WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Chat Analysis and Spam Detection of Whatsapp chats using Machine Learning

Prachi Bhosale[1], Rutuja Muthal[2], Yogesh Giram[3], Prof. Kishor B Sadafale[4]

Government College of Engineering and Research Avasari, Pune

A B S T R A C T

This web application provides an in-depth examination of WhatsApp group chats, covering a wide range of discussion topics among users. Its key features include identifying and filtering spam messages, presenting message analytics such as total counts and monthly trends using graphical representations, and highlighting common words and active participants. Leveraging Python libraries such as Pandas, Streamline, Seaborn, and Word Cloud, along with resource-efficient machine learning algorithms, this tool effectively handles extensive datasets. Its ability to detect and address spam messages enhances the overall quality of conversations by ensuring relevance and meaningful engagement.

Keywords: WhatsApp, Chat analysis, Group conversations, Spam detection, Data visualization, Python modules, Pandas, Streamline, Seaborn, Word Cloud, Machine Learning Algorithms(SVM), Data frames, Graph generation.

1. INTRODUCTION

WhatsApp has become a ubiquitous platform for communication, offering users worldwide the convenience of text, voice, and video interactions across various devices. With its widespread adoption, the need for understanding and analyzing conversations on this platform has grown significantly. However, sifting through large volumes of chat data manually poses challenges, prompting the development of tools like the WhatsApp Chat Analyzer. This research paper explores the functionalities and significance of such tools in providing insights into WhatsApp conversations, including message distribution, participant activity, and spam detection. Leveraging Python modules and data analysis techniques, this study aims to showcase the utility of automated analysis in deciphering the dynamics of WhatsApp communication, thereby addressing the demands of modern digital interaction.

1.1 PROBLEM STATEMENT

WhatsApp-Analyzer is a statistical analysis tool for WhatsApp chats. Working on the chat files that can be exported from WhatsApp, it generates various statistical analysis, total number of messages, analysis about link shared and which other participant a user responds to the most. In addition to chat analysis, there's a growing need for spam detection within WhatsApp conversations. We propose to employ dataset manipulation techniques not only to better understand WhatsApp chats present in our phones but also to detect and filter out spam messages effectively.

1.2 EXISTING SYSTEM

Upon examining the existing systems, it became apparent that there was an opportunity to enhance the analysis capabilities by integrating spam detection into WhatsApp conversations. This integration not only aimed to identify and mitigate the impact of unwanted messages that disrupt the natural flow of discussion but also to ensure a more seamless user experience within the chat environment. By incorporating robust spam detection algorithms, the tool would be able to discern patterns indicative of spam behavior, such as repetitive or unsolicited messages, suspicious links, or excessive use of certain keywords. Moreover, the inclusion of spam detection mechanisms would serve to safeguard the integrity of group conversations by minimizing the intrusion of irrelevant or potentially harmful content. This proactive approach to spam detection would empower users to engage more meaningfully within their chat groups while mitigating the risk of misinformation or malicious activities. In summary, the integration of spam detection capabilities within the WhatsApp-Analyzer tool not only enhances its analytical prowess but also reinforces the quality and authenticity of interactions within WhatsApp conversations, thereby fostering a more positive and productive communication environment for all participants.

2. LITERATURE SURVEY

I. Title: WhatsApp Chat Analysis

Year: 2022

Authors: Meesala Nirmala, Modugaparapu Sravani

Description: Provides general statistics of chat within the WhatsApp app.

II. Title: International Research Journal of Modernization in Engineering Technology and Science

Year: 2022

Authors: Marada Pallavi, Dr. K. Soumya, Meesala Nirmala

Description: Conducted a survey on WhatsApp usage patterns in the southern part of India, focusing on age group 18 to 23. Explores positive and negative impacts of WhatsApp usage.

