Active Chat Monitoring and Suspicious Chat Detection

Project report submitted in partial fulfillment of the requirement for the degree

of Bachelor Technology

in

Computer Science and Engineering/Information Technology

By

Dem Zam (151440)
Tshewang Dema (151441)

Under the supervision of

Dr. Amol Vasudeva

to

Department of Computer Science & Engineering and Information Technology
**Jaypee University of Information Technology, Waknaghat, Solan-173234
Himachal Pradesh**

Certificate

I hereby declare that the work presented in this report entitled **"Active Chat Monitoring and Suspicious Chat Detection"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat is an authentic record of our own work carried out over a period from August 2018 to December 2018 under the supervision of **Dr. Amol Vasudeva**.

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Student1 Name: Dem Zam   Rollno: 151440

Student2 Name: Tshewang Dema   Rollno: 151441

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)

Supervisor Name: Dr. Amol Vasudeva

Designation: Assistant Professor

Department name: Computer Science

Dated:

ACKNOWLEDGEMENT

It had always been a pleasure to thank people who have supported and guided us in accomplishment of this project and we are fortunate enough to get a constant support and guidance from many individuals. This project wouldn't have been possible without such supervision and assistance.

We would like to thank our project guide Dr. Amol Vasudeva (Asst. Professor) for his constant support and guidance while working on our project work and for encouraging us all along, for providing all the necessary information for developing a good system.
He supported us and has been instrumental in introducing us to various people while developing this project and in gathering the information that we needed.

We also like to extend our gratitude to all staff in laboratory for their timely support.

ABSTRACT

With the advancement of chat applications over internet, ones messages can be reached all over the world which means it can be used to influence younger generation in both good and bad ways. Although, these chat applications have many advantages like communication can happen anywhere, anytime but it also has disadvantages like terrorist activists can also convey their messages through these chat applications to make other people all kinds of terrorist, cybercrime, etc. So, we propose a chat application system that monitors the various chats going on and detect the suspicious chats too. The server handles all the chat process and scans it for any suspicious words. If there are suspicious words, then an alert is provided to admin and admin can detect that particular chat. The chat history is being saved in the database from which admin will block any suspicious message. Only admin have the authority to access the database. Therefore, our chat application system is mainly to provide secure communication and reduce illegal activities.

Table of Content

List of Figures

List of tables

1. INTRODUCTION

1.1 Introduction

Chat applications allow all kinds of communication including threatening message and illegal activities. For the purpose of reducing such illegal activities, we have proposed a system called Active Chat Monitoring and Suspicious Chat Detection using tools like Eclipse, MySql and Java Language. In this system, many clients who are also known as users can communicate with each other and their chats can be monitored in the server. The suspicious keywords are stored in the database and only admin has the authority to access that database in order to insert new keywords and alter data if required. The server analyzes plain text and if any suspicious words are found, then it alerts admin. The admin, on getting the notification will delete the particular user so that he/she cannot chat again.

In our active chat monitoring and suspicious chat detection system, user can only send and receive messages to and from the other users and cannot monitor like the admin. Without the knowledge of users the admin is able to see the live chat of users and is responsible for watching out the suspicious conversation between users. We are using Port number to connect two users to start the chat. The system was designed in such a way that admin and users are mandatory to register in this system first in order to access the system. So, admin should have valid account to monitor the chat and same goes to users to chat with other registered users.

Nowadays with development and advancement of new technology especially focusing on chat applications, it connects all the people around the world. It is one of the important technologies to unify the society together and to deliver messages within seconds. But with such kind of advantages and benefits, there comes the disadvantages of it too.

With increasing use of chat application, the illegal activities have also risen drastically. Criminals and all sort of terrorist take advantage of this application to

preach their messages and influence the younger generation to do illegal things. And also sending threatening messages and taunting people through chat has became common because of the fact that the other side user will not be able to see the sender's face and all.

So, it is very important to have chat monitoring and detecting system along with the chat application as chat monitoring and detecting system will detect criminal behind the screen. And also people will be aware of such systems and will withdraw themselves from doing illegal things and could make good use of their time.

Thus, our proposed system will be able to make the society more stable by reducing the number of criminals and it also assures the user security and protection. The system will not only detect the suspicious users but also have the ability to delete them so that they cannot join the chat from next time and the other users will not be influenced by the suspicious users. And also there is a least chance of getting threatening messages and thus users may feel secure and relieve.

1.2 Problem Statement

The Active Chat Monitoring and Suspicious Chat Detection System can detect only plain text and cannot be used for any voice chat and videos shared between the users. It cannot detect many suspicious words online hence it is vulnerable for cyber frauds. But if the framework proposed at server side is integrated, there will be significant reduction in cyber crime. The system will track that word even if the statement is not mentioned in that way. The proposed system first detects the suspicious activities when suspicious user sends some suspicious message to another user and then deletes that message instead of deleting it before delivering the message.

1.3 Objectives

Active chat monitoring and suspicious chat detection is a chat system where suspicious users are identified by determining the keywords used by him/her. The main purpose of this project is to develop software that can be used to find a system that identifies deception in messages through communication. The system is designed in a way that the users can easily interact with the system with minimum knowledge to browse the internet. It detects what kinds of information are being passed from the users and can detect their whole conversation without their notice. It can be used along with most widely used social sites like face book, twitter, etc. to provide security against cyber crime. By the use of this system, one can be saved from involving in illegal activities and from being a cyber victim.

1.4 Methodology

The Chat Application features four sections: the client module, the server module, the storage module (i.e database), and the alert module. The code is developed using 4.00 GB of RAM running on windows 10. We implemented the project in Eclipse using Java due to the ease of implementation. We also used Mysql for storing and saving the suspicious keywords so server can easily recognize the user who is performing illegal activities.
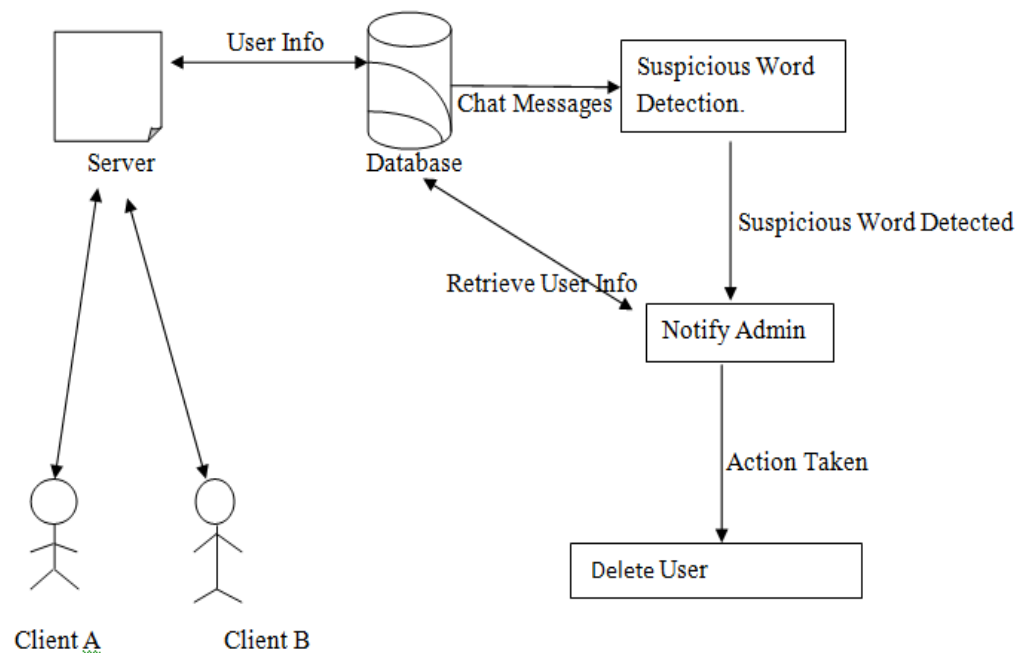

Fig. 1   System methodology

The client module performs the basic functions of the client such as connecting to the server, sending and receiving messages, and handling private messages. It is possible for a server to have a multiple client and this client also handles multiple messages from other clients.

The admin module provides the connection to clients for chatting and monitors their chat. The admin also modifies the keywords and has the authority to delete the suspicious users and is also able to add new keywords.

The storage module is responsible for storing suspicious keywords in the database and whenever a suspicious chat is detected, an alert will be sent to server and server can block or delete the suspicious user by going through the conversation.

