Green University of Bangladesh Department of Computer Science and Engineering (CSE) Faculty of Sciences and Engineering Semester: (Fall, Year:2022), B.Sc. in CSE (Day)

Submission Date
:07/01/23
Course Teacher's Name
: Mahmuda Rahman

1 Lab Project Name: Group Chat App With Encrypted Messaging and Video Streaming.

2 Student Details

	Name	ID
1.	Estiak Hasan Emon	201002059
2.	Shamima Aktar Reya	201002265

[For Teachers use only:Don't Write Anything inside this box]

Lab Project Status

Marks:
Signature:
Comments:
Date:

3 INTRODUCTION:

Every day millions of people are exchanging messages via messaging or rather chat Applications (Apps). However, users do not know what happens to the messages once they have been sent. Initially, encryption was considered to be used only by paranoid users or people with a heightened need for secrecy. After the revelations of become more aware of online privacy and the dangers of digital scoping of data and identity theft. Surveillance activities are increasing globally and concerns amongst people all over the world has been raised considerably whilst data retention laws are being implemented. We live in a digital age where surveillance and data logging occur on almost all our communication. Companies want to collect as much as possible personal information about consumers. Some governments are hacking mobile devices to gain unauthorized access for surveillance and other unknown reasons. Although messaging Apps have been around for a number of years, the development of secure mobile Apps are increasing, focusing on securing the privacy of users and meeting their demands. Recent studies show that users are becoming concerned about protecting privacy on their Smartphone's and opposed apps that collected their contacts.

4 DESIGN GOALS/OBJECTIVES:

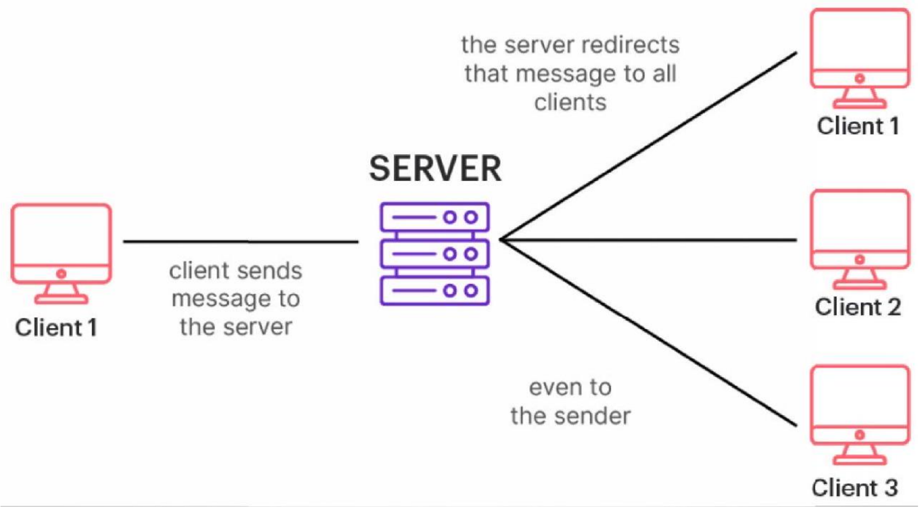
1. To Privacy has become a major concern for the end user of free services.
2. To designed an end-to-end encrypted chatting application to address this issue.
3. To chatting application named "Fun" can stay anonymous throughout the chatting session.
4. To secure and portable and compatible on most of the popular operating systems.
5. To privacy concern of the users will help primarily the small to medium scale business. 6. To operate the every centralized and authorized people.

