WhatsApp with Suspicious Chat Monitoring

Akangsha Salave[1], Rushikesh Borale[2], Tushar Mahale[3], Darshan Nemnor[4], Prof. S. C. Kadam[5].
1,2,3,4 Students of department of Computer Engineering Sandip Polytechnic, Mahiravani, Nashik &
5 Senior Lecturer in department of Computer Engineering Sandip Polytechnic, Mahiravani,

Abstract— **With the expanding utilization of Instant Chat Messengers to share data, dubious exercises have additionally expanded. There are numerous sources to share the data however moment talk couriers and informal communication sites are the fast also, simple intends to share anything. In some cases, even new stories are at first separated via online media locales and further on talk couriers rather than any news channel and paper and so forth Because of these innovation progressions, a few individuals are abusing these moments talk couriers to share dubious exercises and make arrangements to accomplish something dubious. This sort of visit is for the most part accessible in literary design. With the headway of web innovation and the change in the method of correspondence, it is discovered that much direct news has been examined in Internet discussions well before they are accounted for in conventional broad communications. Additionally, this correspondence channel gives a viable channel to criminal operations, for example, communicating of copyrighted films, compromising messages and internet betting and so on Our Proposed Framework will examine online plain content sources from chose conversation gatherings and will arrange the content into various gatherings and framework will choose which post is legitimate and unlawful.**

Keywords— **Suspicious Chat, Chat Monitoring, Abused word, Terrorist chat, Porn Text**

INTRODUCTION

Correspondence gives compelling regions to criminal operations for example, compromising messages. In this task we had utilized information mining calculation to identify law and crimes. ACM Framework will download postings from chose conversation information mining procedures to distinguish most recent subject's creators into various associations utilizing word-based client made profiles. This framework we have delivered called as Active Chat Checking and Suspicious Chat Detection over Internet which will handle with this issues. Web innovation had been expanding more. Our law searching for answers for identify these conversation gatherings for all conceivable crimes and download suspected Postings as proof for examination.

SCM System which will handle with this issue. we have utilized an information mining calculation to identify crimes, legitimate and illicit postings. In this framework will utilize text information mining procedure. SCM System will let us help to examine online plain content sources from chosen conversation discussions and will arrange the content into gatherings and framework will choose which post is lawful and unlawful as needs be to their focuses. It will help us to decrease and limit numerous crimes which are held on social-site, for example, Facebook, Twitter, Tinder, and so on.

PROJECT CONCEPT

We propose a chat application system that monitors the various chats going on and detect the suspicious chats too. The application 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 proposed System will analyse online plain text sources from selected discussion forums and will classify the text into different groups and system will decide which post is legal and illegal. This system will ensure that the admin may not watch all the chat at a time, so in order to stop chatting illegally, the keywords are set by the admin as suspicious words which will be blocked or it cannot be able to view by the other person.

1. The system to be developed here is a chat facility.
2. It is a client-server system with centralized database server.
3. There are two way communications between the client and the server.
4. This chat application can be used for group discussion.

It also monitors the suspicious text chat by admin.

PROJECT DESIGN

This chapter gives a detailed outline of the software development methodology used in this project following up the various existing software development methodology. The strength and weaknesses of the chosen methodology have been outlined. Further, the functional and non-functional requirements of the system are explained in detail and the use cases which are a list of steps, typically defining interactions between a role and system, to achieve a goal. Class diagrams have been given to show detailed data modelling of the system which will be translated into code.

- It allows for development of high-risk or major functions first
- Each release delivers an operational product
- Customer can respond to each build
- Uses “divide and conquer” breakdown of tasks
- Lowers initial delivery cost
- Initial product delivery is faster
- Customers get important functionality early
- Risk of changing requirements is reduced

