MULTI-USER

CHAT APPLICATION

October 12, 2022

****

**INSTRUCTOR: MR. SHOAIB RAZA**

**M. AHSAN RAZA (20K-0137)**

**M. ANAS KHAN (20K-0324)**

**INTRODUCTION:**

In the modern day, there are variety of chat systems but the popularity of Multi-User chat applications is on the rise. Hence, we developed a simple multi-user chat application. It’s an end-to-end messaging system inspired from WhatsApp. Although we included the graphical user interface but it’s not on par with the likes of WhatsApp’s or any other messaging app user interface.

The message transfer is done with the help of socket programming while the security of application is ensured via encryption and key exchange. Encryption is done using Triple DES while Diffie-Hellman is used for key exchange.

**FEATURES IMPLEMENTED:**

* User creation and login
* Group creation and joining facility
* Private messages
* Group messages
* File sharing privately or in groups

**TECHNOLOGY USED:**

* Tkinter library was used for user interface
* Python used for socket programming with required libraries

**PROGRAMMING APPROACH:**

In order to simplify and keep code maintainable we utilized classes for server and clients. Furthermore, security related activities were also allotted respective classes.

A class diagram is shown below to illustrate variables and functions defined for an entity.

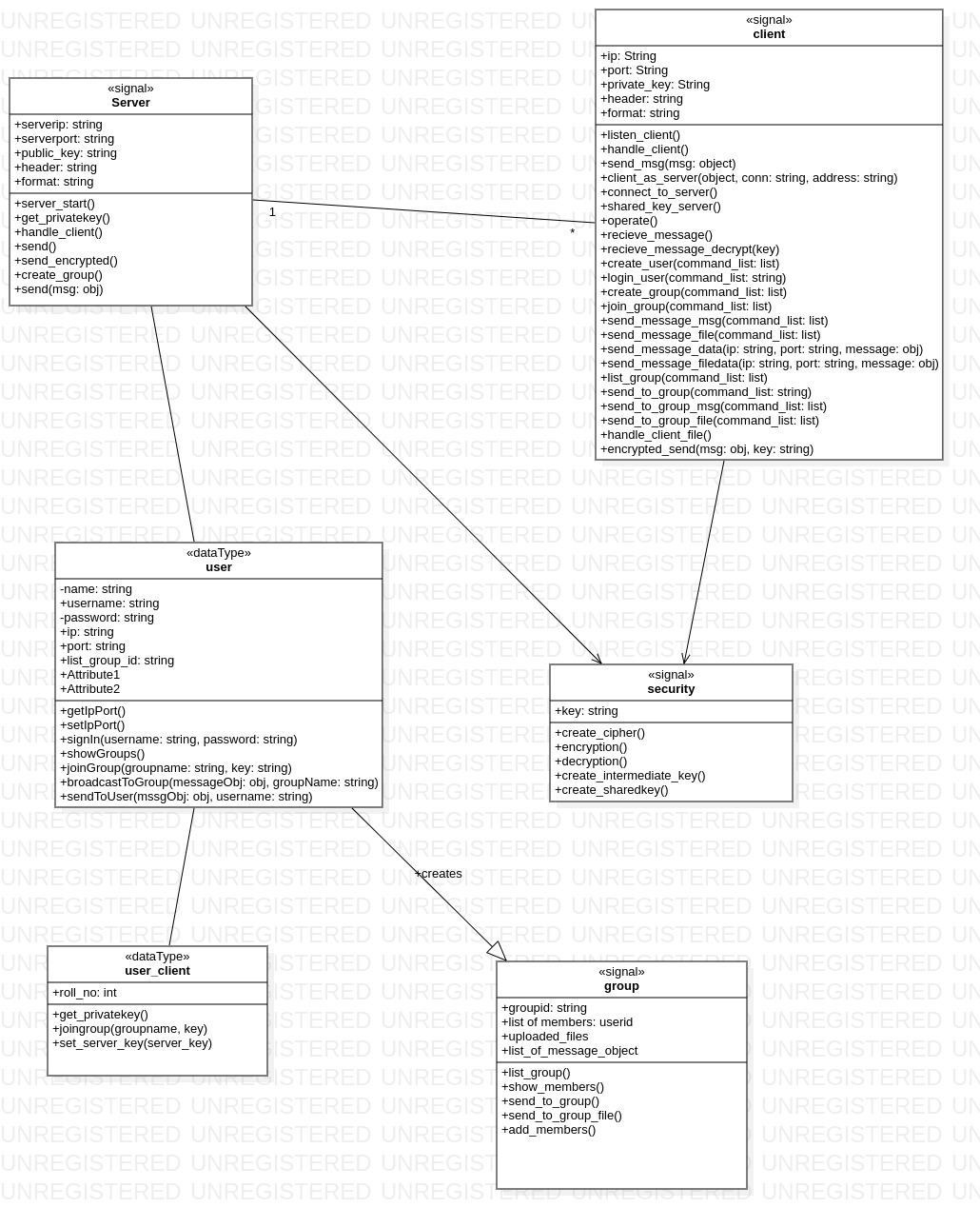


Figure : CLASS DIAGRAM

**PROJECT DESCRIPTION:**

The application supports user creation which is also the first step up that is to be performed upon executing the client.py. Once user is created, he then logins in using credentials decided in sign up process i.e., user creation. User can easily send a group message or individual message to other users with ease. Like, Whatsapp when a user creates a group, he directly joins it. Other users can then join it by giving the correct group name. Files such as documents and images can easily be sent and received.

So, when client makes connection with server, a private key is exchanged between them ensuring security. Message that are sent between clients are encrypted using Triple DES. To perform actions, we use certain commands listed below with their parameters:

* CREATE\_USER <name> <username> <password>
* LOGIN <username> <password>
* CREATE\_GROUP < group name>
* JOIN <group name>
* LIST
* SEND <username> <message>
* SEND\_TO\_GROUP <group name(s)> <message>
* SEND FILE <username> <filename>
* SEND\_TO\_GROUP FILE <group name(s)> <filename>