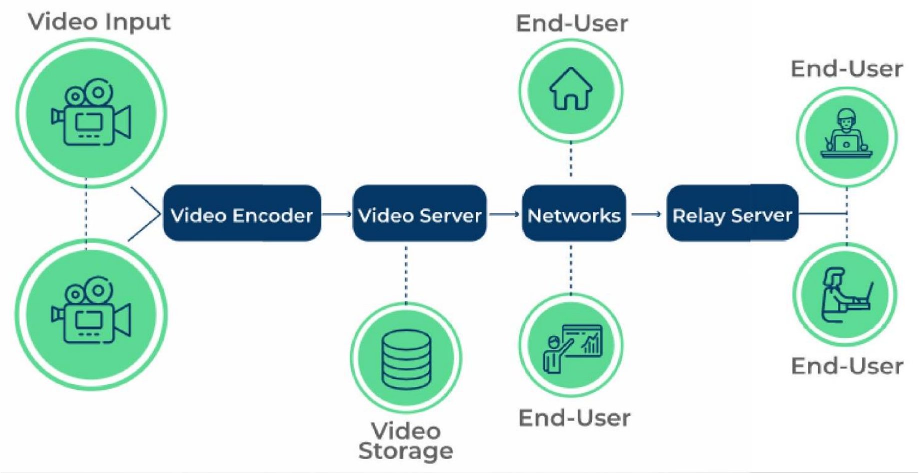
5 Design:

I have used java to environment for writing the software apart from that I have also used visual studio code GUI java library for making the GUI model of the client side of the software, and public keys are generated using java library of. I have also written four user defined libraries for making the GUI models for login/register window and GUI models for the chat room. The server side of the code uses Time, socket and database libraries for receiving and sending the data, the user's login credentials are stored in database on the server. Using this application has some advantages and disadvantages which will be discussed later in the report.

6 Development/Implementation of the Project:

Firstly, we create a java project which name is group chat app with encrypted messaging and video streaming. Then we create five java class which is client, decryption, encryption, rounded panel & server. Then the client class we import the javax crypto, sound & swing. Then client extends the static string. Private static final we add socket, Jlabel, Jbutton, Jpanel, Jfilechooser. We also add name, ip address, port, password & video streaming. Fun is written using java which uses javax library version 4.2, and sockets library. The client side of the first asks the user the IP address of the server, when the user inputs the IP address, the client software sends a TCP/UDP 'connect' sign packet to the server on port '2000', the server side of the application respond with an acknowledgement. Upon receiving the acknowledgement, the GUI model opens on a new maven window. The Log in or register window, either signs up the user credential and sends to the server or sends the log in credentials to the server database, if the user is found to present in the server database then the server will send another acknowledgment sign and the log in window will be closed and the main chat room GUI will start, while logging in a set of 1024-bit public key and private key is generated. The public key was sent to the server and the server send this key to all the other clients present. The user then types a message on the text box and clicks on the send button which is encrypted using the public key of the user who started the session and the message appears on the chat thread as well with time stamps. The text then travels to the server via TCP/UDP protocols. Receiving the sends the other client connected to them via same TCP/UDP protocols. The other client receiving then them decrypts the text using the private key and shows it on the chat thread with name and time stamps. The time stamps on the other hand is taken from the system time using java 'time' library. The detailed process is visualized.


the server redirects that message to all clients
SERVER
Client 1
client sends message to the server
Client 1
Client 2
even to the sender
Client 3



7 An Overview of the Best and Most Secure Messaging Apps:

This section gives an overview of the Apps that are regarded to be the best and the most secure; Facebook, WhatsApp, Telegram, Signal, WeChat, Line, Skype and Viber. Two of the main reasons why chat Applications have become so popular at a rapid pace, are firstly, the rapid growth in access to cell-phones and to the Internet. Secondly the death of SMS messages because chat Applications allow for "richer" methods of remote communication.Facebook's chat Application is called Messenger. This App is used by over two billion users registered on Facebook. The App can be accessed via Facebook and allows for normal chat messages, voice and video calls. End-to-end encryption is not enabled by default and has to be enabled with each and every chat by selecting the Secret Conversation option when messaging a contact. WhatsApp has a simple installation and setup by synchronizing contacts on your phone automatically. It allows for text and multimedia messages with end-to-end encryption by default. It also periodically asks for a password to access the App. WhatsApp is owned by Facebook and there are rumors that Facebook intends to populate members' Facebook profiles with their WhatsApp data. This idea has been blocked by the European Union, but it seems it is only a matter of time before this feature might be built in, posing more security and privacy risks to users. WhatsApp is the most popular messaging App.