Once the user has been deleted from the system and next time the user tries to login, the user is unable to login to the system and cannot chat with other users that are still not deleted and active on the system.

1.5 Proposed system

Our system will detect only online plain text from the discussion forum and will divide or classify the text into different category and it will decide whether the posts are legal or illegal. In our proposed system, the admin that is the server may not always watch the chat. So, in order to prevent illegal or suspicious chatting, admin sets the keywords as suspicious words which will be deleted as an alert will be sent to the admin.

- ➢ The proposed system is a chat facility system.
- ➢ The designed system is a client – server system with database server.
- ➢ The chat system can be used for group discussion.

Advantages

- ➢ The proposed system will reduce any terrorist and illegal activities happening over internet.
- ➢ The proposed system will ensure security for many websites.
- ➢ The proposed system can also be used as evidence for many investigations.
- ➢ This system can also detect any suspicious activities.
- ➢ The major advantage of the proposed system is that the users will not know that they are being monitored or are being checked.

Disadvantages

- ➢ Users need to use provided chat system.
- ➢ The system will track down the word even if word is not meant in that way.
- ➢ Since the keywords are limited, the system is more prone to cyber frauds.

1.6 Features

1) Load balancing

   The amount of load on the server will be limited to time period of admin access as the system will be available only when the admin logs in.

2) Easy accessibility

   Records can be easily stored, retrieved and accessed.

3) User friendly

   The users can accessed this system with the little knowledge of IT. So, the website will be giving a very user friendly approach for the entire user.

4) Efficient and reliable

   The secured and database on the server which will be accessible according to user requirement can be maintained without any maintenance cost is more efficient than storing all the customer data on the spread sheet or in some other record books.

5) Easy maintenance

   Since this system, Active Chat Monitoring and Suspicious Chat Detection over Internet, is designed as easy way, the maintenance is also easy.

2. LITERATURE SURVEY

Besides many advantages and convenient of advanced technologies, there arises many crimes like cyber bullying, fraud, and many more. It is important to prevent criminals from the beginning and is crucial to invent system that could track suspects at any cost.

Murugesan *et al.* [1] (2016) have used statistical corpus based data mining approach for the detection of suspicious activities on online forums. The author used the concept of stop words removal and stemming process so that any suspicious text will become clearer and easy to understand. The approach was to match the keywords with suspicious words by using matching algorithm. In this way the suspicious key words can be recognized. Finally authors have used the keyword spotting techniques, leaning based method and hybrid of defined approaches for the overall recognition of suspicious human activity.

Tayal *et al.* [2] (2015) have proposed the approach of crime detection and criminal identification (CDCI) using data mining approach. The author made modules like Data Extraction (DE) which will extract all unstructured crime data from web sources. Data Processing (DP) which will reduce those extracted data into structured crime data. Other modules like Clustering, Google map, Classification and WAKA implementation are useful for crime detection, criminal identification and crime verification respectively. The author has used k-means clustering algorithm for analyzing crime detection and Google map improves visualization to k-means. KNN classification is used to analyze criminal identification and prediction. The verification of criminals is done with the help of WAKA.
The main purpose for author to develop this kind of system was to reduce crimes and for the betterment of the society. It also helps investigating agencies in crime detection and identification of criminals. So, this system has helped in reducing the crime rate in the society.

With the advancement of chat applications, IC has become day to day utility for everyone and it is one of the latest chat where users can send messages, chat, files and so on. Yahoo chat is a free online chat room service for only yahoo users. It provides users to create public chat and send messages.

Similarly, Skype is also an instant messaging app that provides online text messaging and video services. It allows exchange of digital documents. However, with convenience of such apps come the illegal activities such as increasing terrorist by spreading the message and influencing the innocence, threatening through message, fraud and etc.

In order to reduce such activities and improve the benefits of instant chat applications, applications such as mSpy which is the parental control app for smart phones that allows parents to monitor text messages, calls, current GPS location, Snapchat, Whatsapp and much more. It collects data from the device on which it is installed and display it in the control panel which we can access using any internet browser.

FlexiSpy is software that we install mobile phone. It secretly records events that happen on the phone and delivers this information to a web account, where we can view these reports 24 x 7 from any internet enabled computer or mobile phone. The TruthSpy works directly on the target device and offers wide spectrum of information to the user.

Online social networking sites like Facebook and Google are the great and most popular way to keep in touch with our loved ones and acquaintances. However, such social networking can be used for the purpose of illegal activities such as spreading hate comments which might put the victim into depression and planning terrorism related works. So, Kumar and Singh (2013) [3] have proposed a system for the detection of suspicious users based on their sentiments over chat conversations and comments exchanged on online social networking sites and chat

messengers. The proposed system also identifies the cluster of people exchanging comments about same topics which may result in suspicious activities. The main objective of their system is to analyze the chat messages in social networking sites and to identify group of suspicious users involved in suspicious activities.

Data mining is one of the most powerful ways of extracting useful information or best approach to detect underlying relationships among data using machine learning and artificial intelligence. Now with the advancement of technology, criminals' rate is increasing as they are also adapting smarter ways to commit crimes. So, data mining is powerful tool to detect the activities of criminals by analyzing thir record and information, hence prevents the crimes in future. Hosseinkhani *et al* (2014) [4] have proposed a system for the existing concepts of crime data mining techniques for the detection of suspicious information on the web. According to him, the major challenge for the detection of suspicious activities are the day by day increase in number of cyber data, frequent online transactions and busy network traffic which results to huge amount of illegal activities. He introduced concept such as Web Mining, Criminal Identities and Crime Data Mining techniques.

John Resig Ankur Teredesai [5] have proposed a framework for the analysis of large scale communication media popularly known as IM (instant messaging) and various data mining issues and how these relate to Instant Messaging and terrorism activities. They also focused on user pattern analysis, limited message size and anomaly detection. Their work does not tend to fully detect suspicious messages not even detection of topics.

M. Brindha *et al* [6] have proposed a system to monitor active chat and detect suspicious chat over internet. The proposed system analyzes online plain text from selected discussion group and classifies the text into different group and system will decide whether the text are normal or suspicious. The system developed is chat system and is based on client server.

3. SYSTEM DEVELOPMENT

3.1 System Analysis

The system is designed based on:
- ➢ Server
- ➢ Client

The system is mainly dependent on client and server model. The clients ask permission from or request the server and the server on the other hand responds to the clients request by granting the permission.

Description

Server

A server is a program that responds to the client request and provides services to other programs. A server waits for connection request from client and when the request for connection arrives, it establishes the dedicated connection between client and the server. The client on the other hand is provided a local port number during the connection process. The clients communicate with the server by writing and obtain information by reading from the socket. The server also talks with the client by writing and reading from the socket and it also binds the socket to it.

