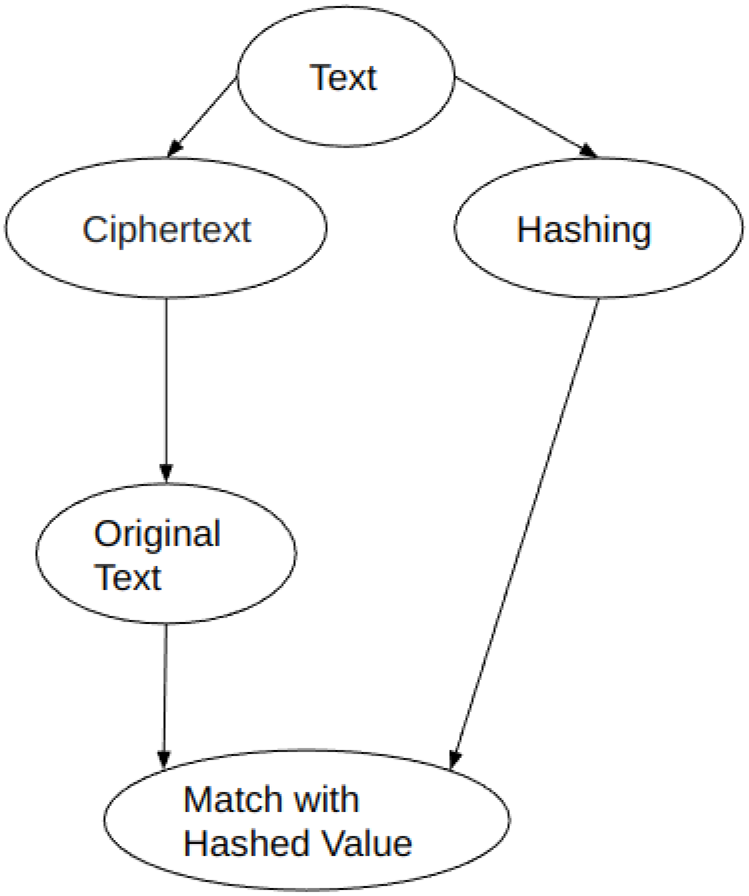
- Built an autoencoder that takes a image as input and converts into a 32*32 size image of 32 channels and outputs the original image with some recompilation loss.
- Built an watermarking system that takes two images (original and watermark) as input and outputs an image with a hidden watermark. The output image can also regenerate watermarks.
- A partially built user interface was constructed using Django.
- Text encryption decryption system was constructed using the RSA algorithm.

Description:

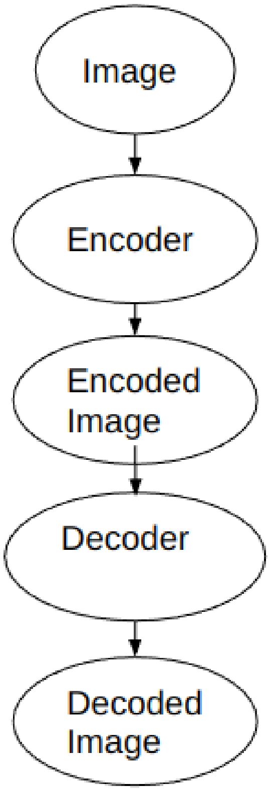
The messaging system will have five major features along with regular prevention from cyber attacks.

- **Message Encryption Decryption:**

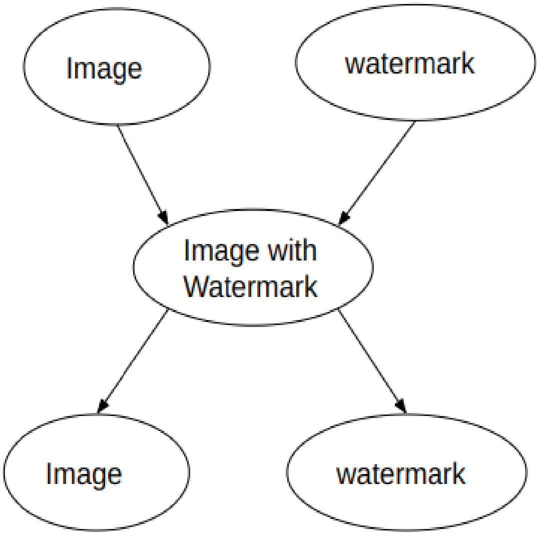
The message in plain text will be encrypted first before sending it through any channel. Moreover, there will be a hash value to make sure the message is not modified along the way.



- **Image Encryption Decryption:**
  For image security, the system will have a deep learning approach to build an autoencoder that will encode the image into a form that is not understood by humans. The encoded image will pass through the channel and will be decoded again on the receiver side.

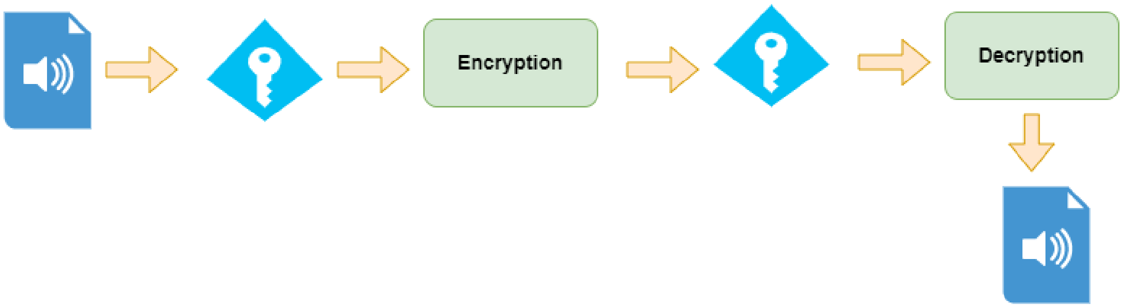


- **Image Watermarking:**
  This system contains a hidden watermark approach to ensure authenticity.