8 COMPARING SECURITY AND PRIVACY FEATURES:

Since consumers demand better security and privacy in messaging Apps, software development companies have been attempting to address these issues. One of the features was to launch end-to end-encryption. End-to-end encryption refers to when messages are encrypted during transmission and no copy is stored unencrypted on the servers of the service providers. Nobody apart from the people communicating can view these messages party; no third party, not even the government or the developers of these Apps. Communication is transmitted using a secret code rather than plain text.

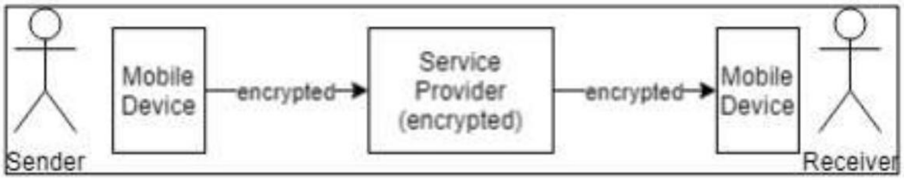


Figure 1. End-to-end Encryption

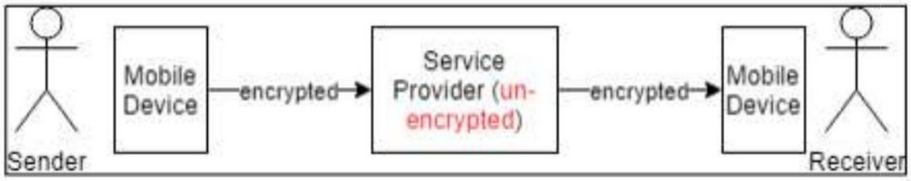


Figure 2. Encryption in Transit

9 PERFORMANCE EVALUATION:

The main purpose of this is to design a secure chat application which protects user's confidentiality and privacy. A research was conducted to investigate current security features of several messaging applications on Smartphone's application stores. The selected instant message applications has been investigated and a list of requirements for the design of a secure chat application was created. Based on different features and requirements, a design has been proposed and a demo is also implemented.

10 GOALS:

In this project different mobile chat applications have been investigated. Based on the threat model of mobile chat applications, different requirements for a secure chat application have been enlisted and a design was also proposed. The goal of this project is to propose solutions for different security challenges of the current chat applications in the market and to design and implement a secure chat application. The main contributions of this research can be structured into the following four sub-goals:

1. Literature study and related security vulnerabilities in current mobile chat apps.
2. To propose a secure mobile chat application architecture.
3. A detailed design of secure mobile chat application.
4. To implement and evaluate a demo as proof of concept (POC).

11 RESEARCH METHODOLOGY:

This thesis is based on design science research methodology which makes it convenient to develop an artifact. In such a methodology [5] a problem is defined and the goals of the research is defined. A research is conducted to investigate current popular mobile chat applications, their features and threats that they might enforce to their users based on security flaws or bugs. As the next step, the requirements for secure chat application are defined and architecture of a secure chat application is proposed. The final result of the research is a secure mobile chat application architecture. Based on the proposed design, a proof of concept is implemented and analyzed.

12 LIMITATIONS:

In this thesis, the proposal and the design of the secure instant messaging application is based on the client/server model. However with the rise of mesh networks and built in features in Smartphone's' operating systems such as iOS* which has the built-in ability of "multi peer connectivity", very few peer-to-peer chat applications are available in the market. Peer-to-peer (P2P) chat clients are omitted from this thesis since their architecture and infrastructure is different. Another thesis can be derived to focus only on such peer-to-peer mobile chat applications and investigation of their security vulnerability and design flaws.

