IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 8, August 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208045 |

Spammer Detection and Fake User Identification on Social Network

Dr. D. J. SAMATHA NAIDU, LAVANYA R

Principal, Annamacharya PG College of Computer Studies, Rajampet, India

MCA Student, Department of MCA, Annamacharya PG College of Computer Studies, Rajampet, India

ABSTRACT: Social networking spots engage millions of druggies around the world. The druggies' relations with these social spots, similar as Twitter and Facebook have a tremendous impact and sometimes undesirable impacts for diurnal life. The prominent social networking spots have turned into a target platform for the spammers to disperse a huge quantum of inapplicable and injurious information. Twitter, for illustration, has come one of the most sumptuously used platforms of all times and thus allows an unreasonable quantum of spam. Fake druggies shoot uninvited tweets to druggies to promote services or websites that not only affect licit druggies but also disrupt resource consumption. also, the possibility of expanding invalid information to druggies through fake individualities has increased that results in the unrolling of dangerous content. lately, the discovery of spammers and identification of fake druggies on Twitter has come a common area of exploration in contemporary online social Networks (OSNs). In this paper, we perform a review of ways used for detecting spammers on Twitter. also, a taxonomy of the Twitter spam discovery approaches is presented that classifies the ways grounded on their capability to descry (i) fake content (ii) spam grounded on URL, (iii) spam in trending motifs, and (iv) fake druggies. The presented ways are also compared grounded on colorful features, similar as stoner features, content features, graph features, structure features, and time features. We're hopeful that the presented study will be a useful resource for experimenters to find the highlights of recent developments in Twitter spam discovery on a single platform

I. INTRODUCTION

It has come fairly unpretentious to gain any kind of information from any source across the world by using the Internet. The increased demand of social spots permits stoners to collect abundant amount of information and data about stoners. Huge volumes of data available on these spots also draw the attention of fake stoners. Twitter has swiftly come an online source for acquiring real- time information about stoners. Twitter is an Online Social Network (OSN) where stoners can partake anything and everything, analogous as news, opinions and indeed their moods. Several arguments can be held over different motifs, analogous as politics, current affairs, and important events. When a user tweets commodity, it's directly conveyed to his/ her followers, allowing them to unfold the entered information at a much broader position. With the elaboration of OSNs, the need to study and anatomize stoners' conduct in online social platforms has boosted. multitudinous people who do not have important information regarding the OSNs can easily be tricked by the fraudsters. There is also a demand to combat and place a control on the people who use OSNs only for adverts and thus spam other people's accounts

II.RELATED WORK

Research on "Spammer detection and fake user identification on social networks" covers a wide range of topics related to identifying and mitigating the presence of spammers and fake accounts on social media platforms. Here are some areas of related work you might want to explore:

Machine Learning and Data Mining Approaches:

Many studies have used machine learning algorithms, such as support vector machines, random forests, and deep learning, to classify users as genuine or fake based on their behavior, content, and network features. Research in this area focuses on feature extraction, model training, and evaluating the effectiveness of various techniques.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208045 |

Feature Extraction and Representation:

Identifying relevant features for distinguishing between genuine and fake accounts is crucial. Researchers have explored features like posting frequency, content sentiment, engagement patterns, network centrality, and the temporal dynamics of user activities.

Behavioral Analysis:

Studying user behavior patterns can reveal differences between genuine users and spammers/fake accounts. Analyzing posting times, interactions, language usage, and patterns of information dissemination can provide insights into detection methods.

Graph Analysis:

Social network graphs can be used to detect fake accounts by analyzing their connections and relationships. Community detection, clustering, and anomaly detection algorithms applied to the network structure can reveal patterns indicative of spam or fake accounts.

Content Analysis:

Analyzing the textual and multimedia content posted by users can offer valuable clues. Sentiment analysis, topic modeling, and content authenticity assessment can aid in identifying accounts that consistently generate spammy or low-quality content.

