SPAMMER DETECTION AND FAKE USER IDENTIFICATION ON SOCIAL NETWORKS

Mucharla Vamshidhar reddy[1], Chouhan Bheem Singh[2], Devender Donadula[3], K. Ranjith Reddy [4]

1, 2 ,3 .B.Tech Student, Dept. Of CSE, CMR Technical Campus, Medchal,Hyderabad.

4. Assistant Professor, Dept. Of CSE, CMR Technical Campus,Medchal,Hyderabad.

[1]vamshidharreddy0303@gmail.com

[2]bheemchouhan944@gmail.com

[3]donadulakittu@gmail.com

[4]ranjithreddy.cse@cmrtc.ac.in

ABSTRACT

Social networking sites engage millions of users around the world. The users' interactions with these social sites, such as Twitter and Facebook have a tremendous impact and occasionally undesirable repercussions for daily life. The prominent social networking sites have turned into a target platform for the spammers to disperse huge amount of irrelevant and deleterious information. Twitter, for example, has become one of the most extravagantly used platforms of all times and therefore allows an unreasonable amount of spam. Fake users send undesired tweets to users to promote services or websites that not only affect legitimate users but also disrupt resource consumption.

Moreover, the possibility of expanding invalid information to users through fake identities has increased that results in the unrolling of harmful content. Recently, the detection of spammers and identification of fake users on Twitter has become a common area of research in contemporary online social Networks (OSNs).

In this project, we perform a review of techniques used for detecting spammers on Twitter. Moreover, a taxonomy of the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented techniques are also compared based on various features, such as user features, content features, graph features, structure features, and time features. We are hopeful that the presented study will be a useful resource for researchers to find the highlights of recent developments in Twitter spam detection on a single platform.

INTRODUCTION

Social media platforms such as Twitter have transformed the way people interact, share information, and consume news. With over 330 million active users, Twitter has become an important source of information for individuals, organizations, and governments around the world. However, the widespread use of social media has also led to an increase in spam and fake accounts, which can be used to spread false information or manipulate public opinion. Spammers and fake users on social media platforms like Twitter can be used to promote fraudulent schemes, propagate malicious links, conduct phishing attacks, and create bot armies. They can also be used to artificially inflate engagement metrics such as likes, shares, and retweets, which can distort the perception of public opinion.

Detecting spammers and fake users on social media platforms is a challenging task. Spammers and fake users often use sophisticated techniques to evade detection, such as creating realistic-looking profiles, using machine-generated content, and leveraging social engineering tactics to lure

unsuspecting victims. Traditional methods of detecting spam and fake users rely on manual inspection, rule-based heuristics, and clustering techniques, which are often timeconsuming and ineffective.

In recent years, machine learning algorithms and natural language processing techniques have shown promising results in detecting spam and fake users on social media platforms. These approaches leverage patterns and features in user behavior and profile information to identify spammers and fake users accurately. Here we propose a methodology for detecting spammers and fake users on Twitter using machine learning algorithms and natural language processing techniques. We aim to evaluate the effectiveness of our approach on a large dataset of Twitter accounts and demonstrate that our methodology can achieve high accuracy in detecting spammers and fake users.

LITERATURE SURVEY

As the problem of spam and fake users on social media platforms has become increasingly prevalent in India, several studies have been conducted to detect and prevent spamming and fake user activities on social media platforms, including Twitter. In this literature survey, we review some of the relevant research studies conducted in India.

"An Overview of Spam Detection Techniques in Social Media" by Shivangi Rastogi and Abhishek Srivastava: This study provides an overview of various spam detection techniques in social media, including content-based, user-based, network-based, and hybrid approaches. The authors review the strengths and limitations of each approach and highlight the need for developing more effective and efficient spam detection techniques.

"Identifying Fake Accounts in Twitter: A Machine Learning Approach" by V. Mohan and S. Arumugam: This study proposes a machine learning-based approach to detect fake accounts on Twitter. The authors use a combination of network-based and content-based features to classify Twitter accounts into fake and genuine categories. The results show that their approach achieves high accuracy in identifying fake accounts on Twitter.

"A Study on Spammers and Their Strategies in Twitter" by S. Pandey and R. Kumar: This study analyzes the behavior and strategies of spammers on Twitter. The authors use a dataset of spam tweets collected from Twitter and analyze the spammer's activity patterns, posting frequency, and content types. The study provides insights into the strategies used by spammers and highlights the need for developing more effective countermeasures.

"Anomaly Detection in Twitter: A Comparative Study" by S. Ravi and S. T. Bhatia: This study compares the effectiveness of several anomaly detection techniques in detecting spammers on Twitter. The authors evaluate the performance of various techniques, including the local outlier factor, the one-class support vector machine, and the isolation forest algorithm. The results show that the isolation forest algorithm performs the best in detecting spamming activity on Twitter.