13 ECOSYSTEM:

The ecosystem of application stores provides a chance for everybody including freelance developers as well as companies to publish their applications to the world via these stores. After the application gets approved by the store, it can be discoverable from anybody who has access to the Internet to surf and search through the app store. Every industry can benefit from such ecosystem. Many industries including insurance, banking, healthcare and even government agencies are getting benefits of Smartphone's' penetration and Internet access to better serve their customers and stakeholders.

14 SECURITY SERVICES FOR MESSAGING:

In order to evaluate any chat application from the security point of view, relevant threats to such application should be identified and described. In the following sections a brief description about different security aspects are explained.

"http://www.cricsson.com/

'https://www.android,com/

' https://play.google.com/store

'https://itunes.apple.com/us/genre/ios/id36?mt=8

Security has three key aspects: confidentiality, integrity and availability [8]. Confidentiality ensures that certain type of information can be accesses by authorized parties. Integrity means information can be modified only by intended and authorized parties. Availability means that information is accessible to authorized parties at appropriate times.

15 CONFIDENTIALITY:

Confidentiality means messages which are exchanged by two parties through a communication channel should be readable only to the intended parties. In order to achieve such a goal, encryption is the mechanism that provides confidentiality between two parties. A message is encrypted by a cryptographic technique and this encrypted message can only be readable by the intended party.

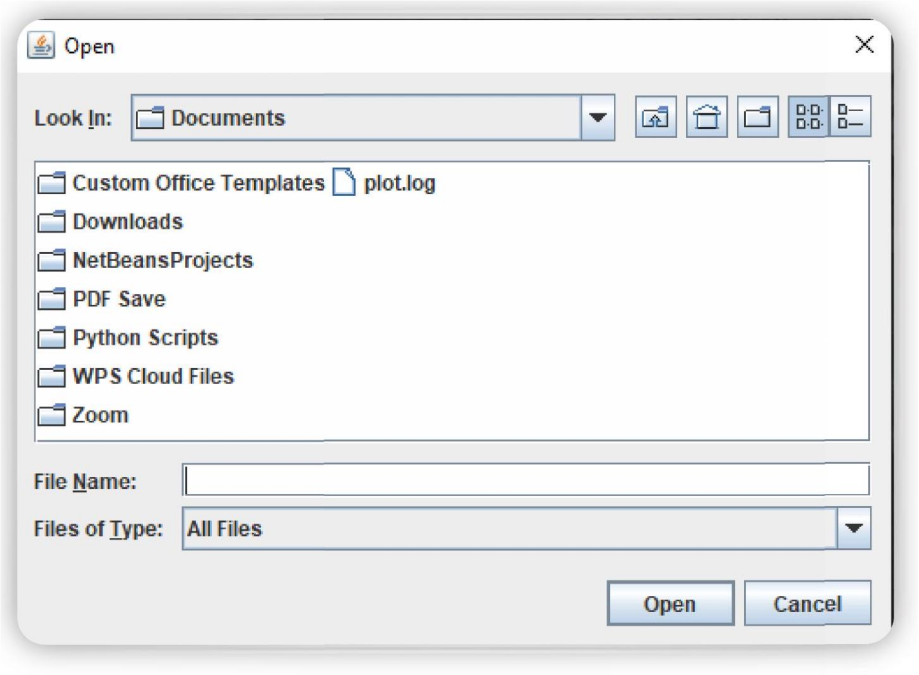
16 CRYPTOGRAPHY:

Cryptography is the practice and study of techniques which are used to secure a communication between two entities while the third party (adversary) exist. Cryptography helps to create an environment or medium channel in which confidentiality, integrity, authentication of the user and non-repudiation are supported.

17 AUTHENTICATION:

Authentication is one of the most important aspects of security, where an entity should identify itself before or during the communication. This avoids any type of attack or malicious activity by which a malicious user impersonates the user and identifies himself as the real user to the server. There are two types of authentication schemes known as weak authentication and strong authentication. Weak authentication (one factor authentication) means that the entity uses only one type of identity credential such as a PIN* or password-based authentication.