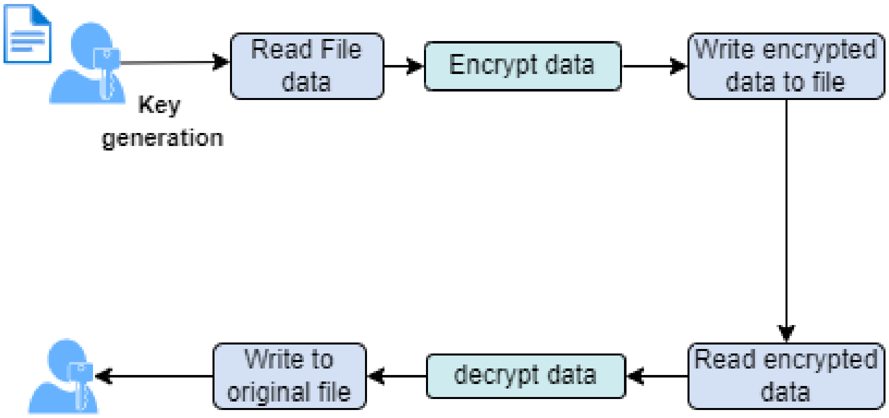


Audio Encryption Decryption:
Similar to the image encryption decryption, there will be an audio encryption decryption method. For this we utilize the cryptography library from python. In the cryptography library their is a

method fernet which generates a secret key and uding this key we encrypt the audio file and using the same key we decrypt the audio file. The process is given below diagram.

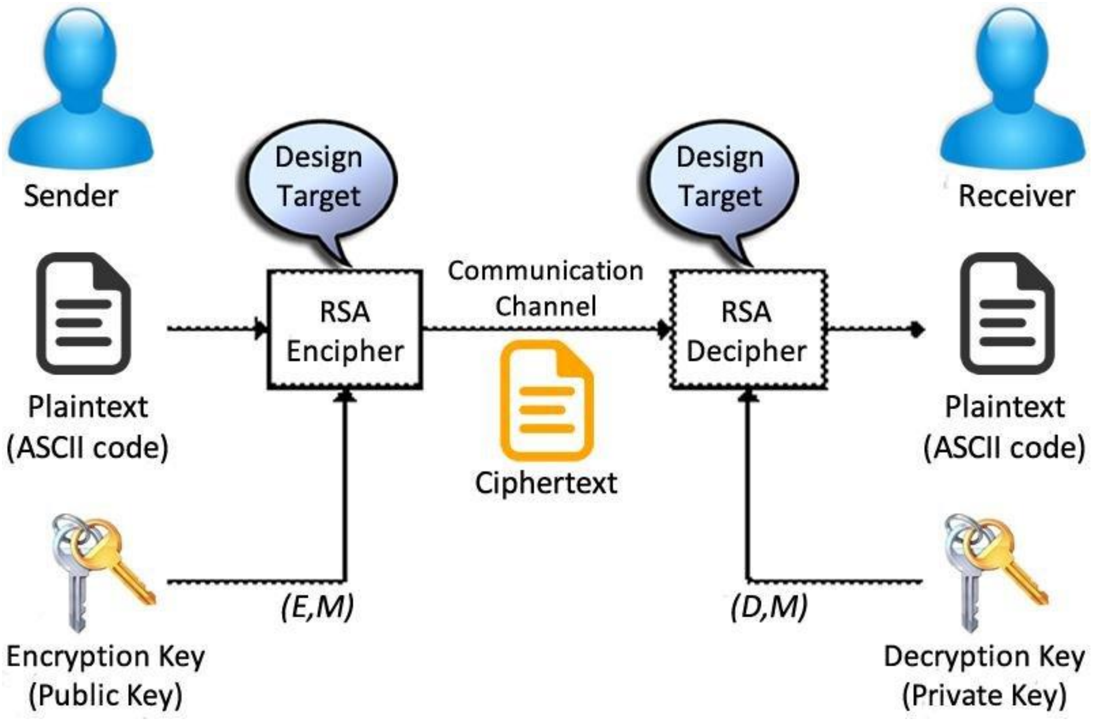


- **Document Encryption Decryption:**
  This approach will also be the same as image and audio.



Text Encryption and Decryption:

We will use the Rivest-Shamir-Adleman(RSA) algorithm for encryption and decryption the text.RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys. (I) Public Keys (II) Private Keys. As the name describes, the public key is given to everyone and the private key is kept private. Here the public key is used for encryption and private key is used for decryption.



Conclusion:

In the proposed system we ensure the security of the exchange data between the users by adapting some modern cryptographic methods. The platform is able to exchange text, images, audio, and documents between two users securely. Considering the limitations of our current system as a future plan we want to have the feature of sending video, a real-time audio recording system, and downloading documents, images, and audio files.

References:

[1] Kuliya, Muhammed, and Hassan Abubakar. "Secured Chatting System Using Cryptography." *International Journal of Creat. Res. Thoughts* 8.9 (2020): 23-26.

[2] *"A comparison of Chat Applications in terms of security and privacy" by Johnny Botha et al*

[3] *“Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (ECC)”*

[4]”*Secure Messaging Platform Based on Blockchain” by Ellewala et al.*