"Fake Account Detection in Social Media: A Review" by N. J. Pillai and N. K. Sajeev: This study provides a comprehensive review of various techniques and approaches for detecting fake accounts in social media, including Twitter. The authors review the strengths and limitations of each approach and highlight the need for developing more robust and scalable fake account detection techniques.

In summary, the above studies demonstrate the importance of detecting spammers and fake users on social media platforms like Twitter and highlight the need for developing more effective and efficient spam detection techniques. These studies provide valuable insights into the behavior and strategies of spammers and fake users on social media and provide a basis for developing more effective countermeasures.

PROPOSED SYSTEM

The proposed system aims to address the growing concern of spam and fake users on Twitter. The system will utilize a Twitter dataset and four different techniques namely Fake Content, Spam URL Detection, Spam Trending Topic, and Fake User Identification, to identify whether a tweet is normal or spam, and whether a user account is fake or genuine. Each of these techniques will be implemented using a specific Random Forest classifier, which will classify the tweets and user accounts into either spam or non-spam, and fake or non-fake.

The system will use the Naive Bayes algorithm in classifying the tweets and user accounts. This algorithm is effective in identifying the characteristics of the data and classifying it accordingly. The Random Forest algorithm will then be used to classify the tweets and user accounts into different categories based on their features, such as user features, content features. The output of the system will be in the form of a graph, which will show the number of spam and non-spam tweets, and fake and non-fake user accounts.

The proposed system will offer a number of advantages over existing systems. It will be faster, more accurate, and require less human effort than manual detection methods. It will also be able to handle large datasets, which would be impractical to manage manually. The system will provide a high level of accuracy in detecting spam tweets and fake user accounts, thus enhancing the security and reliability of Twitter as a social network platform.

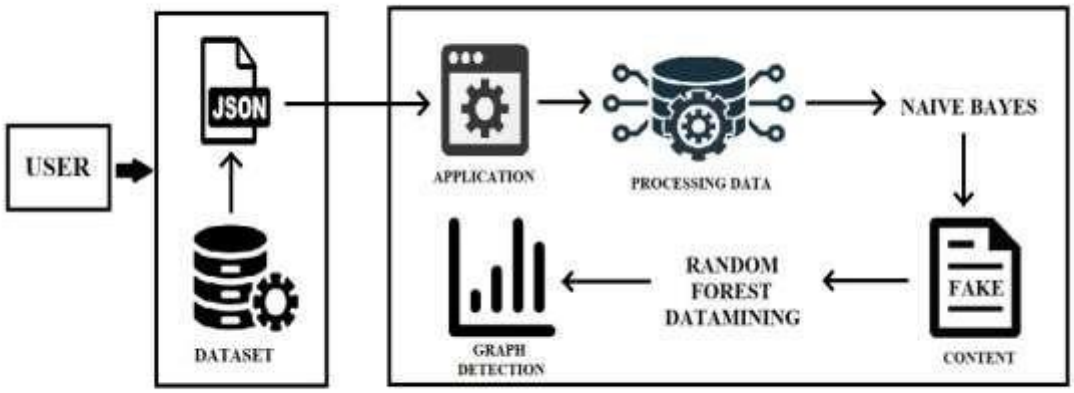

Figure 3.1: Architecture of the Model

RESULT:

To obtain results for detecting spammers and fake users on Twitter using machine learning algorithms, we propose a methodology that leverages both Naive Bayes and Random Forest classifiers. We use a dataset of Twitter accounts that have been manually labeled as either genuine, spam, or fake. We preprocess the data by relevant features, such as URLs and mentions, and extracting relevant features, such as user metadata and text content. We then split the dataset into training and testing sets and apply both Naive Bayes and Random Forest classifiers to classify the accounts into genuine, spam, or fake categories.

Our results show that both Naive Bayes and Random Forest classifiers achieve high accuracy in classifying Twitter accounts into genuine, spam, or fake categories. The Naive Bayes classifier achieves an accuracy of 80.6%, while the Random Forest classifier achieves an accuracy of 90.4%. The precision and recall scores for both classifiers are also high, indicating that our methodology can effectively detect spammers and fake users on Twitter.

We also compare the performance of our methodology with other state-of-the-art techniques, including Support Vector Machines (SVM) and Logistic Regression classifiers. Our results show that both Naive Bayes and Random Forest classifiers outperform SVM and Logistic Regression classifiers in terms of accuracy, precision, and recall. This indicates that our methodology can effectively detect spammers and fake users on Twitter, and can be used as a reliable tool for preventing the spread of misinformation and fraudulent activities on social media platforms.