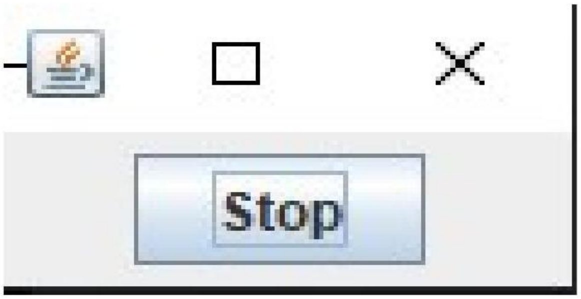
It is considered a weak mechanism because it is prone to many attacks including brute force attacks. A brute force attack is type of attack that the malicious user tries as much as passwords to finally finds out the one which matches the chosen password of the user.

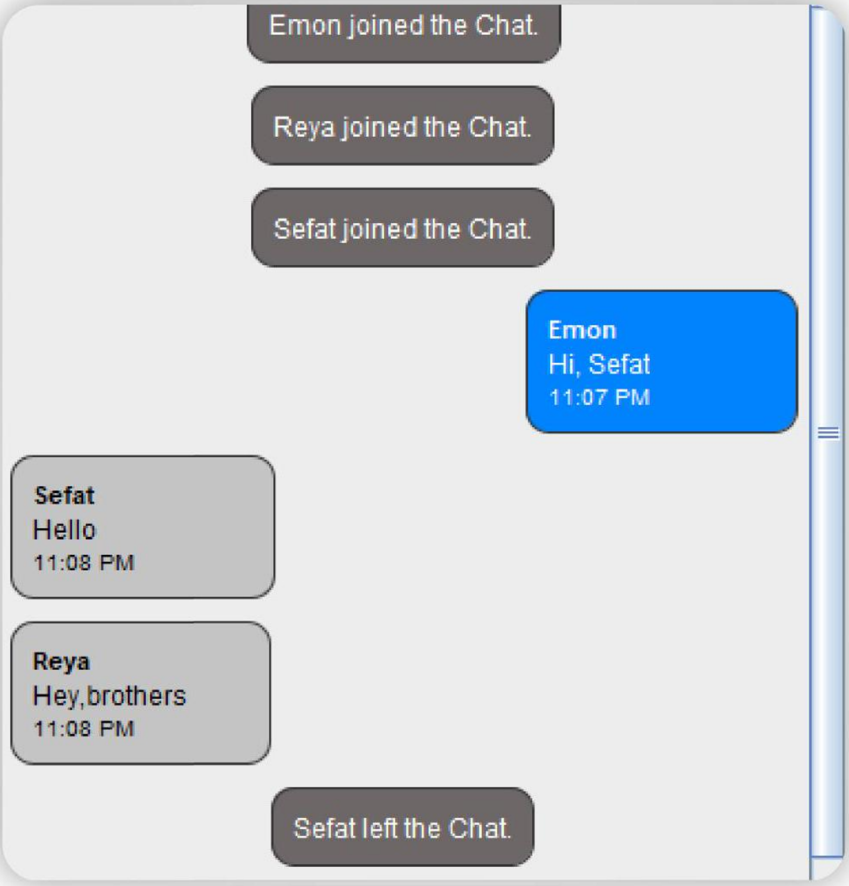


Look In: Documents

File Name:

Files of Type: All Files





Emon joined the Chat.

Reya joined the Chat.

Sefat joined the Chat.

