KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY (KIIT)
Deemed to be University U/S 3 of UGC Act, 1956

Topic : Active Chat Monitoring and Suspicious Chat Detection .

Submitted by :

Ayusha Sharma(21051124)
Anand Sahoo(21051536)
Maitri Keshri(21052907)

Under the guidance of
Dr. Saurabh Bilgaiyan

Table of Contents

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, cyber crime, 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 .

Objective & Methodology

Objective :-

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 .

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.

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 .

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 .

System Development

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.

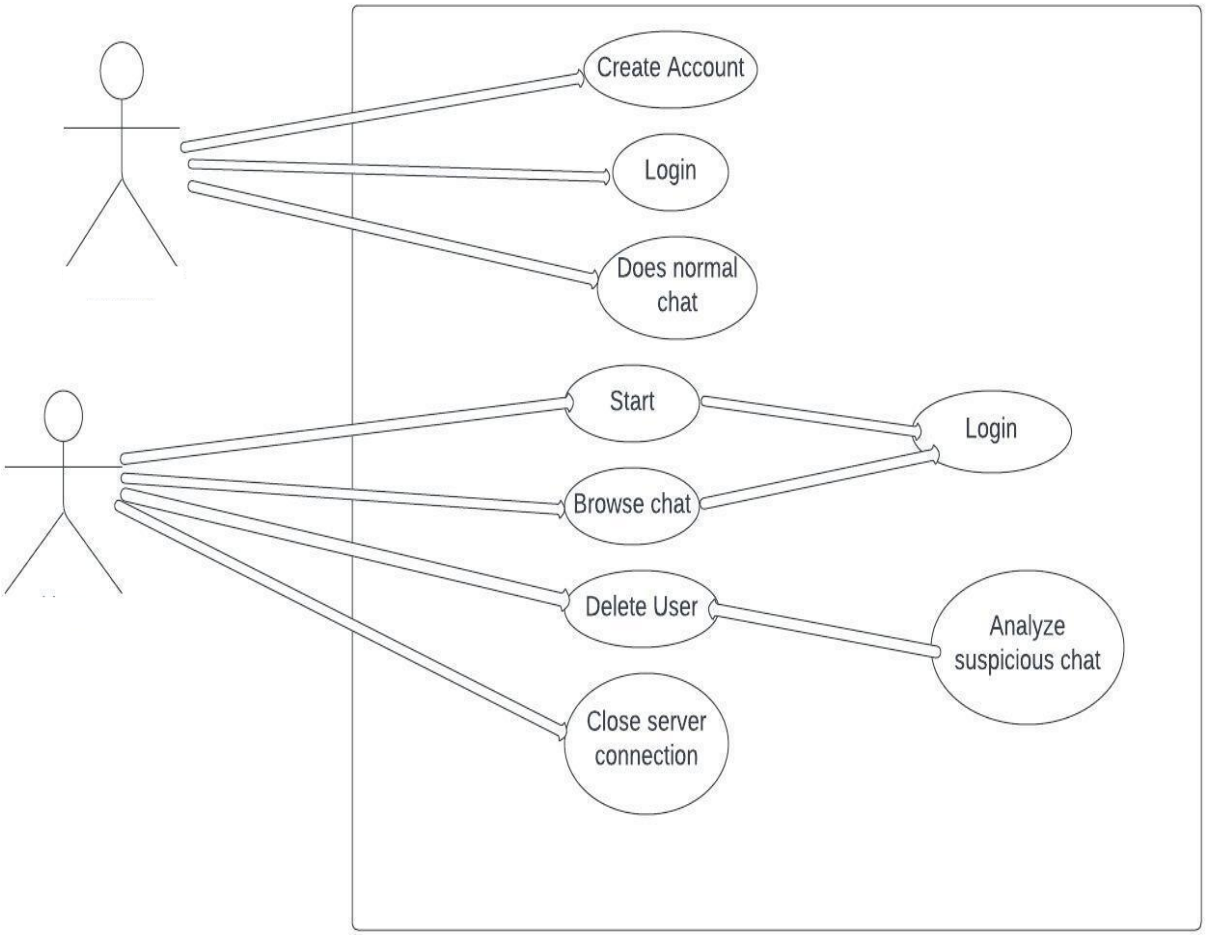
Description :-

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

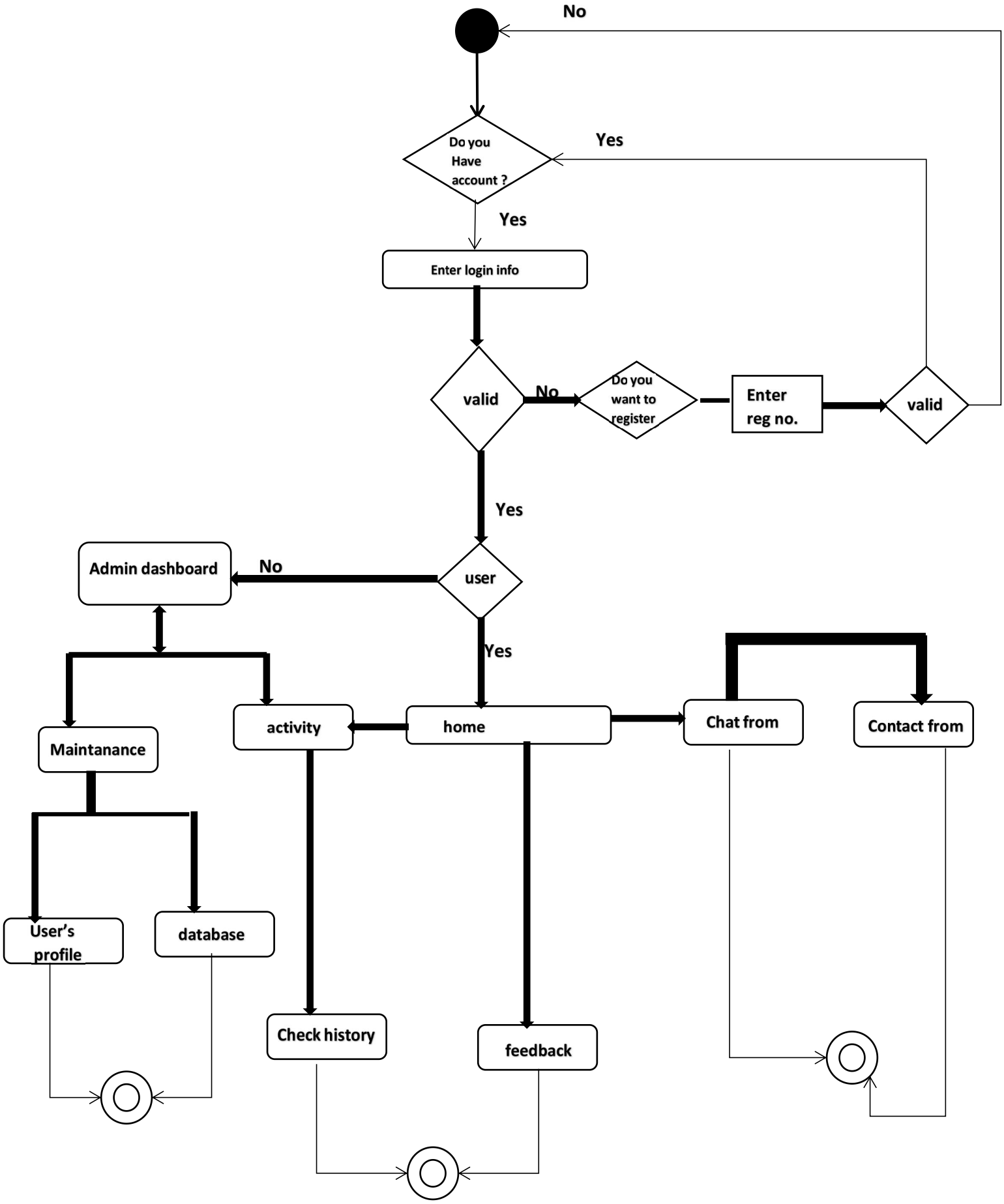
The client has the information about the host name of the machine and knows on which server it is running. It also knows about the port number where the server is listening. The model used in our system is single server and multiple client models. Multiple clients should be able to connect to the single server .