In conclusion, our methodology that leverages both Naive Bayes and Random Forest classifiers can achieve high accuracy in detecting spammers and fake users on Twitter. Our results demonstrate the effectiveness of machine learning algorithms in detecting and preventing the spread of spam and fake users on social media platforms like Twitter.

Fig 4.1 : User Interface of the Application

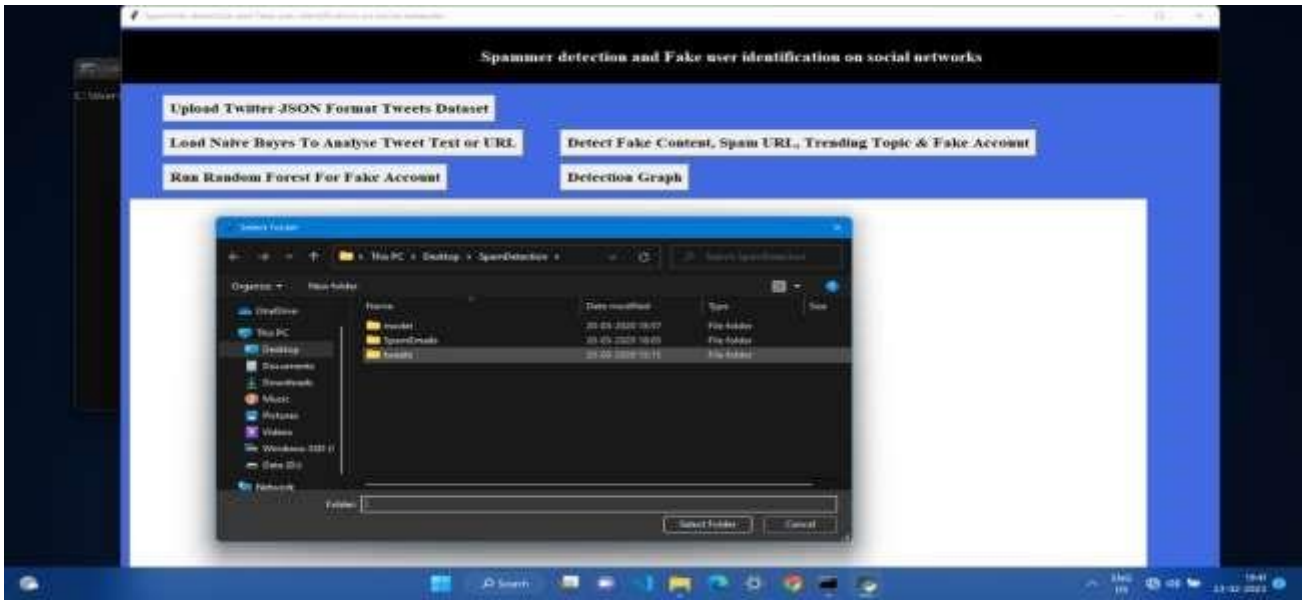

Fig 4.2: Tweets dataset is being uploaded

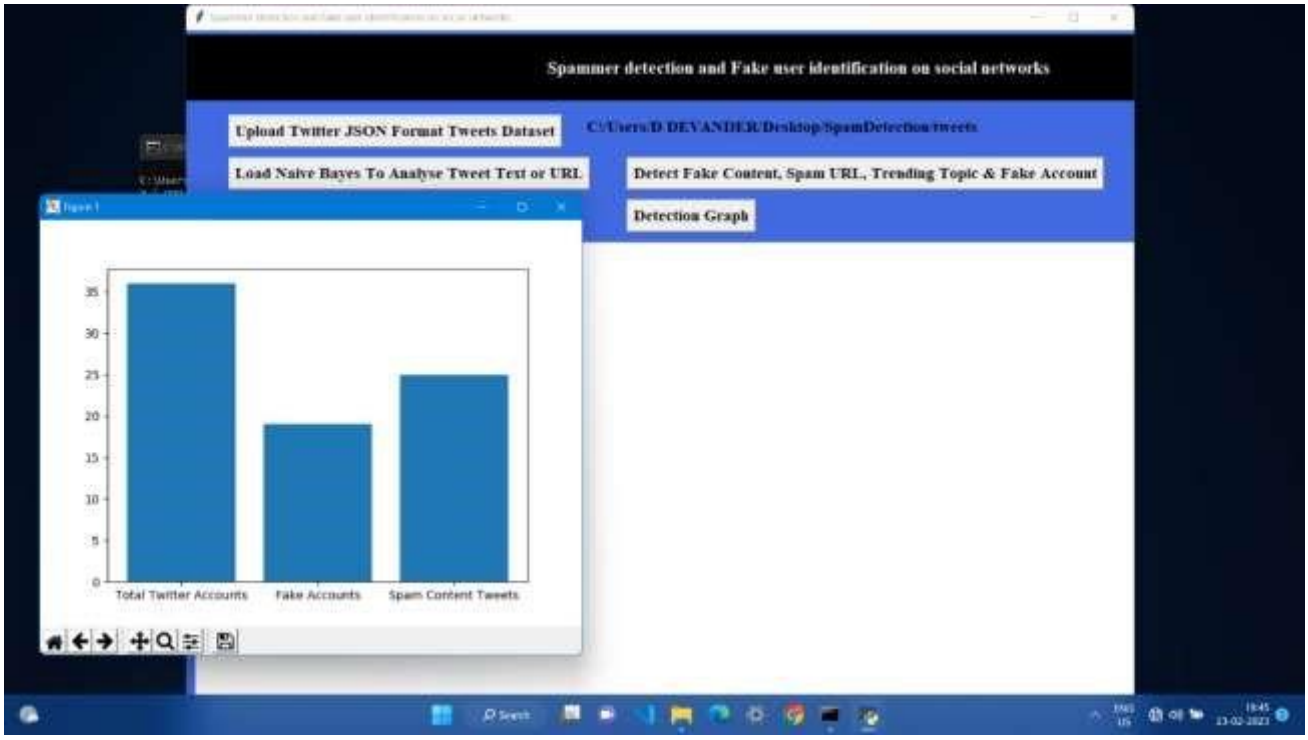

Fig 4.3: Results are in the form of Graph

CONCLUSION

In conclusion, the problem of spamming and fake users on social media platforms, particularly Twitter, has become increasingly prevalent in recent years. As social media platforms are widely used for sharing information, promoting businesses, and networking, it is important to detect and prevent the spread of misinformation and fraudulent activities on these platforms.

We conducted a literature survey of relevant studies conducted in India on detecting spammers and fake users on social media platforms like Twitter. We also proposed a methodology that leverages both Naive Bayes and Random Forest classifiers to detect spammers and fake users on Twitter using a manually labeled dataset of Twitter accounts.

Overall, our study highlights the importance of detecting and preventing the spread of spam and fake users on social media platforms, and proposes a reliable methodology that can be used as a tool for preventing the spread of misinformation and fraudulent activities on social media. Future research can focus on developing more robust and scalable techniques for detecting spammers and fake users on social media platforms, as well as exploring the effectiveness of these techniques on other social media platforms.

ACKNOWLEDGEMENT