Emon
Hi, Sefat
11:07 PM

Sefat
Hello
11:08 PM

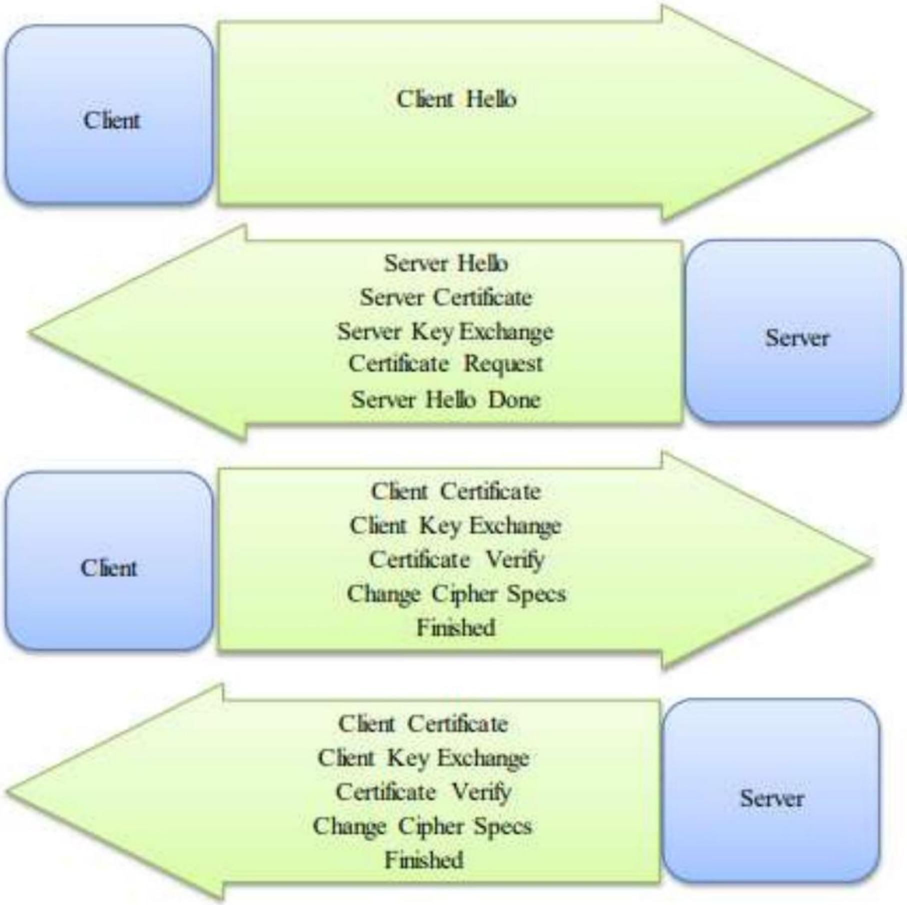
Reya
Hey,brothers
11:08 PM

Sefat left the Chat.

18 SUMMARY:

In this chapter an introduction to the mobile IM applications was presented. Different security issues and background information have been explained and different chat applications have been researched in order to investigate their current security features that they offer to their users.

19 CONNECTION FIGURE:



20 FUTURE WORK:

In order to design very effective secure system different factors should be considered. Although the goal of this thesis was merely to secure messages between two clients, there are some other factors that might be considered for future research such as usability of the application or scalability of the servers or how the design effects the cost of implementation. In order to complete this research the following topics are suggested for future researchers.

21 PERFORMANCE:

The proposed design has not been analyzed to investigate how it effects the performance of the mobile phone. How much it will consume CPU power and how it affects battery drain. Different security algorithms or encryption ciphers might need more computational power and support from the underlying operating system.

22 CONCLUSION:

Privacy has become a major concern for the end user of free services provided by technology giants like Facebook and Google impacts of data falling into the wrong hands. Here I designed an end-to-end encrypted chatting application to address this issue. The user of my chatting application named "Fun" can stay anonymous throughout the chatting session. I have been inspired by several chatting/social media applications such as 4chan, reddit, discord and WhatsApp to design is extremely lightweight secure and portable and compatible on most of the popular operating systems. My solutions to the privacy concern of the users will help

primarily the small to medium scale business internal and communication as the user data except the login credentials will be erased as soon as the session ends.

23 REFERENCES:

https://www.mirrorfly.com/blog/best-secure-messaging-app/

https://www.youtube.com/watch?v=rPp4rQnrG44

https://www.youtube.com/watch?v=1Jj vAh6w0

https://getstream.io/blog/most-secure-messaging-apps/