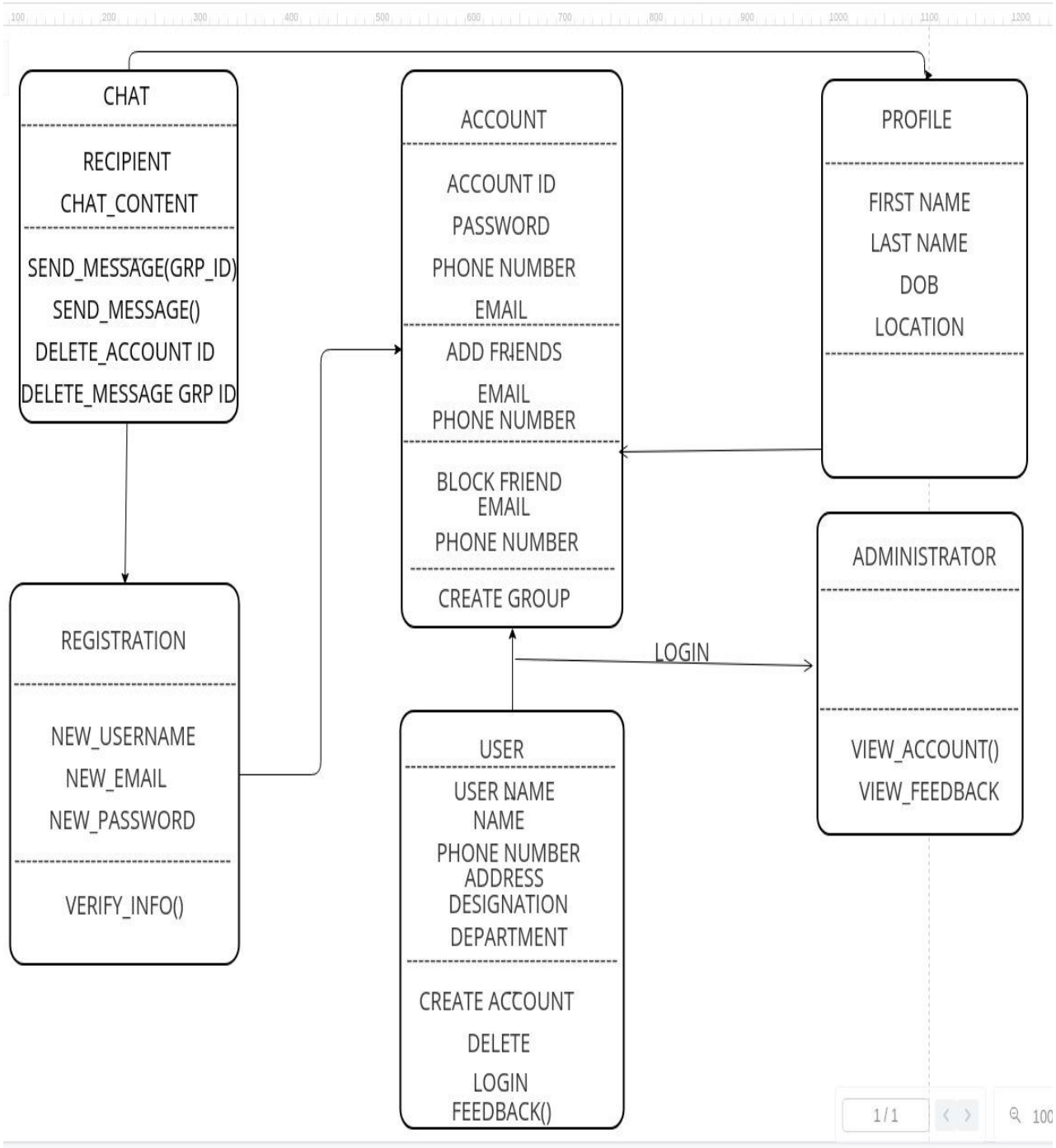
Use case diagram of the proposed system .

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 .