SYSTEM ARCHITECTURE

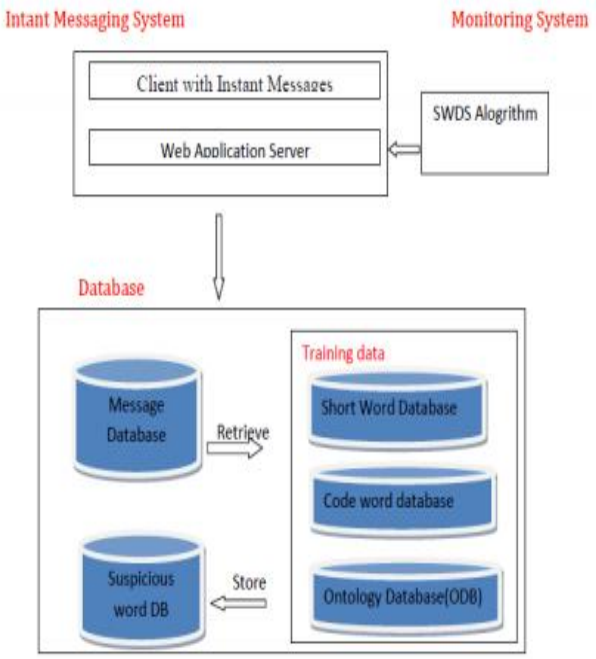

Fig No 1: Basic Architecture of the system

PARALLEL DEVELOPMENT APPROCH

This model of methodology attempts to address the problem of long delay between analysis phase and the delivery of the system. Instead of doing design and implementation in sequence, it performs a general design for the whole system and then divides the project into a series of distinct subprojects that can be designed and implemented in parallel. Once all subprojects are complete,

there is a final integration of the separate pieces, and the system is delivered. Here we had used the same technique for development. For this we had divided our main project into two sub projects or we can say in modules. First subproject is to create a chat application and second one is the detection of the suspicious words present in the messages.

DEVELOPMENT TOOLS

I. Android Studio

Android Studio is the official integrated development environment (IDE) for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. It is available for download on Windows, macOS and Linux based operating systems. It is a replacement for the Eclipse Android Development Tools (ADT) as the primary IDE for native Android application development.

Android Studio supports all the same programming languages of IntelliJ (and Clion) e.g. Java, C++, and more with extensions, such as Go and Android Studio 3.0 or later supports Kotlin and all Java 7 language features and a subset of Java 8 language features that vary by platform version. External projects backport some Java 9 features. While IntelliJ that Android Studio is built on supports all released Java versions, and Java 12, it's not clear to what level Android Studio supports Java versions up to Java 12 (the documentation mentions partial Java 8 support). At least some new language features up to Java 12 are usable in Android.

II. MYSQL

MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses. MySQL was owned and sponsored by the Swedish company MySQL AB, which was bought by Sun Microsystems (now Oracle Corporation). In 2010, when Oracle acquired Sun, Widenius forked the open-source MySQL project to create MariaDB. MySQL is a component of the LAMP web application software stack (and others), which is an acronym for Linux, Apache, MySQL, Perl/PHP/Python. MySQL is used by many database-driven web applications, including Drupal, Joomla, phpBB, and WordPress. MySQL is also used by many popular websites, including Facebook, Flickr, MediaWiki, Twitter, and YouTube.

MySQL is offered under two different editions: the open source MySQL Community Server and the proprietary Enterprise Server. MySQL Enterprise Server is differentiated by a series of proprietary extensions which install as server plugins, but otherwise shares the version numbering system and is built from the same code base.