**SCREEN SHOTS:**

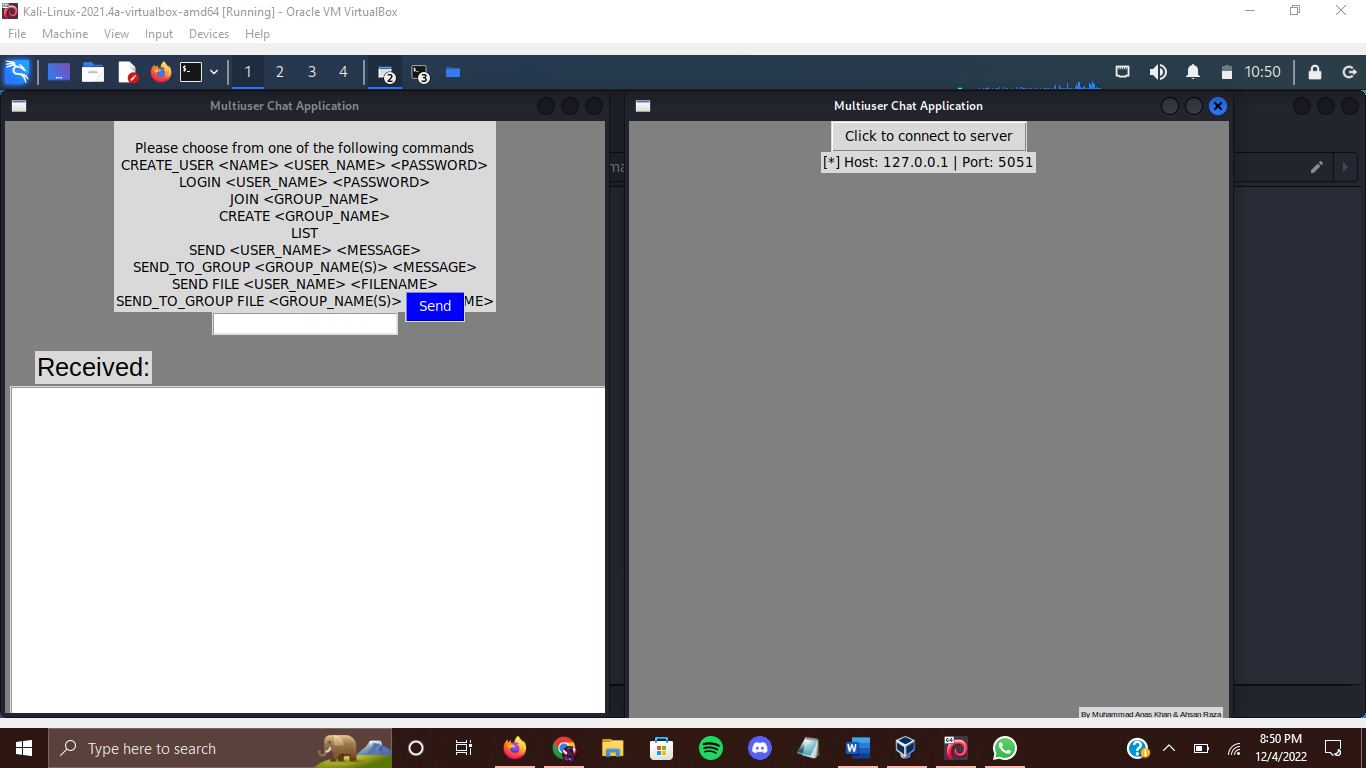


Figure :USER INTERFACE

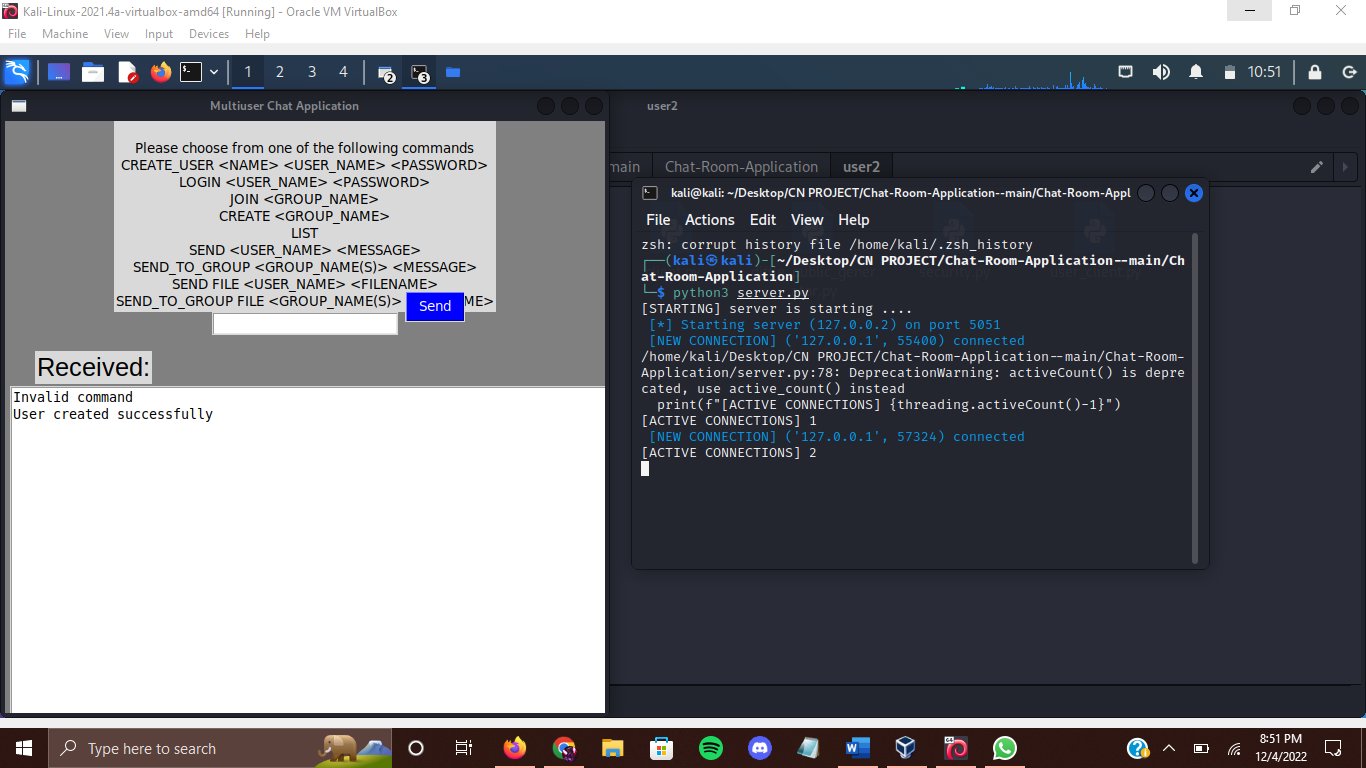


Figure ESTABLISHING CONNECTION

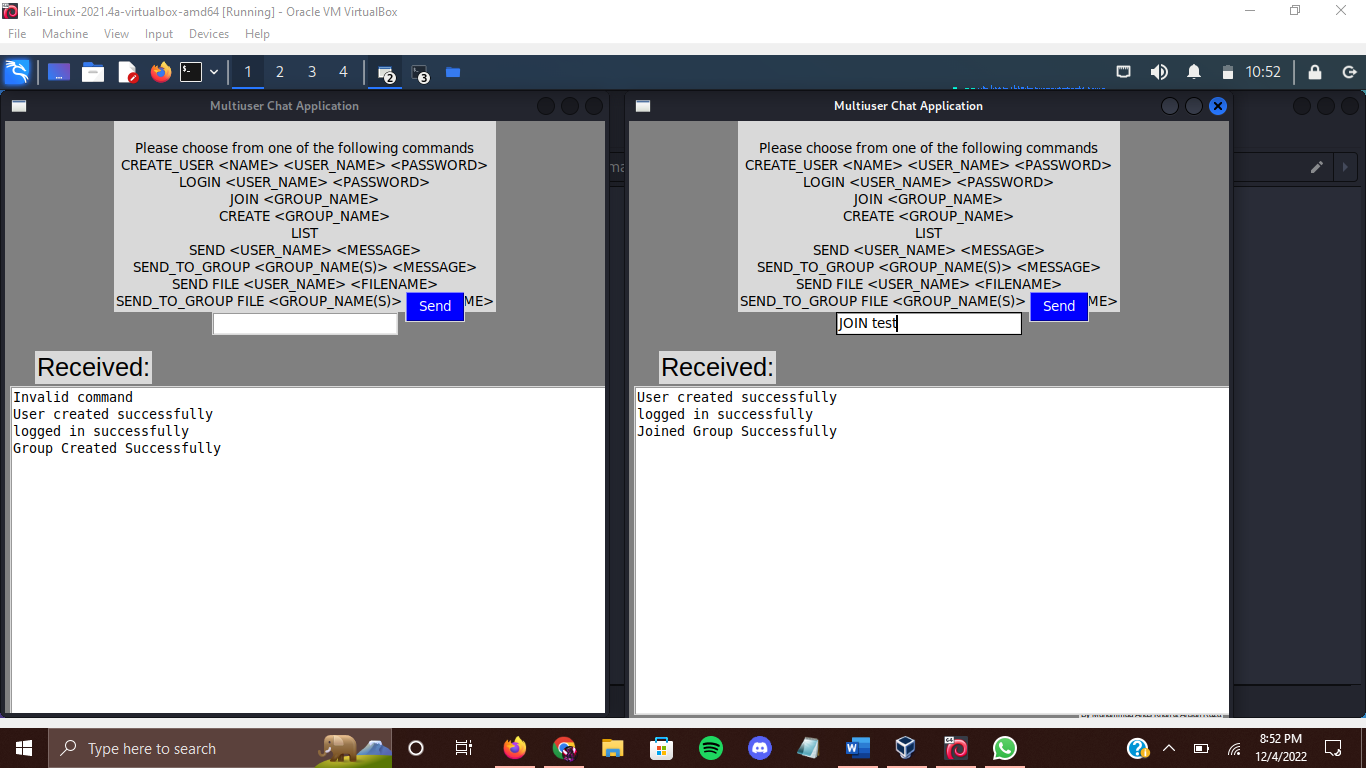


Figure BASIC COMMANDS