Client

The client has the information about the host name of the machine and knows on which server it is running. It also knows about the port number where the server is listening. The model used in our system is single server and multiple client models. Multiple clients should be able to connect to the single server.
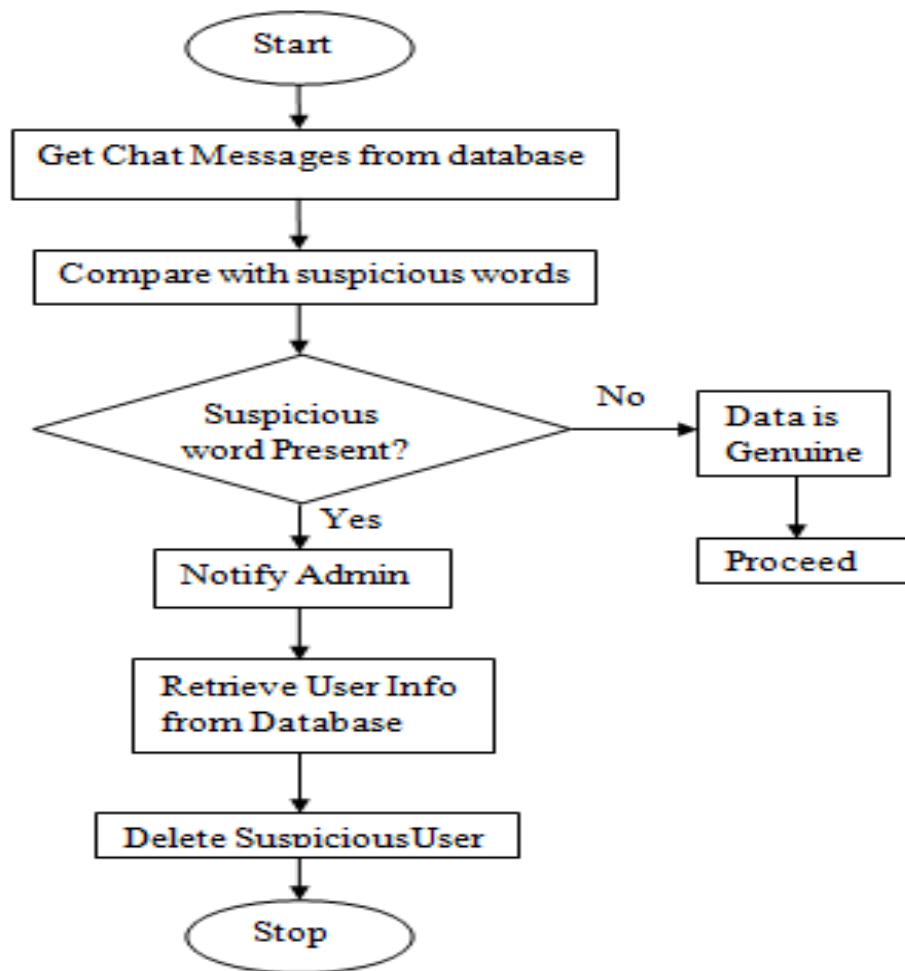
Fig. 2 Flow chart of Active Chat monitoring and Suspicious Chat Detection
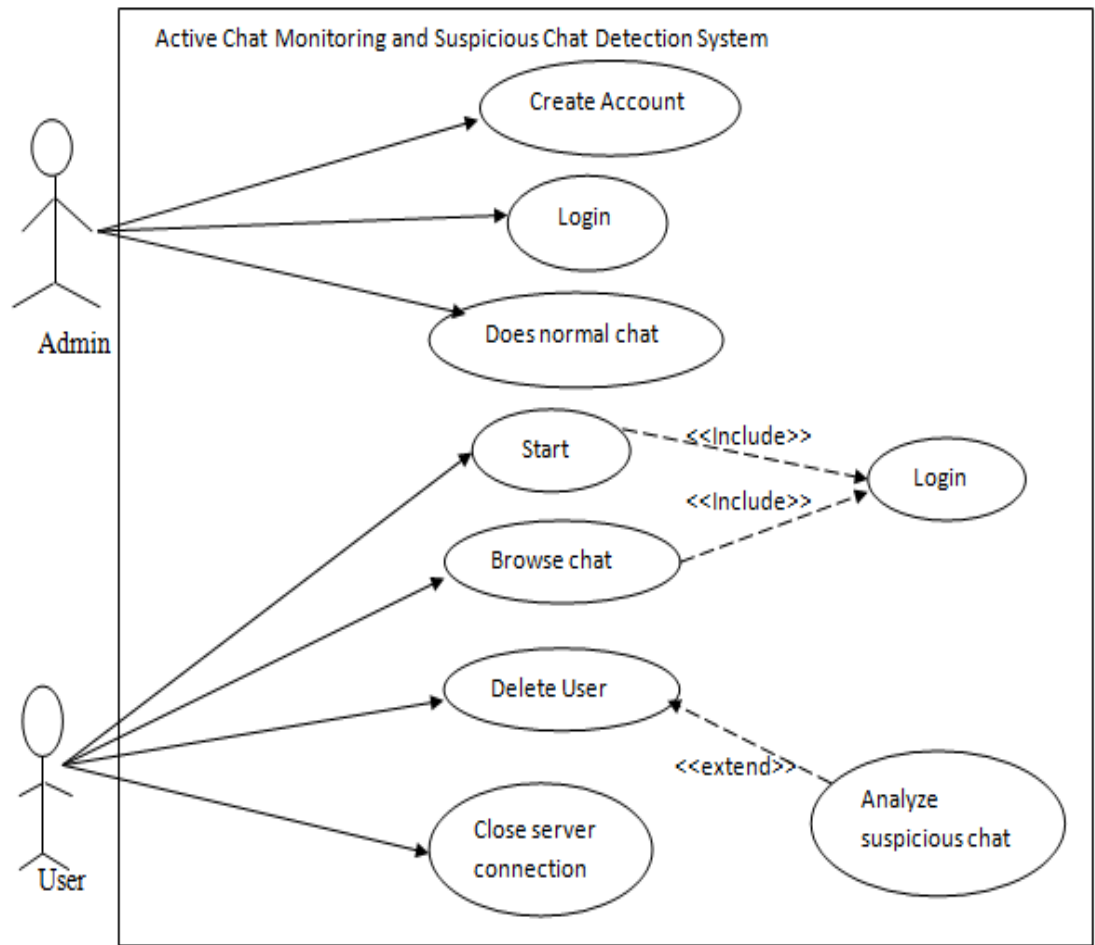
Fig.3 Use case diagram of the proposed system.

From the use case diagram of Active Chat Monitoring and Suspicious Chat Detection, it is clear that both admin and users are required to login to the system. Users, after registering can only do normal chats with other registered users. Admin, on the other hand can do multiple tasks like checking out the chats between users and browsing and updating database which stores the suspicious keywords. If the user uses the suspicious keywords, then the admin gets notification and can delete the user.
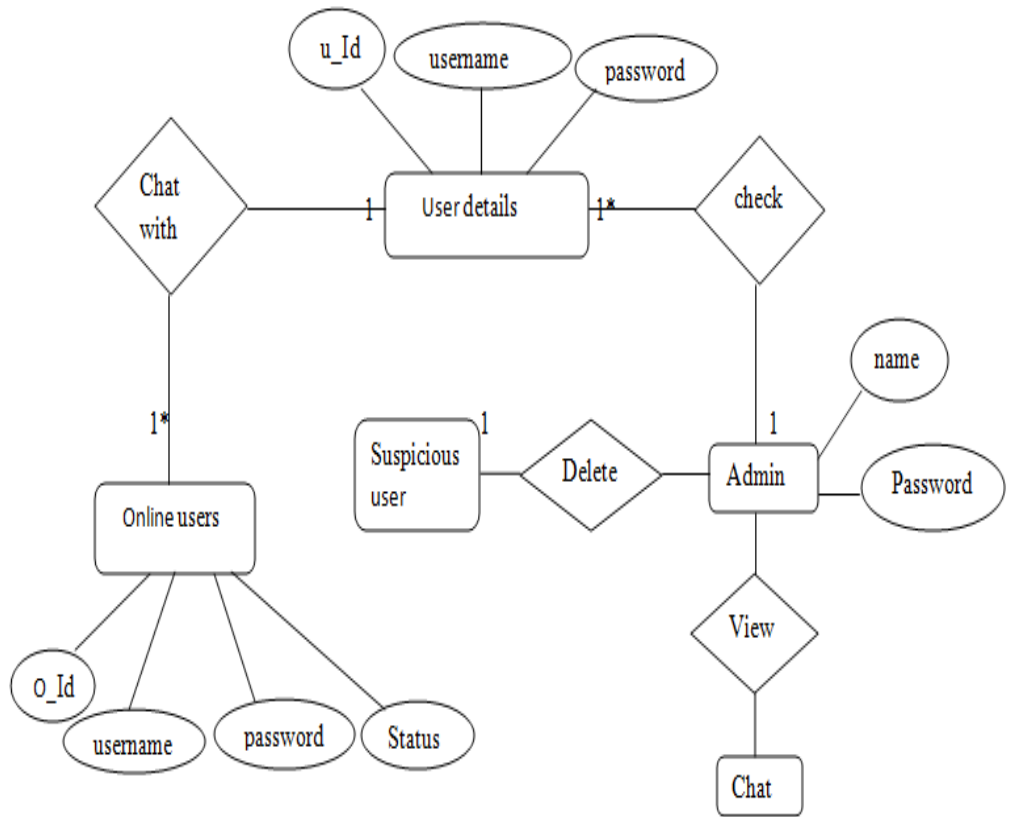
Fig. 4   ER Diagram of Active Chat Monitoring and Suspicious Chat Detection

The entities in above ER diagram such as User details, Admin and Online Users are related to each other through their Id. From the diagram, we can see that users can chat with other users who are online. The users can chat with multiple online at the same time or with particular user privately. The Admin will check the chats of users and has the authority to delete the chats of users if found any suspicious text.