III. Title: JURNAL TEKNOLOGI DAN OPEN SOURCE

Year: 2021

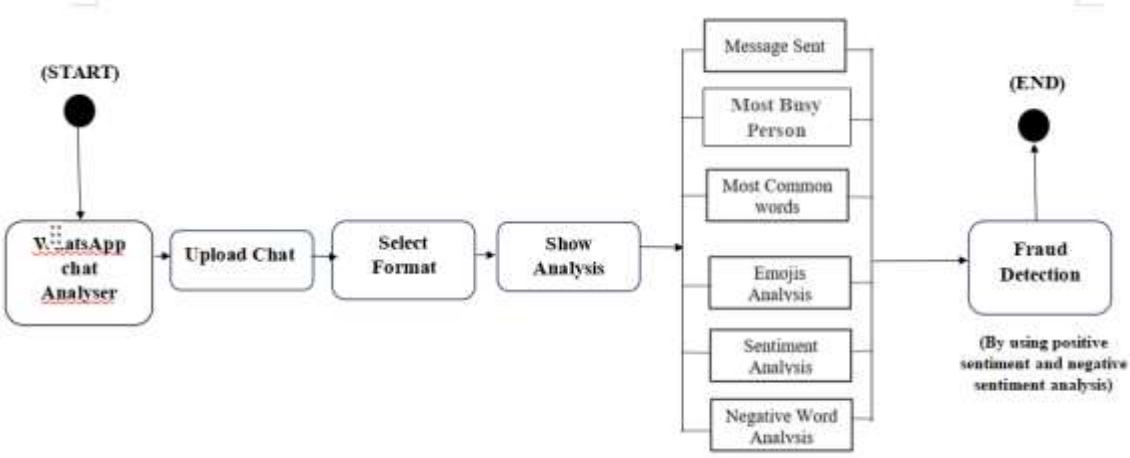
Authors: Fathur Rahman

Description: Investigates the detection of fraudulent words in WhatsApp chats. Utilizes the Support Vector Machine (SVM) algorithm for fraud chat analysis, achieving an accuracy rate of 84.21%.

PROPOSED SYSTEM

The proposed system is a web application powered by machine learning algorithms and other techniques, designed to analyze WhatsApp chats efficiently. Utilizing the Pandas library, it performs data analytics by ingesting chat data in the form of Pandas DataFrames, enabling various analytical functions and visualizations. Capable of analyzing both individual and group chats, the system provides insights such as total message counts, monthly timeline graphs, frequently used words, and active participants. Furthermore, it incorporates spam message detection, showcasing the total number of spam messages within chats. Implemented using lightweight Python modules like Pandas, Streamline, Seaborn, and WordCloud, the system ensures efficiency and minimal resource consumption. Its scalability makes it ideal for handling large datasets from diverse chat sources. Our innovative web application showcases WhatsApp chat statistics, encompassing total messages, media files, links, and images exchanged among users. It also features graphical representations of user activities on a weekly or monthly basis, along with monthly timelines. Additionally, the system efficiently identifies spam messages by sender and provides their total count.

PROPOSED SYSTEM ARCHITECTURE



4. SYSTEM IMPLEMENTATION

1) Programming Language – Python is chosen for its versatility and extensive libraries. Version 3.12 provides access to the latest features and optimizations, ensuring efficient development.

2) Machine Learning Framework –

Support Vector Machine (SVM): SVM is implemented for classification tasks, such as identifying the busiest users or detecting suspicious activity within the chat data. SVM's ability to find optimal hyperplanes makes it suitable for separating data points effectively.

3) Data Preprocessing Libraries:

Pandas: Used for data manipulation and cleaning, facilitating efficient preprocessing of WhatsApp chat data.

NumPy: Provides support for numerical and mathematical operations, enhancing data manipulation capabilities.

URLExtract: Enables extraction of URLs from text data, aiding in parsing and retrieving embedded URLs within chat logs.

WordCloud: Generates visualizations of frequently occurring words, allowing quick identification of prominent terms within the chat.

Collections: Utilized for generating frequency distributions, aiding in the analysis of word occurrences.

Re (regular expressions): Supports pattern matching and text manipulation, enabling advanced preprocessing tasks.

4) Integrated Development Environments (IDEs):

Jupyter Notebook, PyCharm, and Visual Studio Code: These IDEs are utilized for coding, testing, and debugging, providing interactive environments for development tasks.

5) User Interface -

Streamlit: Streamlit is employed to create a user-friendly web application for data analysis. Its simplicity and ease of use allow for the rapid development of interactive interfaces without requiring expertise in front-end development.

Comparison with other algorithms

Algorithm	Accuracy
K-Nearest Neighbour	**72%**
SVM	**85%**

5. EQUATIONS

Given dataset D = {(x1, y1),(x2, y2), …., (xn, yn)}, where xi represents the features extracted from WhatsApp chat messages and yi is the corresponding class label (1 for spam, -1 for legitimate), the objective of the SVM is to find a hyperplane that best separates the spam and legitimate messages.

