Name	Div	Roll no
Kshitij Sonawane	TE-15	42
Sanket Singh	TE-15	41
Pramod Virkar	TE-15	45

Practical 3

Aim:- Preparation of software requirement specification (SRS) document in IEEE Format.

Lab Outcomes:- Identify requirements and apply software process models to selected case study.

Theory:-
A software requirements specification (SRS) is a document that describes what the software will do and how it will be expected to perform. It also describes the functionality the product needs to fulfill all stakeholders (business, users) needs.
An SRS gives you a complete picture of your entire project. It provides a single source of truth that every team involved in development will follow. It is your plan of action and keeps all your teams — from development to maintenance — on the same page

Software Requirements Specification

for

Active Chat Monitoring and Suspicious Chat Detection over Internet

Version 1.0 approved

Prepared by:

Kshitij Sonawane

Sanket Singh

Pramod Virkar

Shah and Anchor Kutchhi Engineering College

8/8/2022

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

To secure an online chatting platform from threat messages and cyber bullying. It will secure the youth from all kinds of illegal stuff while it is carried out over the internet. Terrorist activities communicate over application and chat programs over internet. It also uses these chat applications over the internet for getting their message to younger generation and making all of types terrorists. The chat monitor system is an important application that could allow for secure chats along with terrorism related chat detection that helps track down spread of terrorist networks and locate the activities using IP addresses.

1.2 Document Conventions

The font used for the whole document is Arial.

1.3 Intended Audience and Reading Suggestions

The document is intended for developers or cyber security developers who are working to give online security to common users. Cyber Security enthusiasts can also be encouraged to read the srs.

1.4 Product Scope

It is a web based application which uses Artificial Intelligence to detect any suspicious chat words. The purpose of this product is to gain the ip address of the suspicious chatting party and block them or maybe report them to cyber police if bigger scams are included.

1.5 References

https://nevonprojects.com

2.   Overall Description

2.1   Product Perspective

It is a self contained project. The concept for this project was developed by the idea that every scammer on the internet using it to do illegal tasks must be punished.

2.2   Product Functions

- *Track ip of both chatting parties.*
- *Fetch the chats performed by them and using AI detect if they are suspicious.*

2.3   User Classes and Characteristics

- ➔ *class get_ip*
  - ◆ *It fetches the ip of both chatting parties over the internet.*

- ➔ *class get_chats*
  - ◆ *It lets two people chat over the internet.*
  - ◆ *All the chats that are done between both parties are simultaneously recorded in this class.*

- ➔ *class check_suspicion*
  - ◆ *It uses AI technology to detect any suspicious one among the recorded chats.*

2.4   Operating Environment

It is a website which can be accessed using any latest web browser. It can be viewed on a smartphone, computer or other digital media which can run a web browser.

2.5   Design and Implementation Constraints

Accessing the precise ip address of a user is an offense which if the chatting party is knowledgeable enough can charge a case against us.

2.6   User Documentation

Terms and Condition links for the product are displayed on the website. User manuals as well as contact us options are also available on the front page.

2.7   Assumptions and Dependencies

The exact ip address of the scammer cannot be traced if he/she is using a vpn. Only the government agencies can trace the original ip address.

3.   External Interface Requirements

3.1   User Interfaces

The GUI offers an interface to the user to chat with any random person over the internet.

3.2   Hardware Interfaces

The chats are sent to servers which store them in hardware databases. These are good for storing large amounts of data. Data mining is performed on these databases for fetching the words matching the chats and computes the suspicion level of the chats.

3.3   Software Interfaces

This app makes use of the MySql database for storing suspicious words / sentences which are likely to be encountered at some point in the chatting process. These are fed directly by the developers or the system can dynamically detect these words / sentences using some algorithms included in the program. The linux based operating system is good for gaining ip related information as it provides better tools for doing the same.

3.4   Communications Interfaces

HTTPS protocol is used in the application for secure communication and transfer of data(in this case chats and ip addresses). IRC (Internet Relay Chat) protocol provides the base for the chatting interface. IP tools provided by linux are used for ip address tracking of both parties.

4.   System Features

4.1   Security

4.1.1   Description and Priority

Security is the highest priority feature of this product. Around 60-70% of the development cost id consumed by security.

4.1.2   Stimulus/Response Sequences

Different types of threat chats and illegal activities chats typed by the users stimulates this feature.

4.1.3   Functional Requirements

No functional requirements are needed on the user side, only an operating system that can run an updated version of any web browser.