Admin:

Field Name	Data Type	Nullable	Description
Username	Varchar(255)	No	Admin Username
Password	Varchar(255)	No	Password set by admin

    I.   Data Dictionary of admin

User:

Field Name	Data Type	Nullable	Description
User Id	Integer(6)	No	Unique Number
Username	Varchar(255)	No	Admin Username
Password	Varchar(255)	No	User Password

    II.   Data Dictionary of user

Online users:

Field Name	Data Type	Nullable	Description
User Id	Integer(6)	No	Unique Number
From Name	Varchar(255)	No	User name from whom the message is received
To Name	Varchar(255)	No	User name to whom the message is sent

    III.   Data Dictionary of online users

3.2 Software Architecture

Socket Overview

A socket is an object that allows communication between two different processes on different or same machine. It is able to deliver and receive information on data down disconnection. Data is sent in the form of blocks of and these blocks are referred to as packets. Every packet that passes over the web or internet should use IP (Internet Protocol). It means that the source address and destination address has to be included in the packets. Packets contain a port number and these port numbers are important while programming your own network system.

Port numbers are of two types:

- ➢ UDP(User Datagram Protocol)
- ➢ TCP/IP(Transmission Control Protocol)

UDP (User Datagram Protocol) is connectionless and unreliable and it has lower latency as compared to TCP/IP. However, UDP can be considered easier to use than TCP, if data integrity is not concerned. TCP/IP on other hand is more complex but it ensures that data won't be corrupted while passing over the internet. TCP/IP is connection Oriented and it is a reliable protocol.

UDP Ports

The User Datagram Protocol, which is connectionless, and unreliable uses port number and IP address to identify the destination application. The UDP port is of 16-bit address and the port number is different from much physical port on the system.

The UDP datagram header contains four fields:

- ➢ Source Port Number

- ➢ Destination Port Number
- ➢ Datagram size
- ➢ Checksum

Connection

Active Chat Monitoring and Suspicious Chat Detection application module deals with making connection between the desired host system and selected system from the list. The connection is established using socket protocol which makes use of ports number to deliver and receive blocks which is known as packets from one system to other system.

3.3 MODULES:

The system is developed using:

- ➤ Registration module
- ➤ Login module
- ➤ Admin module
- ➤ User module
- ➤ Keywords
- ➤ Delete

Module description:

Registration:

Both the admin and client have to register before logging into chat application. Registration is must as without registration the user won't be able to access the chat application.

Login:

After registration is done, both the admin that is the server and client can login with their registered email id and password. After logging in, the admin can monitor the chat and the client or user can join the chat group or discussion forum and they can send their messages to other client.

Admin:

The major task of admin is to set suspicious keywords into the system and to monitor the chat messages of the client in order to detect the illegal or suspicious activity over the internet.

User:

User which is also known as client is responsible for chatting and sending messages over the web. They can chat privately or publicly depending upon the content of their messages. These clients are also responsible for chatting over the web using suspicious words.

Keywords:

Keywords are the set of suspicious words which are provided by admin for the chatting purposes. These keywords will be stored in database and an alert message will be provided to the admin whenever the user uses this keywords.

Delete:

Delete is also set by the admin. It means the account will be deleted by the admin if found doing illegal activity. Once a user is deleted, he or she must again register themselves in order to join the chat system or discussion forum.

Functional requirements

➢ User
➢ Administrator
➢ Keywords
➢ Send Message
➢ Message Status

User

User which is also known as the client is responsible for joining the discussion forum and chatting with the other online users. These users are also responsible for using suspicious words.

Administrator

Message Status

Admin which is also known as the server is responsible for setting the suspicious keywords. The admin is also responsible for monitoring the whole chat and deleting or blocking the user in case suspicious or illegal activities been found.

Keywords

Keywords are the set of the words that are being set by the admin as the suspicious keywords. In case, online users are chatting using suspicious or illegal words, an alert will be provided to the admin and admin on monitoring or checking the whole chat will take action. Admin will delete or block the user if found using suspicious words and keep it as it is if not found guilty.

Send Message

Send Message is a button that is used to send the messages to the online users. This button is often used by the users to deliver their messages to the final destination. Users can send messages either privately or publicly.

Message Status refers to the status of the messages that is whether the message that has been delivered contains any suspicious or illegal contents or whether it is the normal messages. User or the client can take actions based on the status of the messages.

Non Functional Requirement

- ➢ Privacy
- ➢ Reliability
- ➢ Robustness
- ➢ Performance

Description

Privacy

The system should ensure privacy and security to its end users. The messages send between the users or the clients should be encrypted to ensure privacy.

Reliability

The system should be reliable. It should protect its end users from virus and it should provide its end user a user friendly approach.

Performance

Application must be light weight and send message should be available 24/7.

3.4 System Architecture
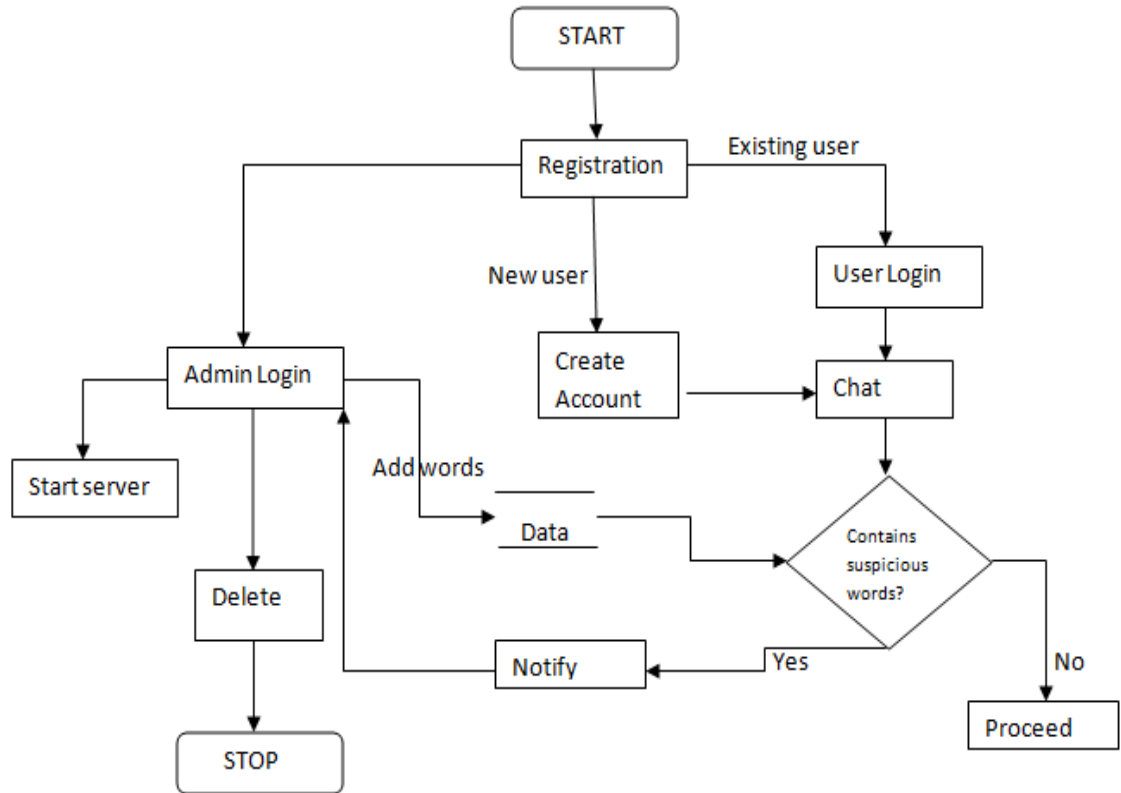
Fig. 5   System Architecture

In this system, both admin and user have to be authenticated admin and user to access the system. The authenticated admin will start the server and authenticated users will the do the normal chat. The suspicious keywords will be selected by admin and if any of the users use that keyword, the system will notify the user as suspicious. Then, the admin will delete that particular user from the system so that he will not be able to login again and chat with other users.

3.5 Mathematical

Mathematical Formulation:

S=I,F,O

Where,

I=Set of inputs

i1=Normal text message

i2=suspicious words

F=Set of functions

f1=deletion of words

f2=word substitution

O=Set of outputs

o1=Messages in normal form

o2=Identity of suspected person

Success Condition = Gets the relevant information from communication of suspected person.

Failure Condition = Connection is loss system does not work.