The decision function for the SVM is defined as,

$$f(x)=w \cdot x+b$$

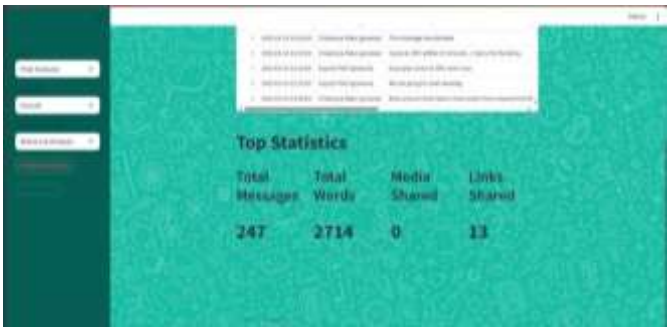
- w is the weight vector.
- x is the feature vector extracted from a WhatsApp chat message.
- b is the bias term.

The goal is to find the optimal w and b that maximizes the margin between the hyperplane and the nearest data points from both classes while minimizing classification errors. This can be formulated as the following optimization problem,

$$\text{minimize } \frac{1}{2}||\mathbf{w}||^2 + C\sum_{i=1}^{n}\xi_i$$
$$\text{subject to } y_i(\mathbf{w}\cdot\mathbf{x}_i + b) \geq 1 - \xi_i \text{ for } i = 1, 2, ..., n$$
$$\xi_i \geq 0 \text{ for } i = 1, 2, ..., n$$