5.   Other Nonfunctional Requirements

5.1   Performance Requirements

The website should load within 5 seconds. It should be compatible with all the web browsers. Message delivery should be efficient.

5.2   Safety Requirements

As this website is only capable of detecting suspicious chats, any mental damage done to the other person who is a victim may not be avoided. It is suggested to use vpn for chatting.

5.3   Security Requirements

Chatting parties should not feel that they are being monitored. Use of legal software must be done for development of this application in order to avoid data breaches.

5.4   Software Quality Attributes

It should have an user-friendly interface. Must correctly handle data transfer in case of network failure. It must introduce new features / updates frequently to keep up with the latest security standards.

5.5   Business Rules

The website must be free of cost. Users can report any malicious chatting party. It must be advertised as a normal online chatting application.

6.   Other Requirements

There are no other specific requirements that are not mentioned in the SRS

Appendix A: Glossary

- ***Suspicious***: *having or showing a cautious distrust of someone or something.*
- ***ip address:*** *a unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.*
- ***Data Mining:*** *Data mining is the process of sorting through large data sets to identify patterns and relationships that can help solve business problems through data analysis.*
- ***Chatting party:*** *A user involved in a chatting process.*
- ***Database:*** *A database is an organized collection of structured information, or data, typically stored electronically in a computer system.*

Appendix B: Analysis Models
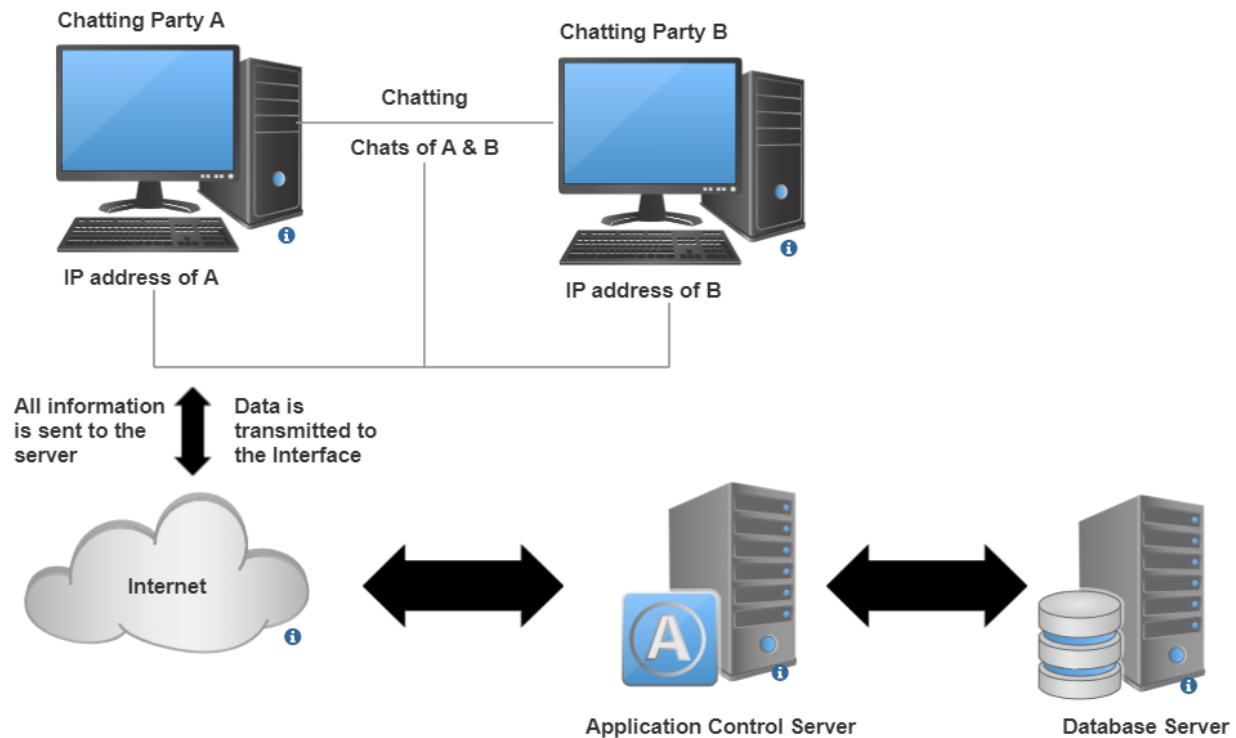
Appendix C: To Be Determined List

https://nevonprojects.com

https://www.researchgate.net/publication/330686371_Active_Chat_Monitoring_and_Suspicious_Detection_over_Internet