4. ALGORITHM

4.1 Algorithm of Active chat monitoring and suspicious chat detection:

Input: Text messages of chatters

Output: Suspicious words

Steps:

Start

1. Store user list and keywords in database.

2. Retrieve user information.

3. Monitor chat in server

4. Detect suspicious user

5. Notify admin

6. Delete the suspicious user.

7. Stop

5. Testing

Testing is a method of executing a source code in order to find an error. Testing of designed system is important in implementation of the system. A program should be tested to find any bugs in the application. Testing is done along with application being developed, and the more the application being developed, the more the testing has to be done. By testing the program, we are able to reduce the possibility of error or malfunction in the program. Lots of parameters and function implementation might change, and it may cause the system to not working as it should, even when the code is compiling without any errors.

We should also test the system to check that no function has been missed out while running the project. Testing is done after completion of the project. There are lots of test types to ensure that the system is working fully and is working as expected. Here, we will focus on unit testing and integration testing.

Unit Testing is the testing of unit or single components. It is done as part of unit test phase of software life cycle and it can be done as two different phases. We tested for the correct names of the application connected to the network and then we tested for two way connection between the server and the client. We can either test top down or bottom up and then isolation in unit testing.

After the unit testing, we have conducted integration testing. The main objective of integration testing is to check whether the modules are able to integrate properly, that is testing interfaces between the modules. After the connections are established between the modules, we have to conduct total testing. And system testing is done after the completion of the application.

Tools used:

Software Requirement:

Eclipse

Java Applicatio

Mysql Database

Hardware requirement:

Windows 10

6. RESULTS AND PERFORMANCE ANALYSES

6.1 Performance analyses

The project is made based on socket programming where the client makes request to server and server perform the request made by the client. The server is implemented by two classes and they are StartServer and Thread. The StartServer starts the server listening on the specific port. A Thread is created when a new client gets connected in order to serve that client.

The server is able to handle multiple clients at the same time because each connection processed in separate thread. The Thread class has the responsibility of reading the messages that the client sent and these messages are broadcast to other clients.

The client is implanted by three classes: Client, ReadThread and Write Thread. The Client starts thee client program and connects to the server. The connection of client is specified by IP address and Port number. The two threads, ReadThread and Write Thread, are created right after the connection is made.

The ReadThread reads the input from the server and prints it on the console until the client is disconnected. The WriteThread reads input from the user and sends it to the server.

Code

Server:

```java
package server;

import java.awt.EventQueue;

public class Server extends javax.swing.JFrame {


    private static final long serialVersionUID = 1L;
    private JFrame frmServer;
    ArrayList<PrintWriter> clientOutputStreams = new ArrayList<>();
        ArrayList<String> users = new ArrayList<>();


        public class ClientHandler implements Runnable
        {
            BufferedReader reader;
            Socket sock;
            PrintWriter client;
            int id_privateChat ;


            public ClientHandler(Socket clientSocket, PrintWriter user)
            {
                client = user;

                try
                {
                    sock = clientSocket;
                    InputStreamReader isReader = new InputStreamReader(sock.getInputStream());
                    reader = new BufferedReader(isReader);
                }
                catch (Exception ex)
```

```java
                for (String current_user : users)
                {
                txtarea_chat.append(current_user + ", With ID = " + getid(current_user) );
                txtarea_chat.append("\n");
                }
            }else {
                txtarea_chat.append(" No one is online ...");
            }// TODO Auto-generated method stub


        }

    protected void btn_startActionPerformed(java.awt.event.ActionEvent evt) {
        Thread starter = new Thread(new ServerStart());
        starter.start();
        txtarea_chat.setEditable(false);
        txtarea_chat.append(" Server has been started \n Waiting for connection ...");
        // TODO Auto-generated method stub

    }



        private javax.swing.JButton btn_clear;
        private javax.swing.JButton btn_close;
        private javax.swing.JButton btn_start;
        private javax.swing.JButton btn_online;
        private javax.swing.JTextArea txtarea_chat;
        private JScrollPane scrollPane;
}
```

Client:


```java
package client;

import java.awt.EventQueue;

public class Client {

    public static String username1;
    String address = "localhost";
    @SuppressWarnings({ "unchecked", "rawtypes" })
    ArrayList<String> users = new ArrayList();
    int port = 8000;
    public static Boolean isConnected = false;

    Socket sock;
    BufferedReader reader;
    PrintWriter writer;

    public static JFrame frmClient;
    private JTextField txt_address;
    public static JTextField txt_username;
    private JTextField txt_port;
    private static JTextArea txtarea_chat;
    public static JTextField txt_input;

    /**
     * Launch the application.
     */
    public static void main(String[] args) {

        EventQueue.invokeLater(new Runnable() {
            public void run() {
                try {
                    Client window = new Client();
```



```java
            txt_address = new JTextField();
            txt_address.setText("localhost");
            txt_address.setEditable(false);
            txt_address.setBounds(86, 8, 123, 20);
            frmClient.getContentPane().add(txt_address);
            txt_address.setColumns(10);

            txt_username = new JTextField();

            try{
                Class.forName("com.mysql.cj.jdbc.Driver");
                Connection con = DriverManager.getConnection("jdbc:mysql://localhost:3306/login", "root", "");
                Statement stmt = con.createStatement();
                String sql = "Select * from users where username = '"+User_Login.txtUsername.getText()+"' and password = '"+User_Login.txtPas
                stmt.executeQuery(sql);
                txt_username.setText(User_Login.txtUsername.getText());

                } catch(Exception eve) {
                    System.out.print(eve);


            }

            txt_username.setEditable(false);
            txt_username.setBounds(86, 33, 123, 20);
            frmClient.getContentPane().add(txt_username);
            txt_username.setColumns(10);

            txt_port = new JTextField();
            txt_port.setText("8000");
            txt_port.setEditable(false);
            txt_port.setBounds(416, 8, 58, 20);
            frmClient.getContentPane().add(txt_port);
```

30

6.2 Results

Through this chat application, we can study the characteristics or behavior of each user in the chat or discussion forum, for example what is their intention and plan while chatting. Our system have server which acts as an admin and client or user. The clients who are also called user chat with each other and their chat will be monitored by server. User can chat privately if they don't want to share the message with the entire user who are online and can chat publicly if they don't have any private message. This chat application helps reduce terrorist activities as it monitors all the chat that is happening in the discussion forum. The advantage of our system is that it monitors the entire chat without the knowledge of the user.

An alert message will be provided to server if the user or clients are using suspicious words. The admin that is the server can then monitor or check the message and confirm whether the user has use suspicious words. If the users have use suspicious words, then that particular user will be deleted and they won't be able to login. They again have to register or sign up or make a new account if they want to join the chat forum.

Though this process, our system will be able to ensure security and reliability to the user and other people and the stored data will also be secured thus reducing terrorist activities.

Output:

Step 1: Admin logged in and started the server and user logged in and connected to server.
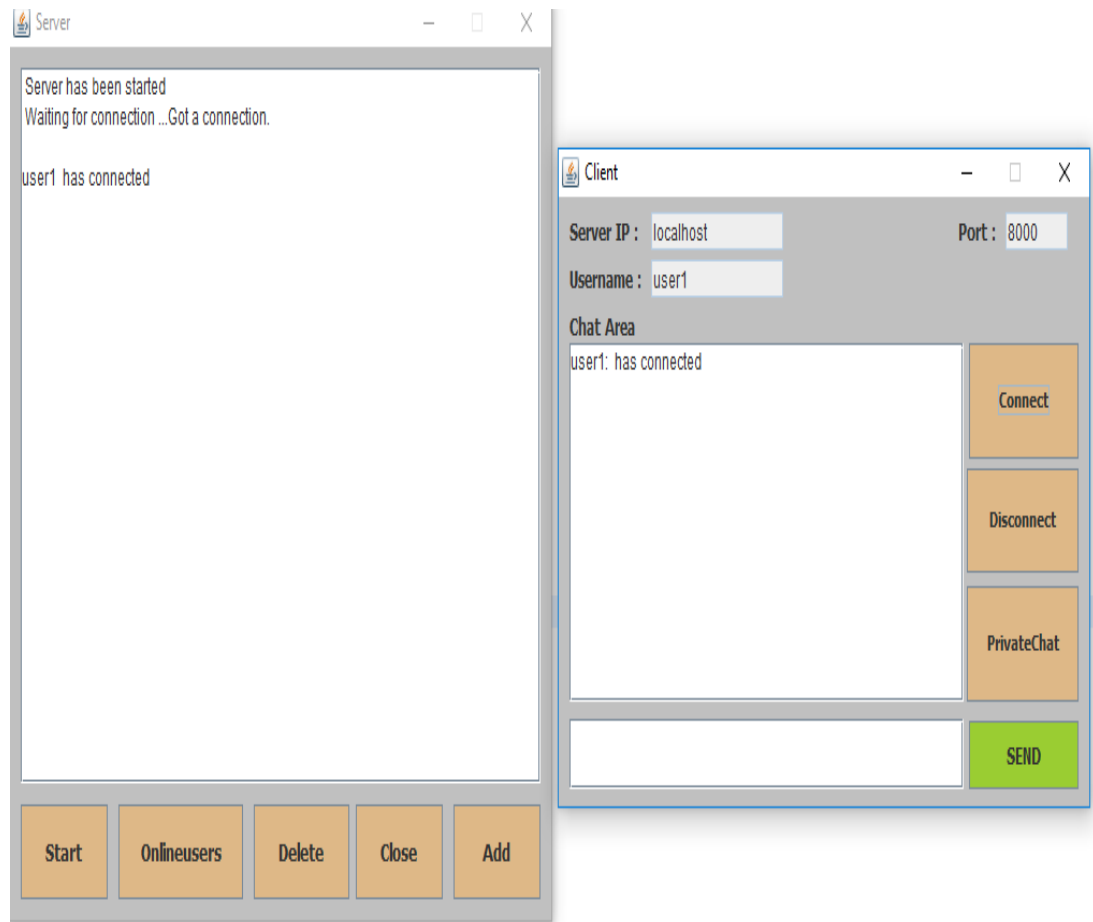
Step 2: Suspicious keywords added
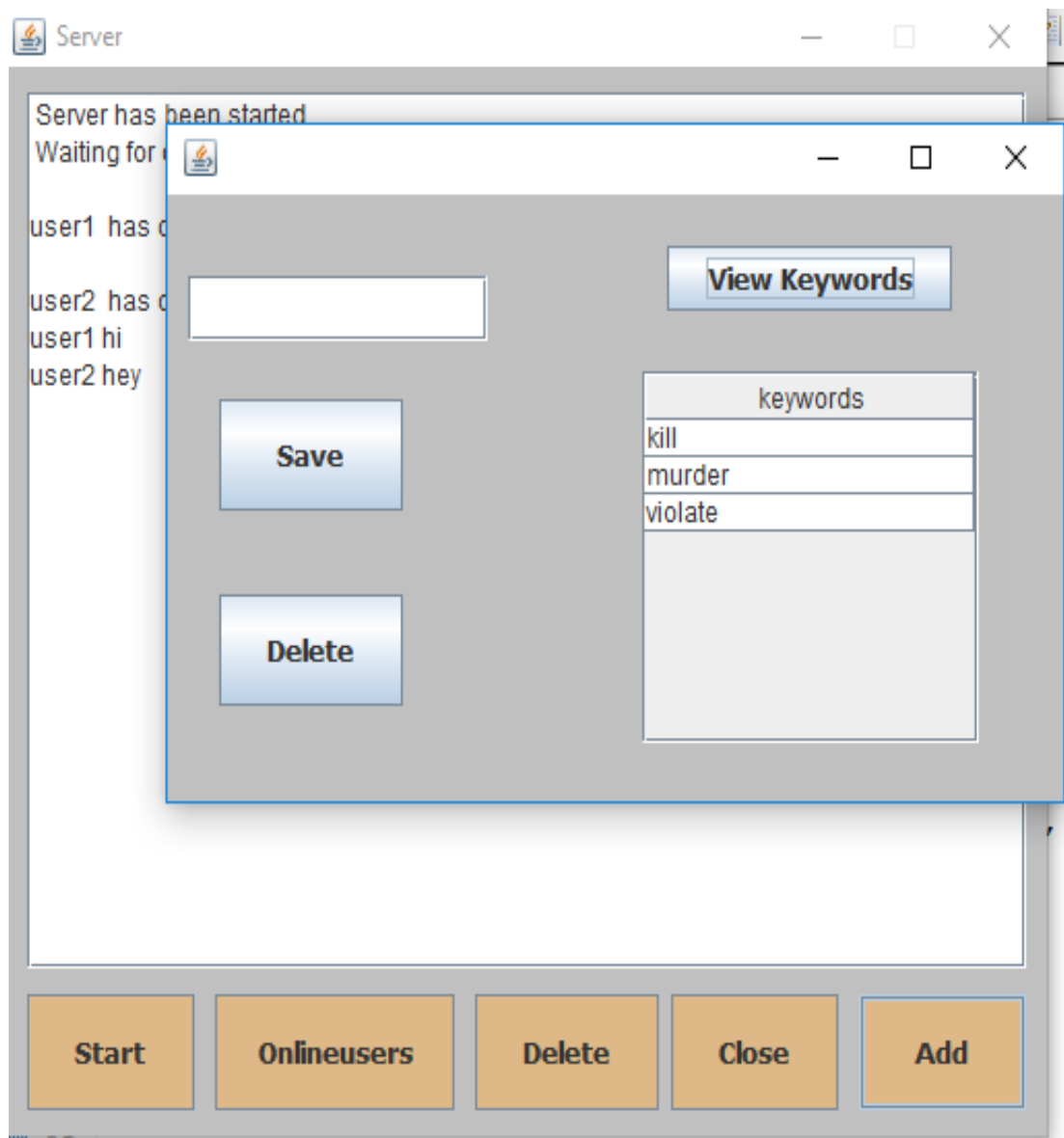
Step 3: Suspicious keyword detected