SYSTEM WORKFLOW

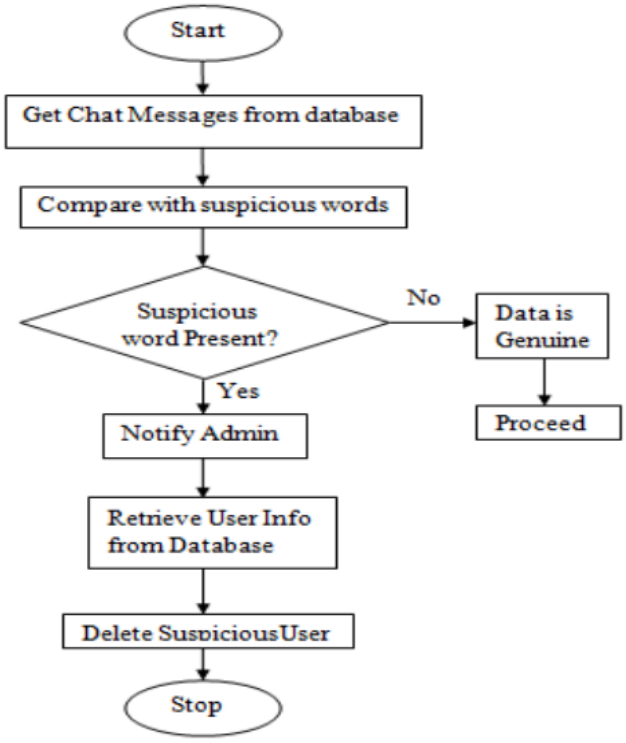

Fig No 2: Workflow of the system

DATA FLOW DIAGRAM

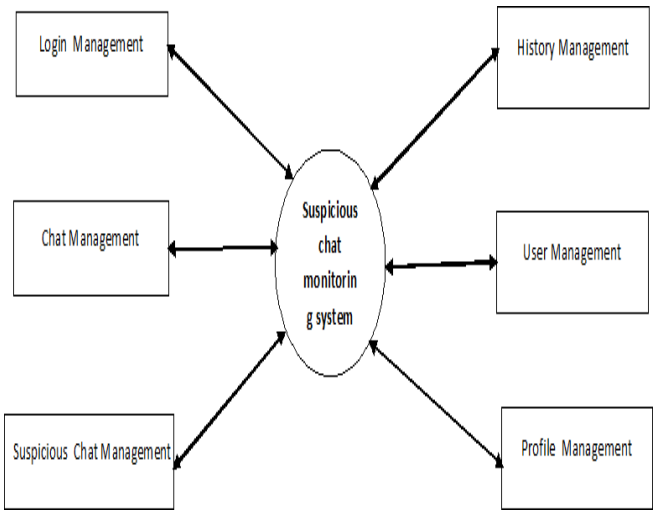

Fig No 3: Data Flow Diagram

APPLICATIONS

1. This system can be used by government officials to check any suspicious activities that are going on the website
2. This system can also be used as an extension on popular sites such as Facebook, twitter etc.
3. Third parties such as Detective can also this type of system legally.
4. The system used to track the IP address of both the chatting parties

ADVANTAGES

1. This system will reduce illegal activities held on internet.
2. This system will provide security for many messengers.
3. This system will act as an evidence for investigation

LIMITATIONS/CONSTRAINTS

1. Requires Internet connection.
2. Requires Android Smart Phone.

CONCLUSION

By this work, Active chat monitoring and suspicious chat detection over internet we conclude that using a chat for inappropriate conversation provide a secure access over internet without any further monitoring process. This could be further developed into two user communication with the help of server control. Overall process of Active chat monitoring and suspicious chat detection over internet is done the process helps the people. This can be assured from the above analysis and works. If the given future enhancements are implemented in a correct manner, then it can be extending the success of this project in the future. The Project titled Active chat monitoring and suspicious chat detection over internet is tested with sample data and found to be working well. The system has been developed for the users/people. The database approach of developing the system has helped in reducing redundancy of data and improving the consistency of data in the system. This system is flexible, user friendly. The system satisfies the client requirements specified.

REFERENCES

[1] Rob Kavet and Gabor Kenzo, “A Perspective on Chat Associated with Suspecious Chat Technology”, published by IEEE in 2010.

[2] David W. Cheung, and et al., “Maintenance of discovered association rules in largedatabases: an incremental updating technique,” published by IEEE in 1996.

[3] Michael Robertson, Yin Pan, and Bo Yuan, “A Social Approach to Security: Using Social Networks to help detect malicious web content,” published by IEEE in 2010

[4] Harsh Arora and Govind Murari Upadhyay,” A Framework for the Detection of Suspicious Discussion on Online Forums using Integrated approach of Support Vector Machine and Particle Swarm Optimization”, published by IJARCS in 2015.

[5] Alami, Salim, and Omar EL Beqqali. "Detecting Suspicious Profiles Using Text Analysis Within Social Media.," published by JATIT in 2015.

[6] http://www.public.iastate.edu/~CYBERSTACKS/Live

[7] http://www.aserl.org/projects/vref/default.htm

[8] https://www.researchgate.net/publication/330686371