Cognitive and Behavioral Psychology:

Research in psychology can provide insights into the cognitive and behavioral characteristics of spammers and fake users. Understanding their motivations and patterns of interaction can help develop more accurate detection methods.

Data Collection and Labeling:

Creating reliable datasets with accurately labeled accounts (genuine, spam, fake) is essential for training and evaluating detection models. Researchers often employ crowdsourcing, manual labeling, or hybrid approaches to build these datasets.

Feature Engineering for Social Network Data:

Developing novel features that capture unique aspects of social network data is an ongoing area of research. Features that consider user influence, user activity patterns, and network dynamics can enhance the accuracy of detection algorithms.

Cross-Platform Analysis:

Exploring how spammers and fake users operate across different social media platforms can reveal common tactics and behaviors. This broader perspective can help improve detection techniques.

III. METHODOLOGY

Designing a robust methodology for "Spammer detection and fake user identification on social networks" involves a systematic approach that integrates various techniques and steps. Here's a general outline of a methodology you can follow:

Problem Definition and Scope:

Clearly define the problem you're addressing: detecting spammers and fake users on social networks. Specify the social networks you'll focus on, the types of spammers/fake users you're targeting, and any specific objectives you have.

Data Collection and Preparation:

Gather a comprehensive dataset containing information about users, their activities, connections, and content. You may need to crawl data from various social media platforms or use publicly available datasets. Clean and preprocess

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208045 |

the data, handling missing values, outliers, and ensuring data quality.

Feature Extraction:

Extract relevant features from the dataset that can help differentiate between genuine users and spammers/fake users. These features can include behavioral, content-based, network-related, and temporal features.

Exploratory Data Analysis (EDA):

Perform EDA to understand the distribution of features, identify patterns, and visualize the differences between genuine and fake users. This step helps you gain insights that can guide feature selection and model development.

Model Selection:

Choose appropriate machine learning algorithms for classification. Common choices include support vector machines, random forests, gradient boosting, and neural networks. Consider the strengths and weaknesses of each algorithm in relation to your problem.

Feature Engineering:

Engineer new features, if necessary, based on the insights gained from EDA. Feature engineering can enhance the model's ability to capture relevant patterns in the data.

Data Splitting:

Divide the dataset into training, validation, and test sets. Cross-validation techniques can help ensure robust model evaluation.

Model Training:

Train the selected machine learning models on the training dataset using the chosen features. Adjust hyperparameters and use techniques like grid search or random search to find the optimal model settings.

Model Evaluation:

Evaluate model performance on the validation set using appropriate metrics such as accuracy, precision, recall, F1-score, and ROC curves. Compare the performance of different models to select the best one.

Tuning and Validation:

If needed, fine-tune the chosen model by adjusting hyperparameters based on the validation results. This step helps optimize the model's performance.