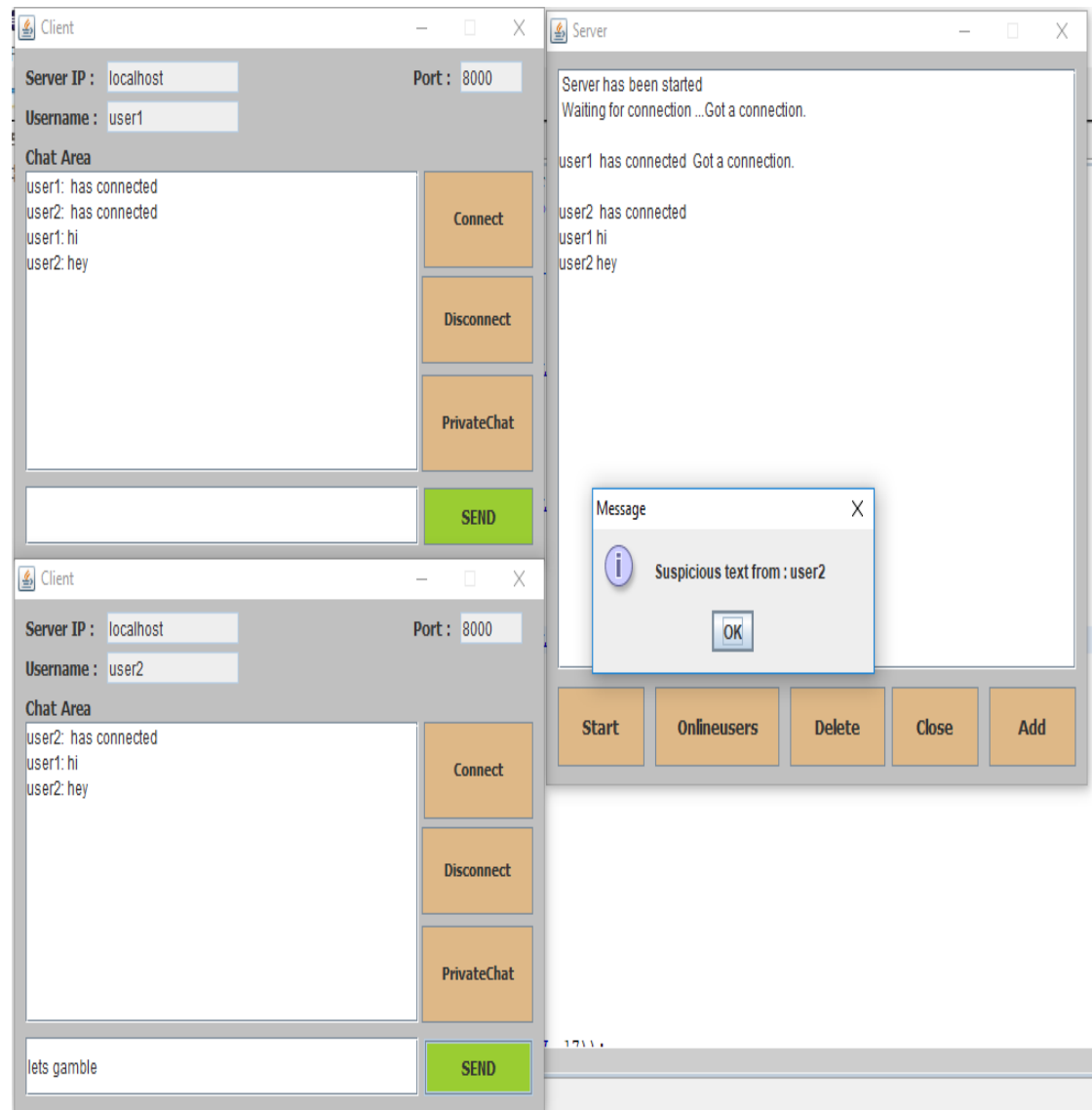
Step 4: Admin deleted the user
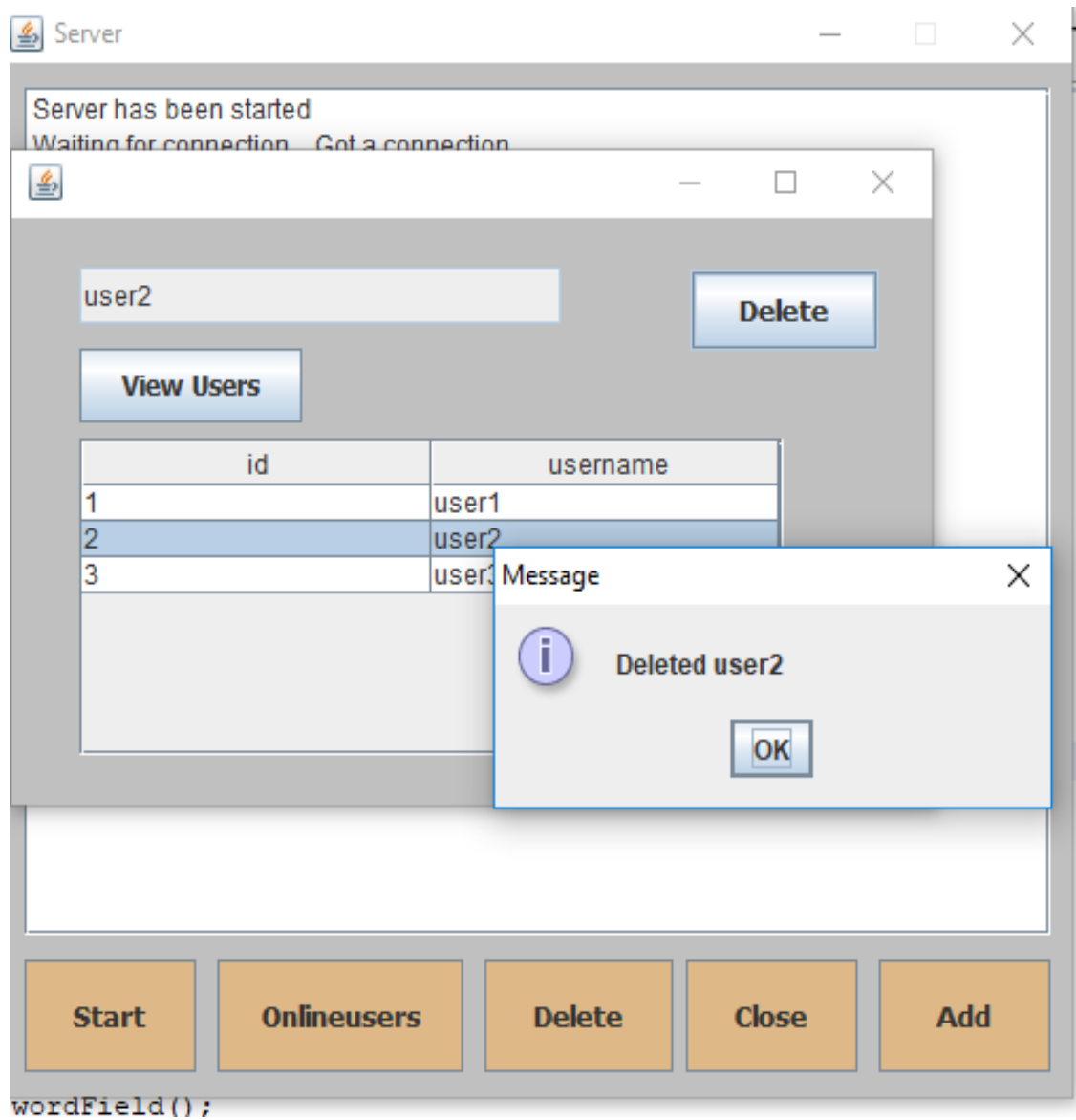
Step 5: User got deleted and could not log in
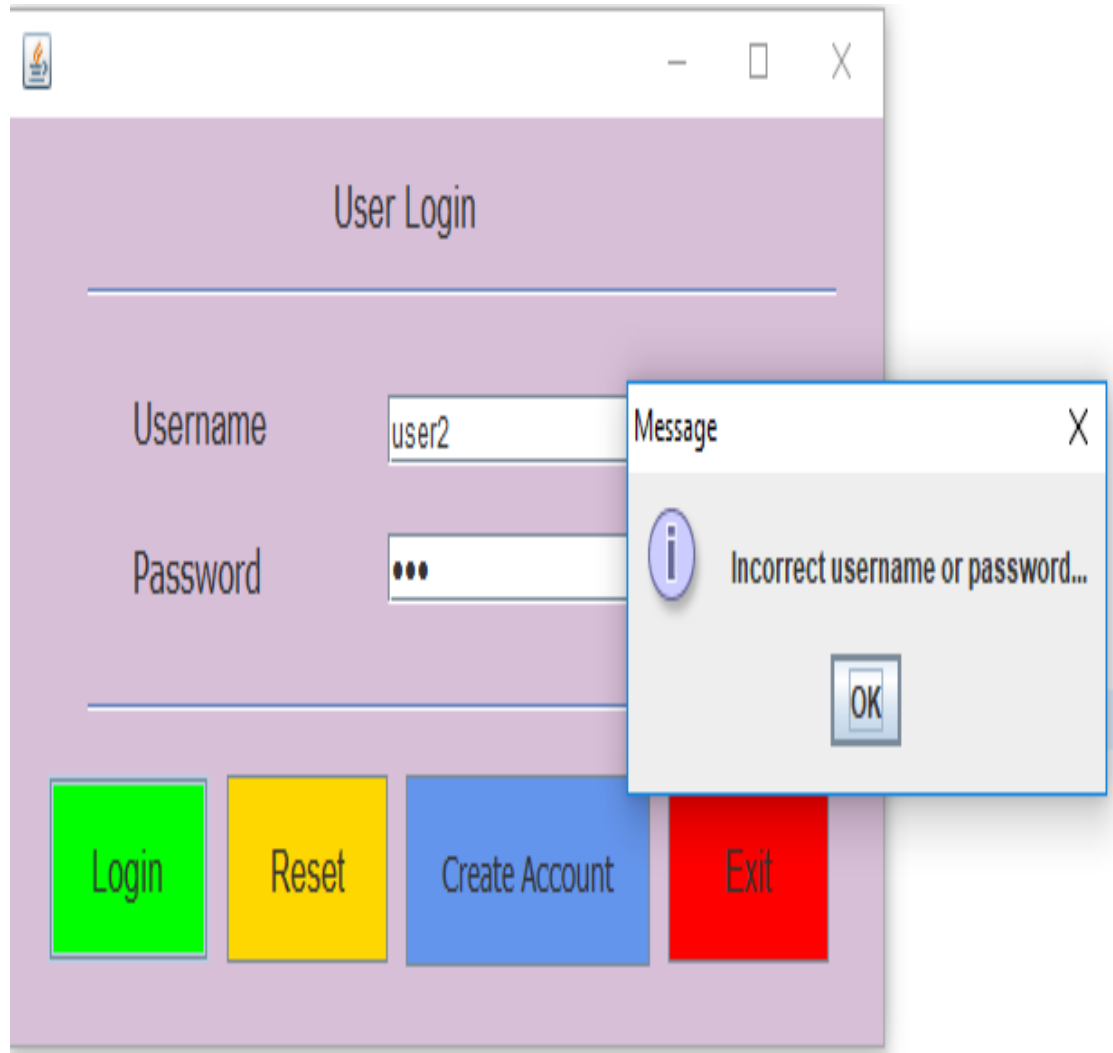
7. CONCLUSION