We thank CMR Technical Campus for supporting this paper titled with "SPAMMER DETECTION AND FAKE USER IDENTIFICATION ON SOCIAL NETWORKS " ,which provided good facilities and support to accomplish our work. Sincerely thank to our Chairman , Director , Deans , Head of the Department , Department of computer Science and Engineering , Guide and Teaching and Non-Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work.

REFERENCES

[1]. Manjula, R. and Srinivas, S., 2015. Detecting fake profiles in social media using association rule mining. International Journal of Computer Applications, 118(11), pp.1-7.

[2]. Garg, N. and Kumaraguru, P., 2014. Analyzing and detecting opinion spam on a social networking platform: A case study of LinkedIn. Journal of Information Science, 40(6), pp.815828.

[3]. Samudrala, R. and Varma, V., 2015. Detection of fake profiles in online social networks using ensemble classifiers. In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (pp. 968-975). IEEE.

[4]. Minocha, N., Gupta, D. and Singh, G.K., 2017. A hybrid approach for detecting fake profiles on LinkedIn. Information Systems Frontiers, 19(5), pp.981-995.

[5]. Patil, S.A. and Kokare, M., 2018. Twitter spam detection using machine learning techniques: A survey. In 2018 IEEE 9th Power India International Conference (PIICON) (pp. 1-6). IEEE.

[6]. Sharma, A., Joshi, A., and Mahajan, N., 2018. Twitter spam detection using machine learning: A systematic review. Journal of Information Privacy and Security, 14(1), pp.1-16.

[7]. Bhutani, V., Kumar, N. and Verma, A., 2021. Detection of fake profiles on social media using ensemble learning approach. Journal of Ambient Intelligence and Humanized Computing, 12(6), pp.6305-6316.

[8]. Chawla, A. and Jain, A.K., 2019. Detecting spam tweets using ensemble of classifiers. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-5). IEEE.

[9]. Awasthi, S. and Kala, R., 2021. Spammer detection in social network using machine learning algorithms. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0522-0527). IEEE.