IV. EXPERIMENTAL RESULTS

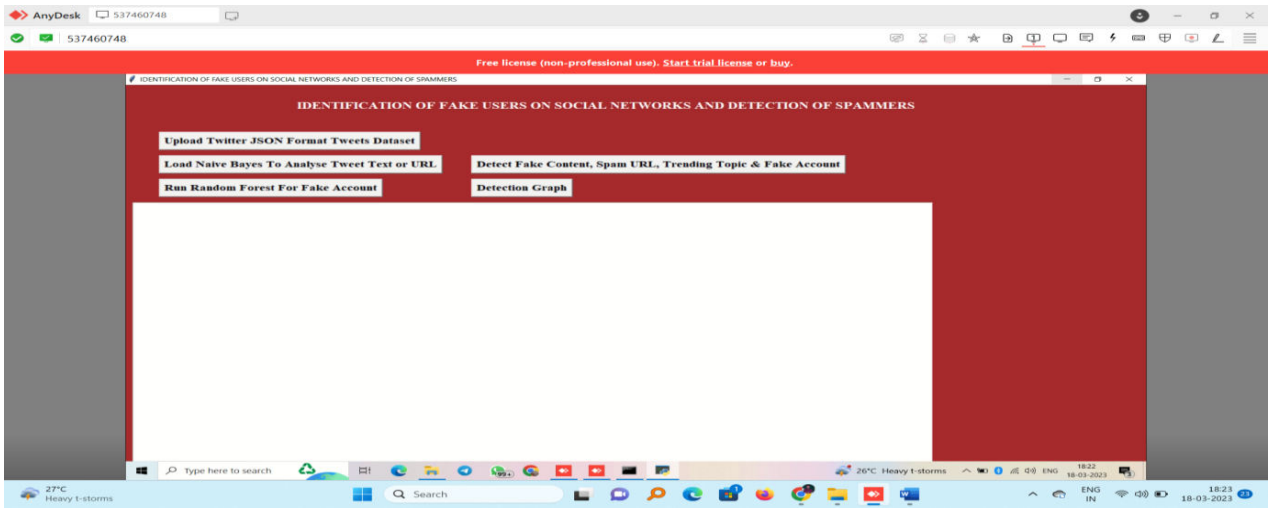

Fig 1. Home page

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208045 |

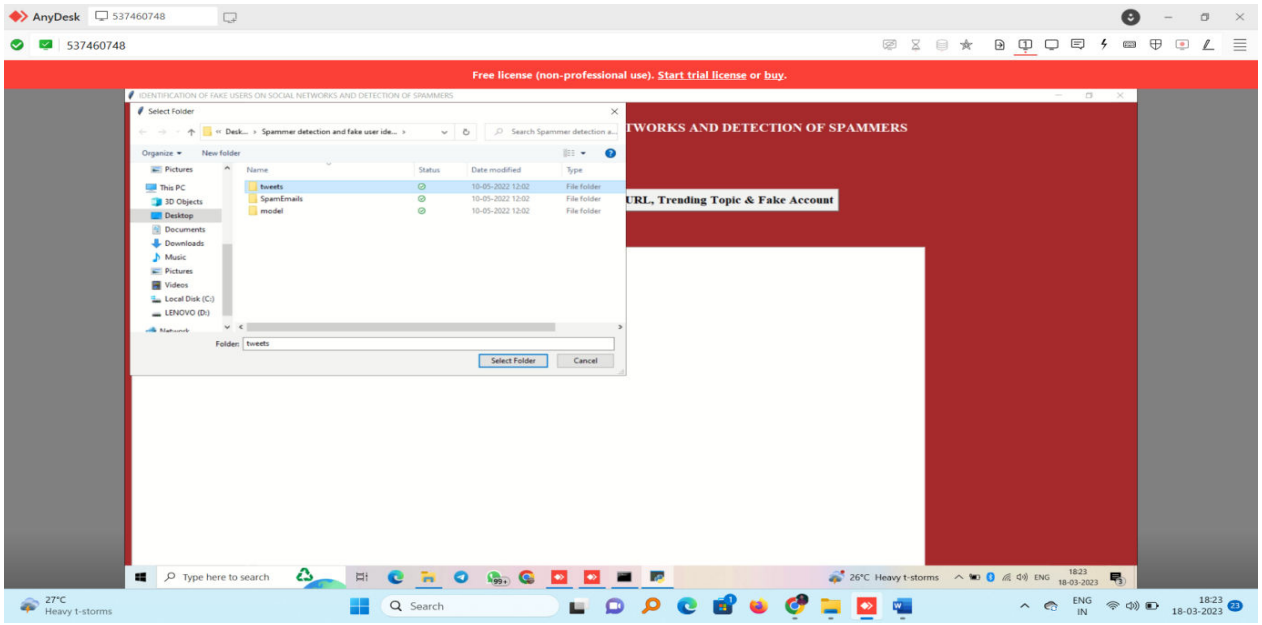

Fig 2. Upload twitter JSON format tweets dataset

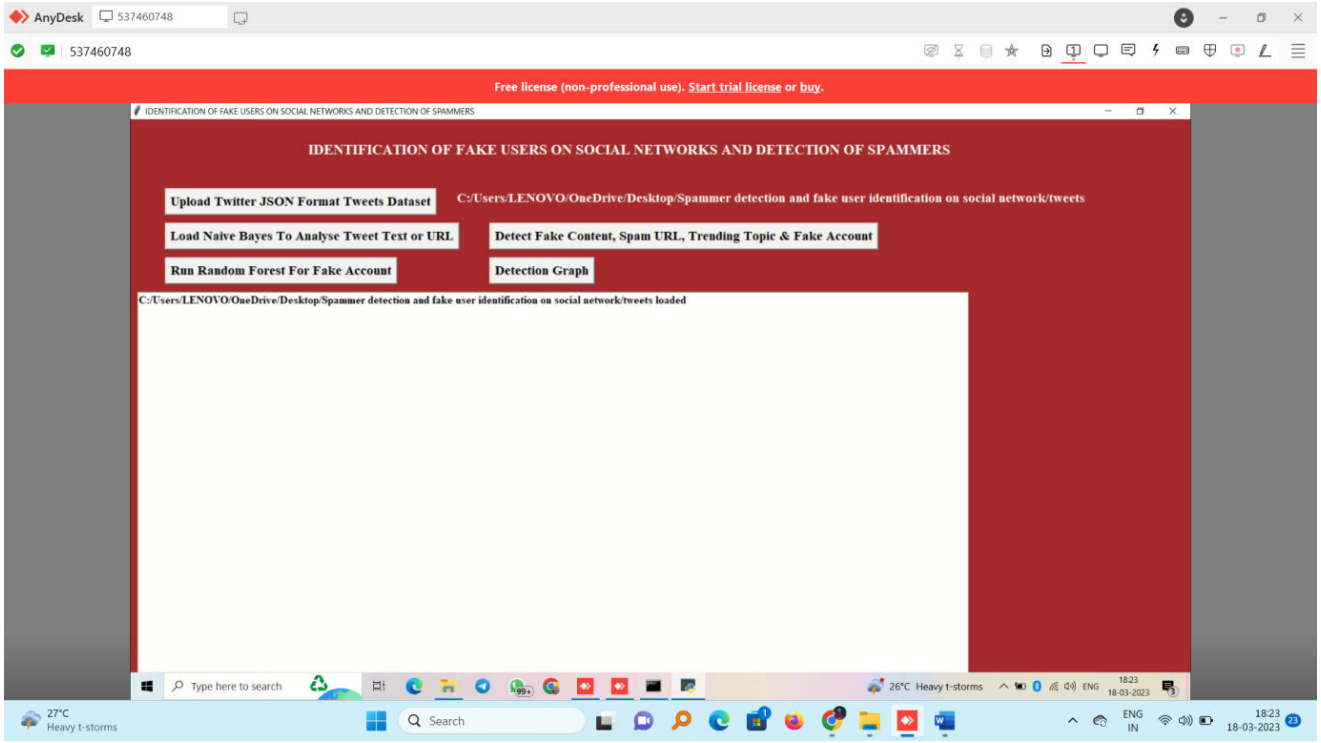

Fig 3. Load naïve bayes to analyse tweet text or URL

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208045 |

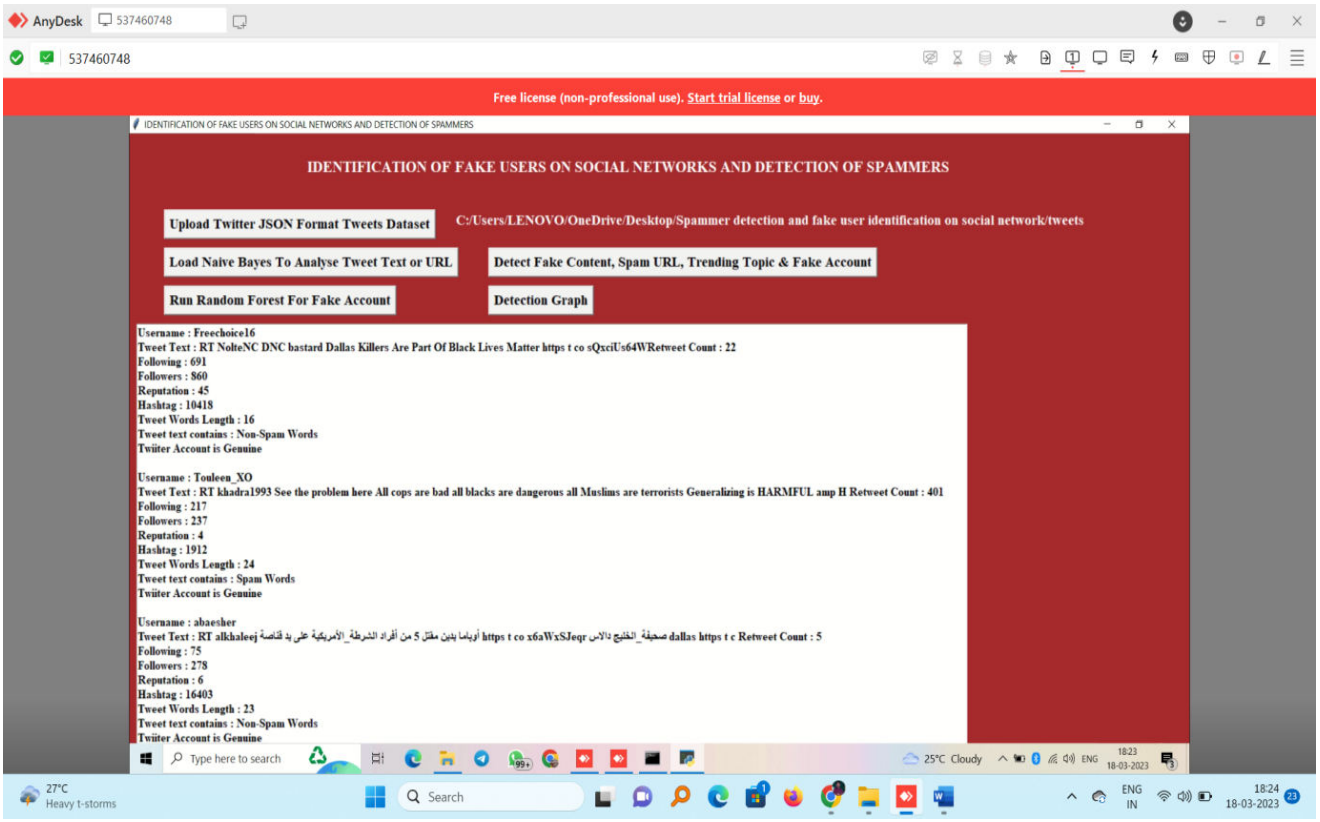

Fig 4. Run Random Forest for fake account

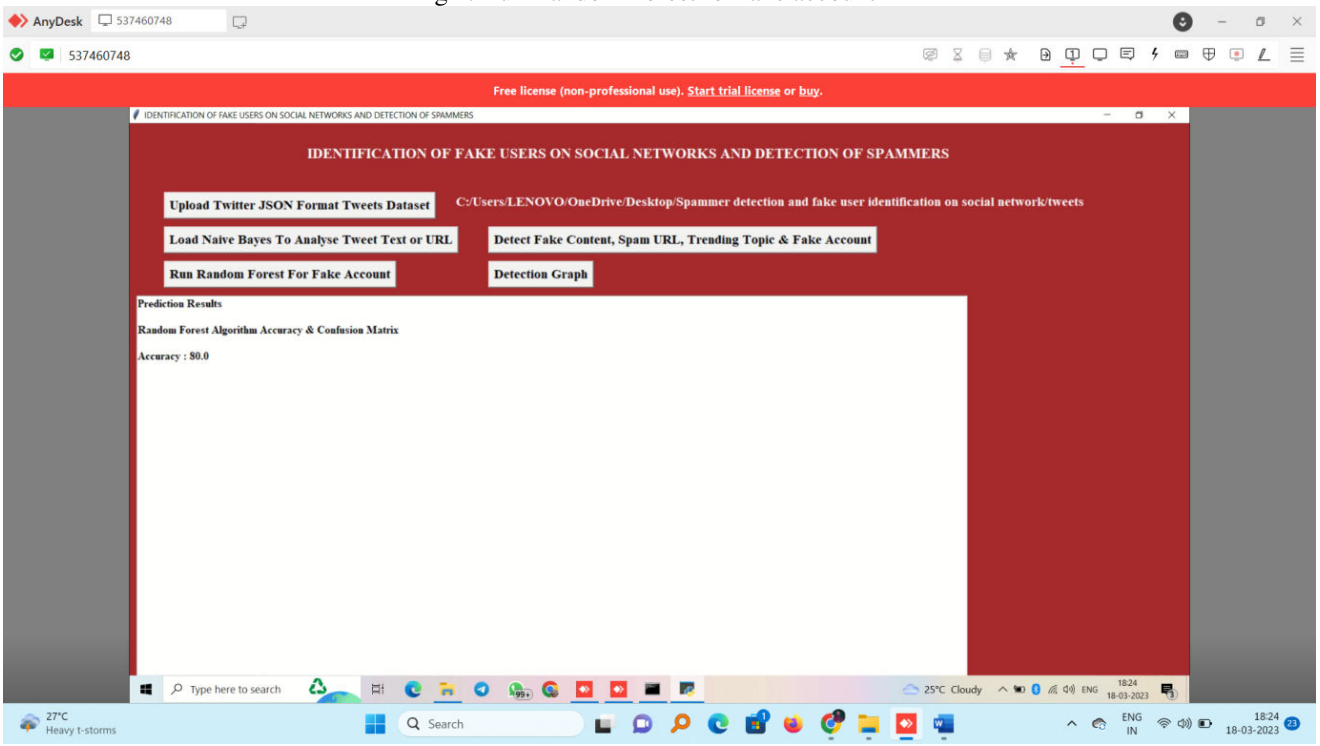

Fig 5. Detect fake content, spam URL, Tending Topic and fake account

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208045 |