7.1 Conclusion

The Active Chat Monitoring and Suspicious Chat Detection System will analyze plain text and can detect the suspicious words. In this system the users can communicate with each other and admin monitors the chat between the users. This system can be also used to detect suspicious words used between the users and avoid further usage of those words by blocking it from the server database.

Since the target users will not have the knowledge that they are being detected, it easier to keep track of the suspects without being notice by them and have full control over them. Thus, his system will reduce illegal activities going on and probably reduce the number of users getting involved in such kind of activities. So, this system provides security for users and also admin could know what plans are going on between the users.

7.2 Future Scope

In future, this system can be used as an evidence for investigation activities. In the investigation activities, this system can store all the information about the user and what kind of suspicious keywords he/she has used. Later during the investigation, the data is retrieved from the system and used as evidence.

Using this application we will able to give security alert to government agencies about all sorts of crime going on in the country. Whenever suspicious activities are going on in the chat forum, the system is capable to give alert saying that particular user is suspicious. In this way one does not have to keep monitoring all the time and thus saves the time.

We can also use this system in banks to detect frauds and save one from being the victim. It can be helpful to parents to keep track of their children and save their child from being cyber victim. By installing such system on child's phone, parents can detect whether their child is not being bullied by other children or whether their child is not the suspects. In this way, parents are able to keep their children in right direction and also it is easy for parents to watch out their children.

And also it can be use in the business by managers to monitor their employees and know the intentions of their employees. Without being noticed by employees, the manager could detect what are going on among employees and how loyal they are to the company. So, this system could be used to detect the trust of employees and how well they are performing their job.

7.3 Applications

> ➢ The proposed system can be used by officials to check whether there are any suspicious activities going on over the internet.

> ➢ The proposed system can also be used as an extension on sites like twitter, email etc…

> ➢ It can also be used as evidence by detectives.

> ➢ The system can be also used to extract or identify the information or data of suspicious users

REFERENCES

1. Murugesan, M. Suruthi, R. Pavitha Devi, S. Deepthi, V. Sri Lavanya, and Annie Princy. "Automated Monitoring Suspicious Discussions on Online Forums Using Data Mining Statistical Corpus Based Approach." Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on, pp. 2015-2020. IEEE, 2016. Imperial Journal of Interdisciplinary Research [8].

2. Tayal, Devendra Kumar, Arti Jain, Surbhi Arora, Surbhi Agarwal, Tushar Gupta, and Nikhil Tyagi. "Crime detection and criminal identification in India using data mining techniques." 2, no. 5 (2016).

3. Kumar, A.S.; Singh, S., "Detection of User Cluster with Suspicious Activity in Online Social Networking Sites," Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference on , pp.220,225, 15-17 Dec. 2013 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=671416 7&isnumber=6714118

4. J. Hosseinkhani, "Detecting suspicion information on the Web using crime data mining techniques," International Journal of Advanced Computer Science and Information Technology, vol. 3, pp. 32-41, 2014

5. John Resig Ankur Teredesai, "Data Mining Research Group", Department of Computer Science, Rochester nstitute of Technology, {jer5513,amt}@cs.rit.edu

6. M. Brindha[1], V. Vishnupriya[2], S. Rohini[3], M. Udhayamoorthi[4], K.S.Mohan[5], "Active Chat Monitoring and Suspicious Chat Detection over Internet", [1,2,3]UG Scholars, Deparment of IT, SNS College of Technology, Coimbatore, Tamilnadu, India. [4,5]Assistant Professor, Department of IT, SNS College of Technology.

7. Ms. Pooja S. Kade1, Prof. N.M. Dhande, " A Paper on Web Data Segmentation for Terrorism Detection using Named Entity Recognition Technique" presented at International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056,Volume: 04 Issue: 01 | Jan -2017.

8. M.F. Porter, (1980) "An algorithm for suffix stripping", Program, Vol. 14 Issue: 3, pp.130-137".

9. T.K.Ho, ―"Stop Word Location and Identification for Adaptive Text Recognition".

10. T.Bhaskar, ―"Fast identification of stop words for font learning and keyword spotting".

APPENDIX

```java
package server;

importjava.awt.EventQueue;

public class Server extends javax.swing.JFrame {

        private static final long serialVersionUID = 1L;

        privateJFramefrmServer;

        ArrayList<PrintWriter>clientOutputStreams = new ArrayList<>();

        ArrayList<String> users = new ArrayList<>();

        public class ClientHandler implements Runnable

           {

        BufferedReader reader;

            Socket sock;

        PrintWriter client;

        intid_privateChat ;

        publicClientHandler(Socket clientSocket, PrintWriter user)

            {

        client = user;

        try

              {

        sock = clientSocket;

        InputStreamReaderisReader = new InputStreamReader(sock.getInputStream());

        reader = new BufferedReader(isReader);

              }
```

```java
            catch (Exception ex)

                {

            txtarea_chat.append("Unexpected error... \n");

                }

            }

@Override
        public void run() {
                String message, connect = "Connect", disconnect = "Disconnect", chat = "Chat",
        privatemsg = "private" ;

            String[] data;

try

                {

            while ((message = reader.readLine()) != null)

                {

            txtarea_chat.append("\n");

                data = message.split(":");

                int counter2steps = 0;

                for (String token:data)

                        {

                        if(counter2steps!=2)

                txtarea_chat.append(token + " ");

                counter2steps++;

                        }

    if (data[2].equals(connect))

                        {

                tellEveryone((data[0] + ":" + data[1] + ":" + chat));
```

```java
                userAdd(data[0]);

                        }
                else if (data[2].equals(disconnect))

                        {
                tellEveryone((data[0] + "  has :Disconnected" + ":" + chat));


                clientOutputStreams.remove(getid(data[0]));
                userRemove(data[0]);

                        }
                else if (data[2].equals(chat))  {
                tellEveryone(message);

                        }
                else if (data[2].equals(privatemsg)) {


                intrecievedID  = getid(data[3]);
        if (recievedID != -1) {

        tellthispersononly(message, recievedID, data[3]);

                } else {

                tellthispersononly(message, recievedID, data[0]);

                String Errormsg = data[0]+ ": User Not Found from the online users :private";

                tellthispersononly(Errormsg, getid(data[0]), data[0]);

                        JOptionPane.showMessageDialog(null, "No Name of the online users matches
this name : "+ data[3] +"\n Check the online users correctly ", "This user is not found or not
online", JOptionPane.ERROR_MESSAGE);

        }else if (data[2].equals("request")) {

        intrecievedID  ;

        StringBuilderstringBuilder = new StringBuilder();
```

```java
        for (String current_user : users)
                {
recievedID  =getid(current_user);

stringBuilder.append(current_user).append(", With ID = ").append(recievedID);

stringBuilder.append(".  ");

                }
recievedID  =getid(data[0]);

                String finalString = stringBuilder.toString();

finalString = data[0]+ ":" +finalString+ ":" + "request" ;

tellthispersononly(finalString, recievedID, data[0]);

                }
else
                {
txtarea_chat.append("No Conditions were met. \n");

                }

                }

            }
  catch (Exception ex)
                {
  txtarea_chat.append("Lost the connection. \n");

                }

                }

    }
  public static void main(String[] args) {
            EventQueue.invokeLater(new Runnable() {
                    public void run() {
                            try {
```

```java
for (String current_user : users)

        {

txtarea_chat.append(current_user + ", With ID = " + getid(current_user) );

txtarea_chat.append("\n");

        }

}else {

        txtarea_chat.append(" No one is online ...");

    }// TODO Auto-generated method stub


        }


        protected void btn_startActionPerformed(java.awt.event.ActionEventevt) {

                Thread starter = new Thread(new ServerStart());

starter.start();

txtarea_chat.setEditable(false);

  txtarea_chat.append(" Server has been started \n Waiting for connection ...");

        // TODO Auto-generated method stub


        }

        privatejavax.swing.JButtonbtn_clear;

        privatejavax.swing.JButtonbtn_close;

        privatejavax.swing.JButtonbtn_start;

        privatejavax.swing.JButtonbtn_online;

        privatejavax.swing.JTextAreatxtarea_chat;

        privateJScrollPanescrollPane;

  }
```