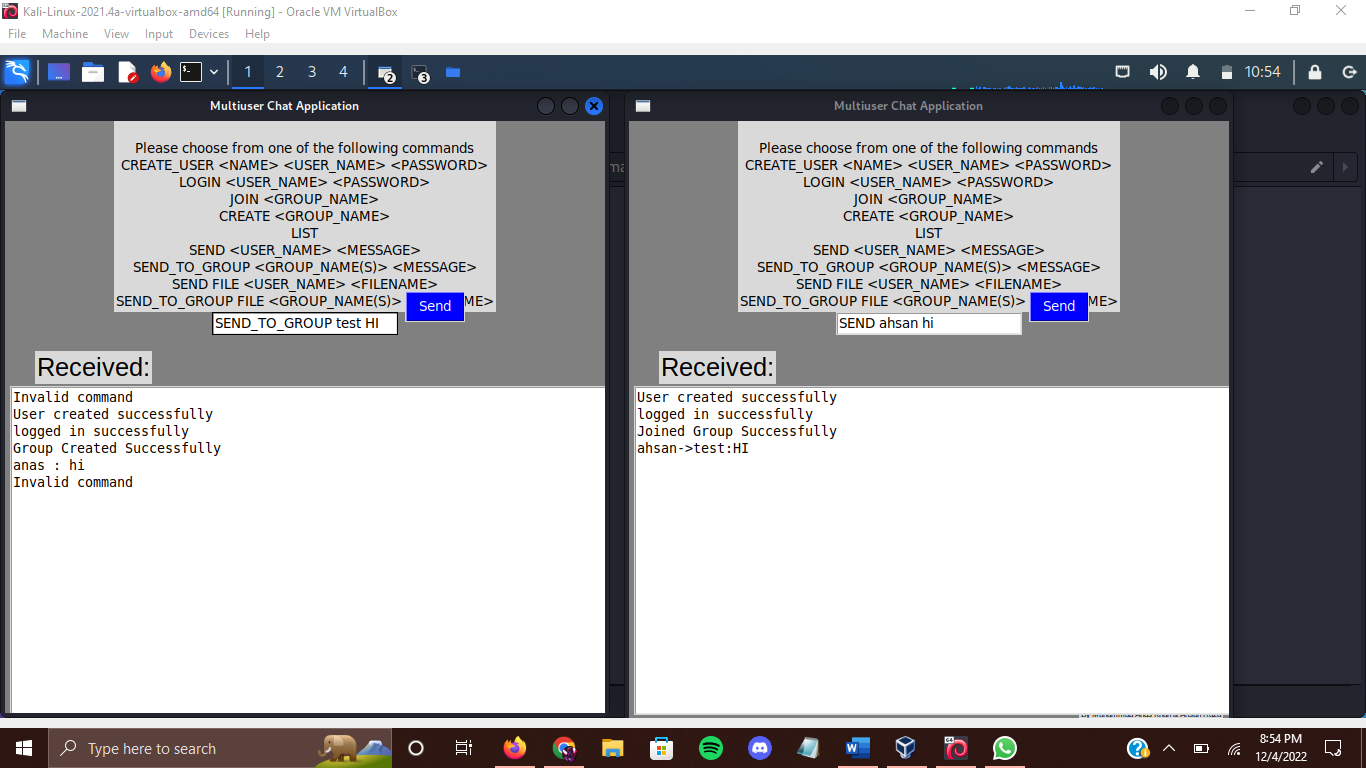


Figure : EXCHANGE MESSAGES

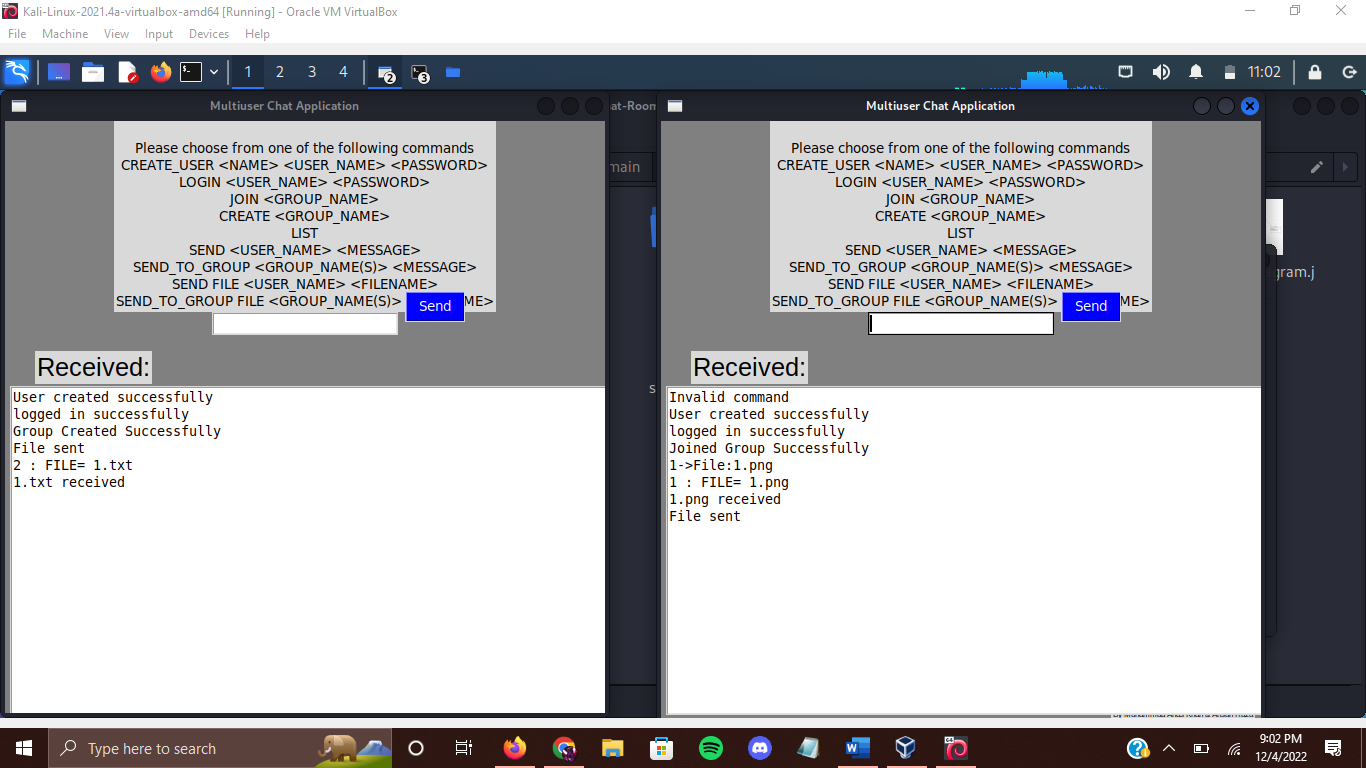


Figure FILE EXCHANGING

**FUTURE WORKS:**

* LOAD BALANCING
* BETTER USER INTERFACE
* AUDIO SUPPORT

**REFERENCES:**

The idea behind implementing security using Diffie-Hellman with Triple Des was taken from a security blog (<https://www.comparitech.com/blog/information-security/3des-encryption/>). Tkinter library documentation was used extensively for help in creating user interface.

Various articles and YouTube videos (like <https://www.youtube.com/watch?v=CqWorn8dR_A>) were consulted to shape up multi-user chat application.