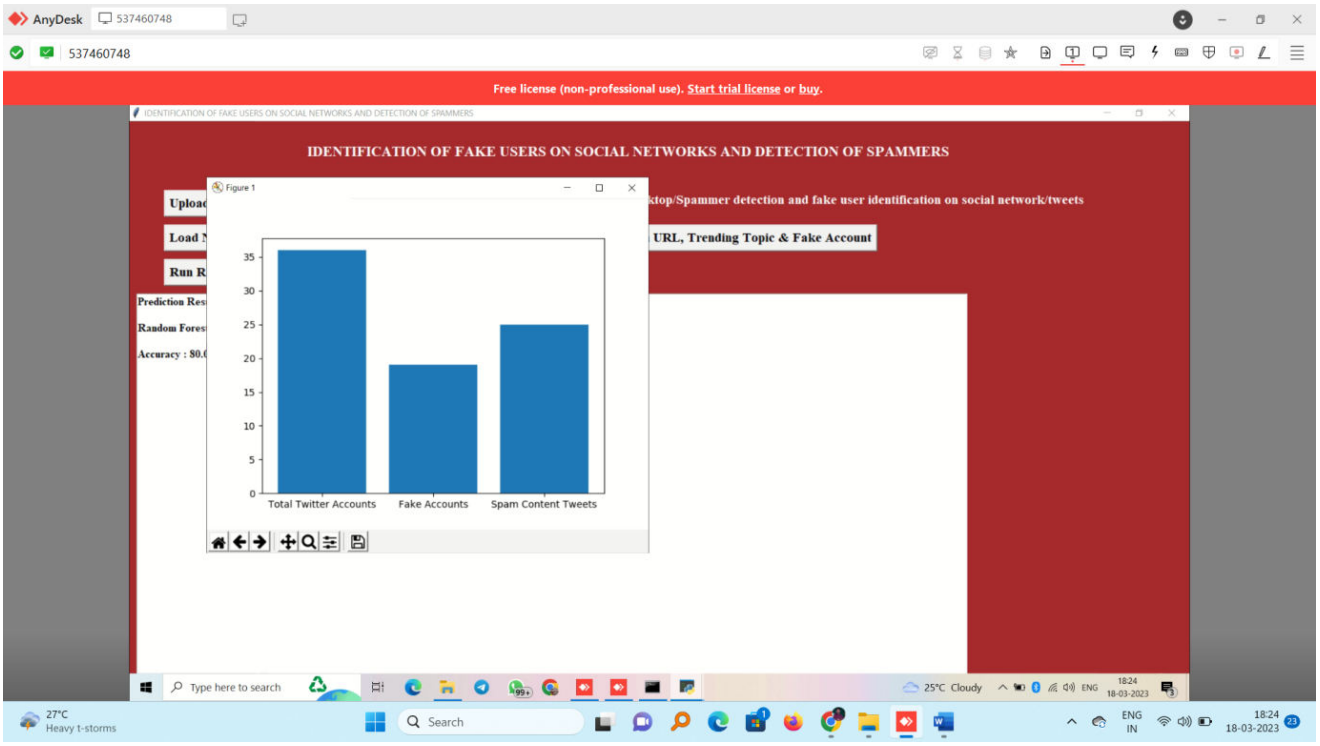

Fig 6. Detection

V. CONCLUSION

In this paper, we performed a review of techniques used for detecting spammers on Twitter. In addition, we also presented a taxonomy of Twitter spam detection approaches and categorized them as fake content detection, URL based spam detection, spam detection in trending topics, and fake user detection techniques. We also compared the presented techniques based on several features, such as user features, content features, graph features, structure features, and time features. Moreover, the techniques were also compared in terms of their