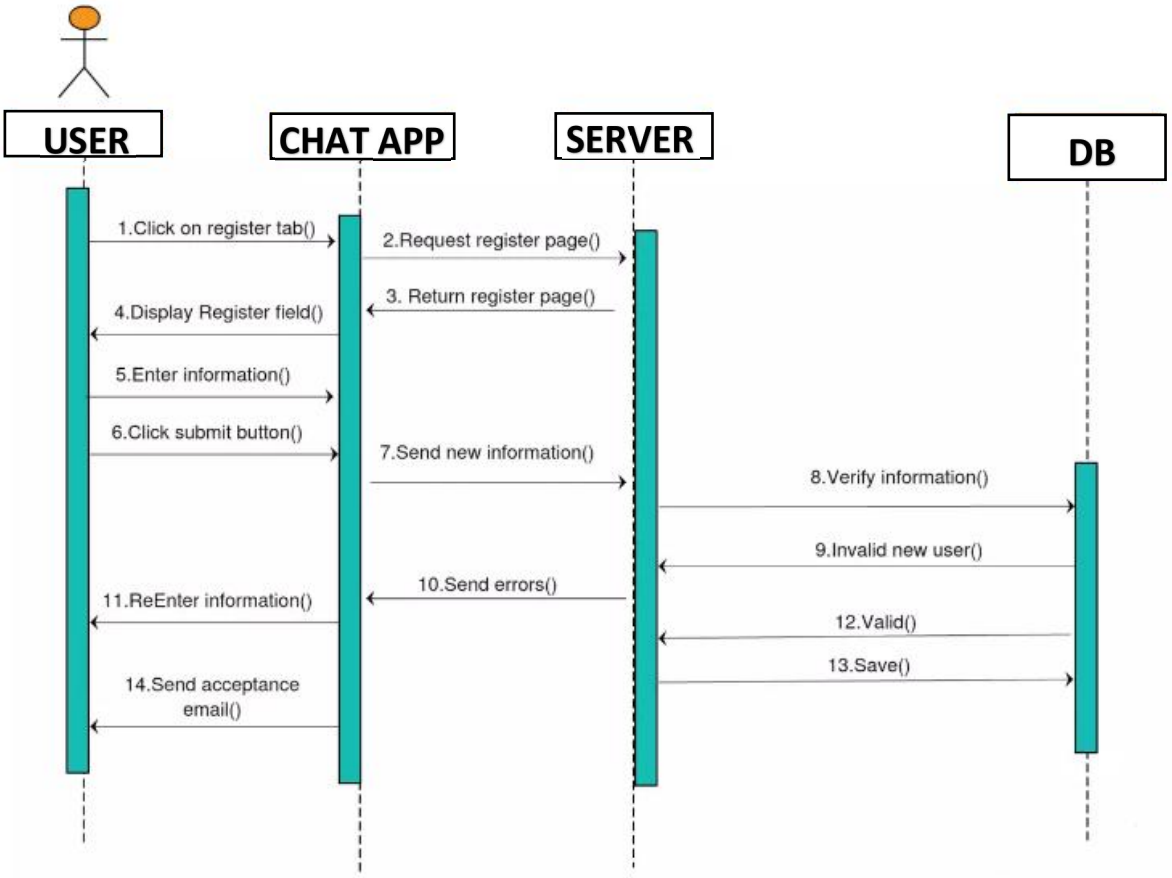
ACTIVITY DIAGRAM



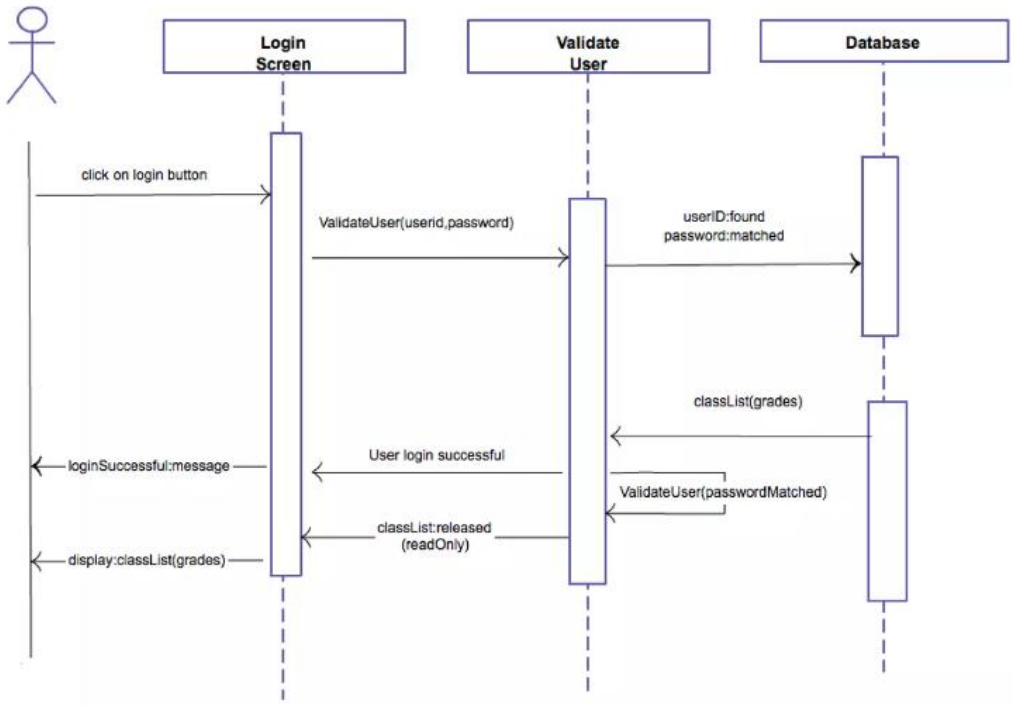
CLASS DIAGRAM



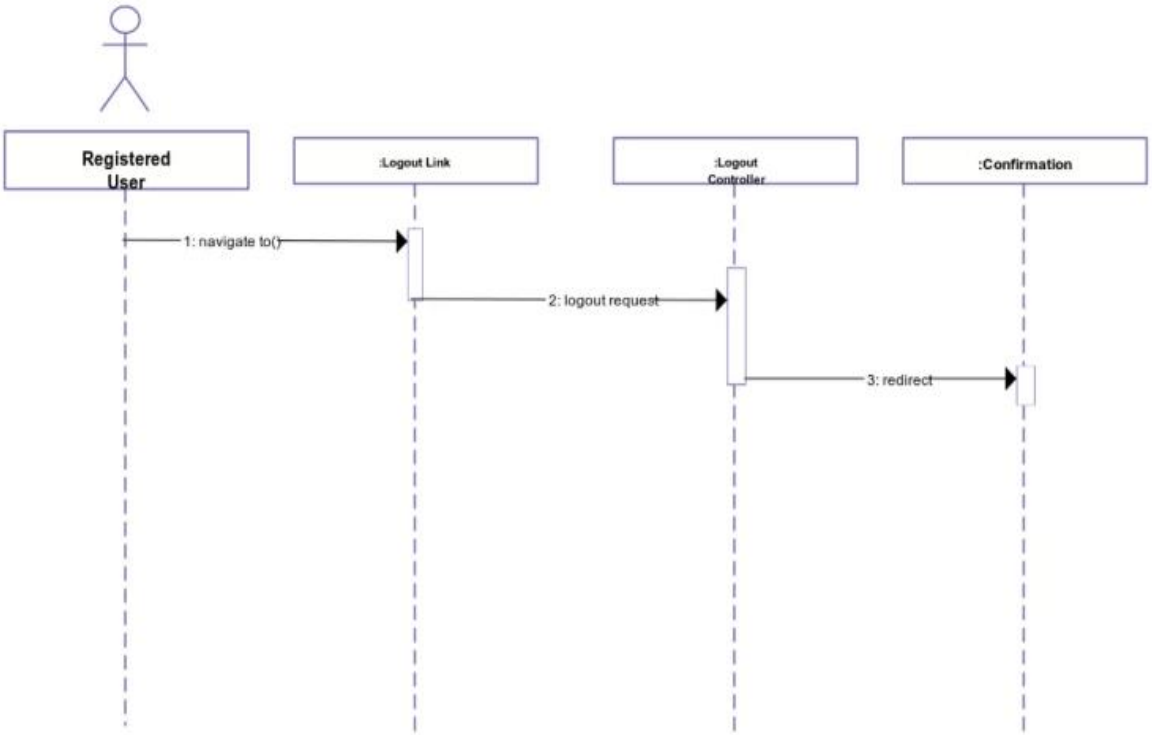
SEQUENCE DIAGRAM



SEQUENCE DIAGRAM FOR REGISTRATION FUNCTION

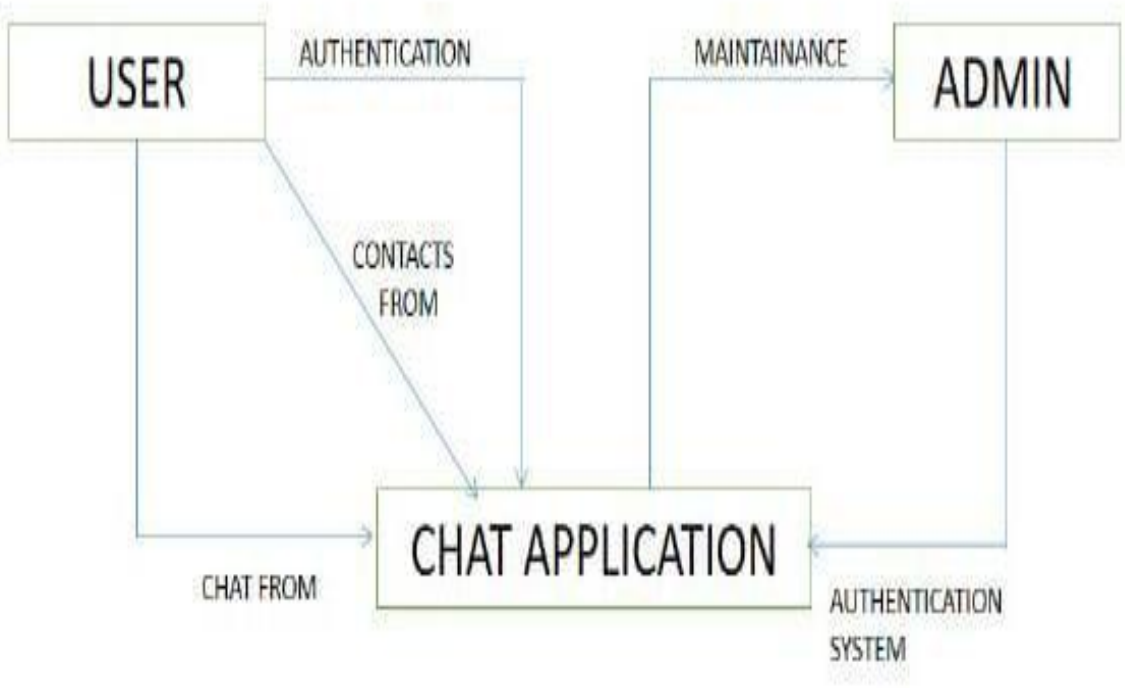


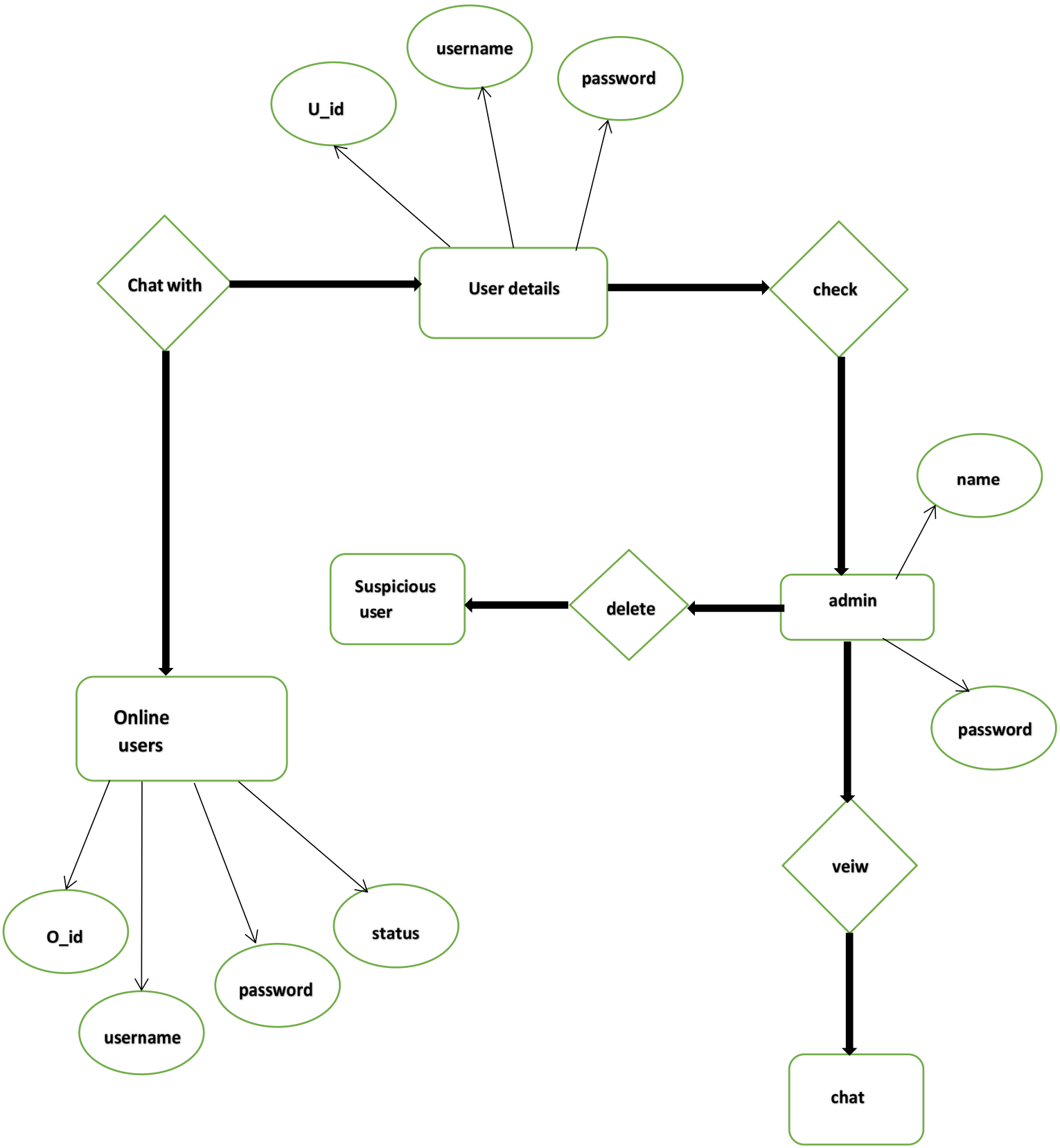
SEQUENCE DIAGRAM FOR LOGIN



SEQUENCE DIAGRAM FOR LOGOUT

DATA FLOW DIAGRAM





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(200)	NO	ADMIN USERNAME
PASSWORD	VARCHAR(200)	NO	PASSWORD SET BY ADMIN

I. Data Dictionary of admin

User:

FIELD NAME	DATA TYPE	NULLABLE	DESCRIPTION
USER ID	INTEGER(10)	NO	UNIQUE NO.
FROM NAME	VARCHAR(200)	NO	ADMIN USERNAME
TO NAME	VARCHAR(200)	NO	USER PASSWORD

II. Data Dictionary of user .

Online users:

FIELD NAME	DATA TYPE	NULLABLE	DESCRIPTION
USER ID	INTEGER	NO	UNIQUE NUMBER
FROM NAME	VARCHAR	NO	USER NAME FROM WHOM THE MESSAGE IS RECIVED
TO NAME	VARCHAR	NO	USER NAME FROM WHOM THE MESSAGE IS RECIVED USER NAME TO WHOM THE MESSAGE IS SENT

III. Data Dictionary of online users .

Modules used for development :-

The system is developed using:

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

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.