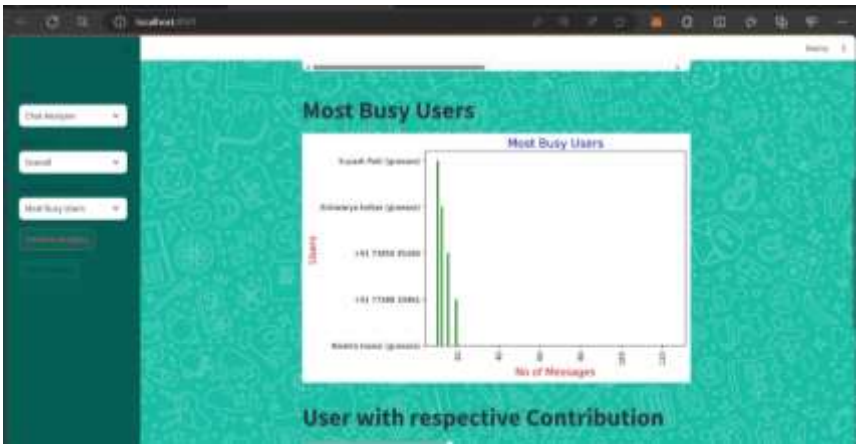
RESULTS AND ANALYSIS

6.1 Top Statistics -



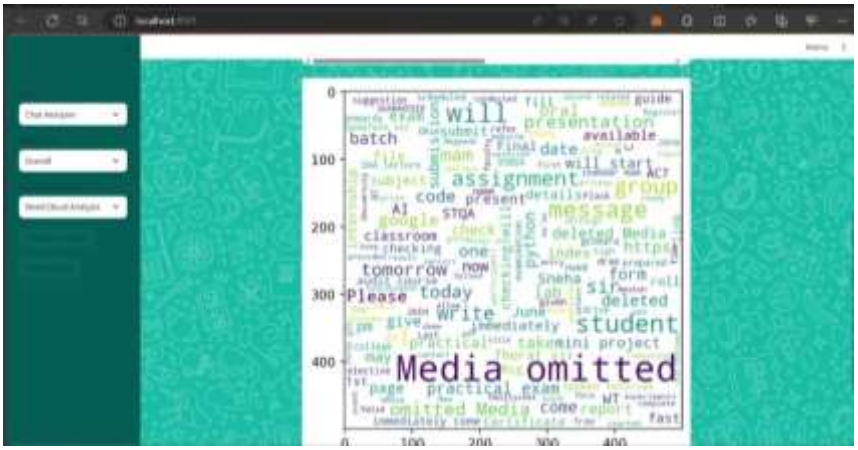
6.2 Users Contribution in chats -

6.3 Most Busy User -



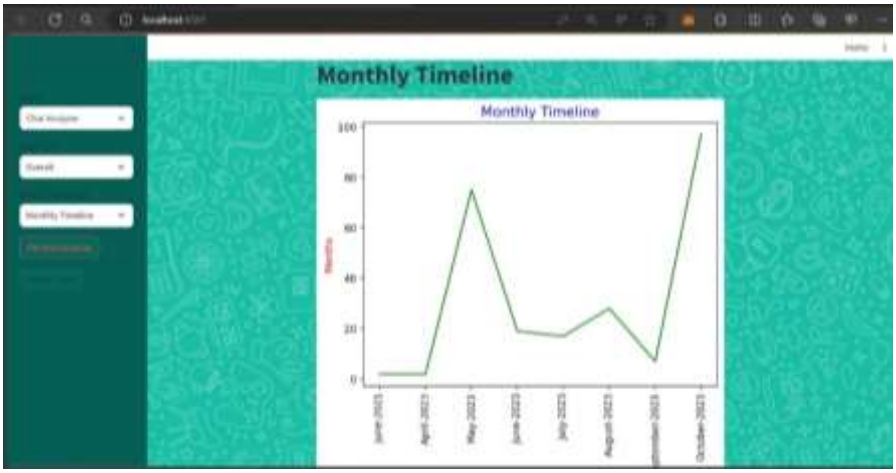
6.4 Most Common Words -

6.5 Word Cloud -

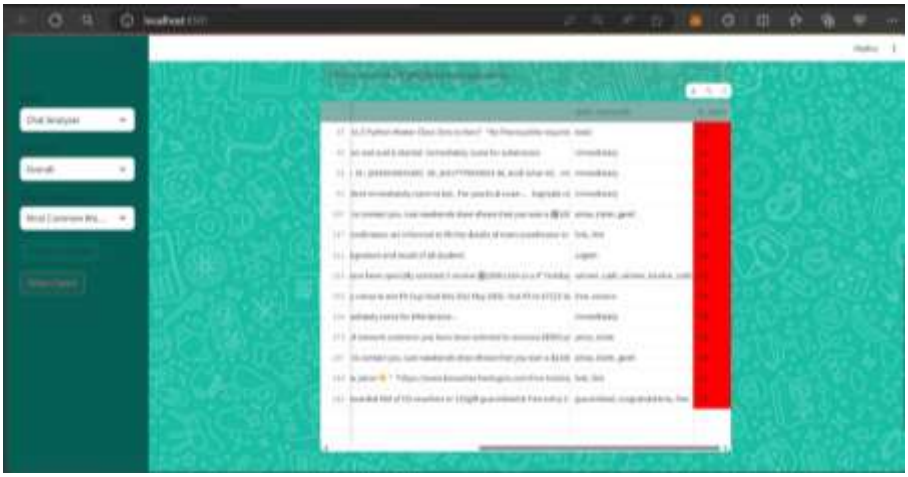


6.6 Weekly Activity Heatmap -

6.7 Monthly Timeline -



6.8 Spam Detection -



7. CONCLUSION

Our project on WhatsApp chat analysis and spam detection has provided valuable insights into user behavior and communication patterns within WhatsApp groups. Through our analysis, we identified significant trends in WhatsApp usage and developed an effective system for spam detection using the Support Vector Machine (SVM) algorithm. The findings highlight the importance of data preprocessing and feature engineering in optimizing machine learning models for chat analysis. Our system demonstrates promising results in accurately classifying messages and detecting spam, contributing to the enhancement of communication experiences for WhatsApp users.

REFERENCES

[1] M. Pallavi, M. Nirmala, M. Sravani, M. Shameem, and K. Soumya, "WhatsApp Chat Analysis," *Int. Res. J. Modern. Eng. Technol. Sci.*, vol. 4, no. 5, pp. 1-5, May 2022.

[2] R. K, D. Vaisakh, and S. I S, "WhatsApp Chat Analyzer," *Int. J. Eng. Res. Technol.*, vol. 9, no. 5, pp. 1-5, May 2020.

[3] F. Rahman et al., "WhatsApp Chat Fraud Analysis Using Support Vector Machine Method," *J. Teknol. Open Source*, vol. 4, no. 2, pp. 174-179, Dec. 2021.

[4] S. Suhardjono et al., "Forensic Analysis Video Metadata Authenticity Detection," *J. Innov. Res. Knowl.*, vol. 1, no. 12, pp. 1727-1734, 2022.

[5] D. Radha et al., "Analysis on Social Media Addiction using Data Mining Technique," *Int. J. Comput. Appl.*, vol. 139, no. 7, pp. 23-26, Apr. 2016.

[6] A. M. Puspitasari, D. E. Ratnawati, and A. W. Widodo, "Klasifikasi Penyakit Gigi Dan Mulut Menggunakan Metode Support Vector Machine," *J-Ptiik*, vol. 2, no. 2, pp. 802–810, 2018.

[7] W. A. Luqyana, I. Cholissodin, and R. S. Perdana, "Analisis Sentiment Cyberbullying Pada Komentar Instagram dengan Metode Klasifikasi Support Vector Machine," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 11, pp. 4704–4713, 2018.