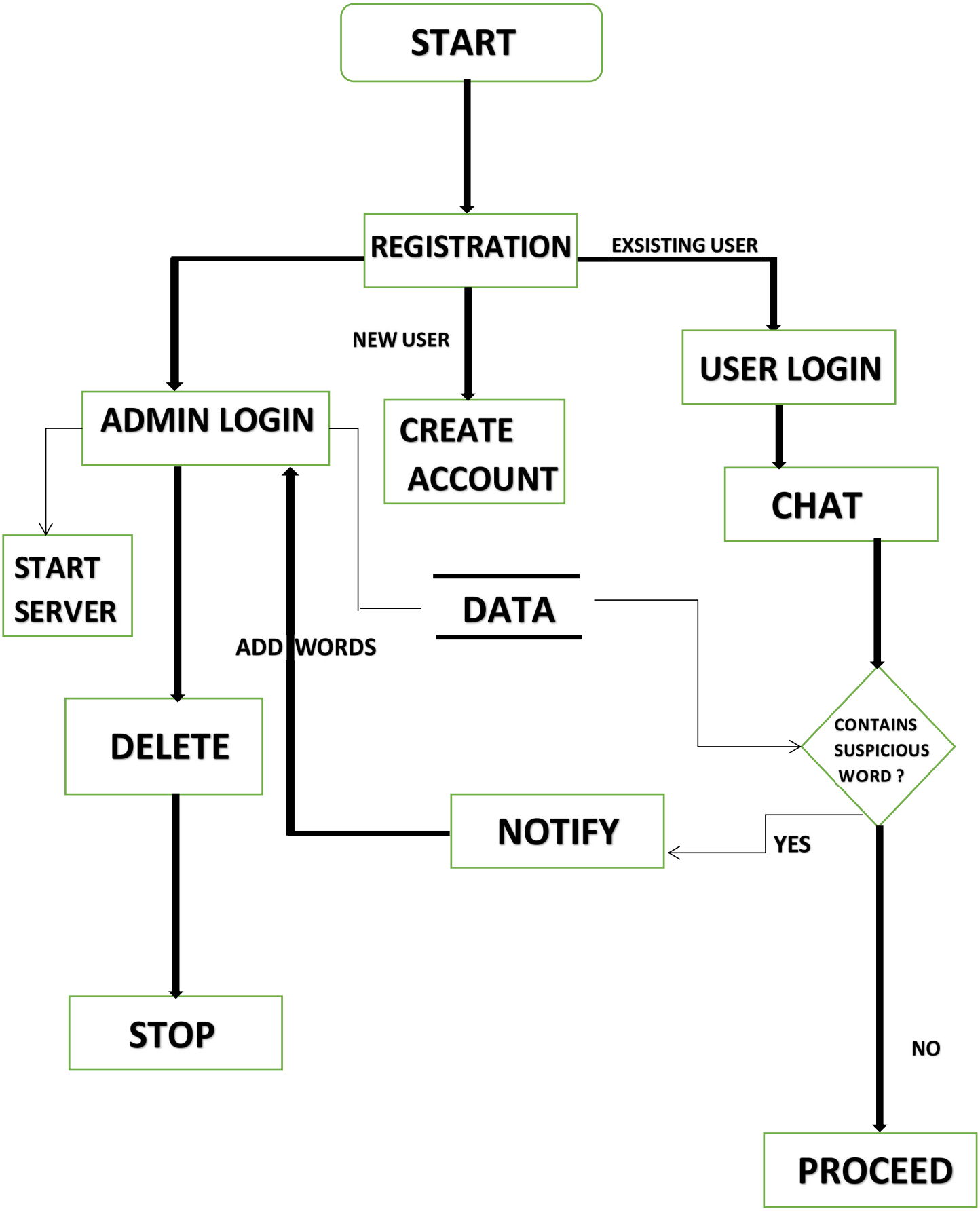
Delete: Delete is also set by the admin. It means the account will be deleted by the admin if found doing illegal activity. Once a user is deleted, he or she must again register themselves in order to join the chat system or discussion forum .

Functional requirement :-

- User
- Administrator
- Keywords
- Send message
- Message Status

Nonfunctional requirement :-

- Privacy
- Reliability
- Robustness
- Performance .



SYSTEM ARCHITECTURE FLOWCHART .

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

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 .

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.

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=6714167&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
5. M. Brindha1 , V. Vishnupriya2 , S. Rohini3 , M. Udhayamoorthi4 , K.S.Mohan5 , "Active Chat Monitoring and Suspicious Chat Detection over Internet", 1,2,3UG Scholars, Deparment of IT, SNS College of Technology, Coimbatore, Tamilnadu, India. 4,5Assistant 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".