specified goals and datasets used. It is anticipated that the presented review will help researchers find the information on state-of-the-art Twitter spam detection techniques in a consolidated form.

REFERENCES

[1] B. Erçahin, Ö. Aktaş, D. Kilinç, and C. Akyol, ‘‘Twitter fake account detection,’’ in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388–392.

[2] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, ‘‘Detecting spammers on Twitter,’’ in Proc. Collaboration, Electron. Messaging, AntiAbuse Spam Conf. (CEAS), vol. 6, Jul. 2010, p. 12.

[3] S. Gharge, and M. Chavan, ‘‘An integrated approach for malicious tweets detection using NLP,’’ in Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT), Mar. 2017, pp. 435–438.

[4] T. Wu, S. Wen, Y. Xiang, and W. Zhou, ‘‘Twitter spam detection: Survey of new approaches and comparative study,’’ Comput. Secur., vol. 76, pp. 265–284, Jul. 2018.

[5] S. J. Soman, ‘‘A survey on behaviors exhibited by spammers in popular social media networks,’’ in Proc. Int. Conf. Circuit, Power Comput. Technol. (ICCPCT), Mar. 2016, pp. 1–6.

[6] A. Gupta, H. Lamba, and P. Kumaraguru, ‘‘1.00 per RT #BostonMarathon # prayforboston: Analyzing fake content on Twitter,’’ in Proc. eCrime Researchers Summit (eCRS), 2013, pp. 1–12.

[7] F. Concone, A. De Paola, G. Lo Re, and M. Morana, ‘‘Twitter analysis for real-time malware discovery,’’ in Proc. AEIT Int. Annu. Conf., Sep. 2017, pp. 1–6.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208045 |

[8] N. Eshraqi, M. Jalali, and M. H. Moattar, ''Detecting spam tweets in Twitter using a data stream clustering algorithm,'' in Proc. Int. Congr. Technol., Commun. Knowl. (ICTCK), Nov. 2015, pp. 347–351.
[9] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, ''Statistical features-based real-time detection of drifted Twitter spam,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 914–925, Apr. 2017.
[10] C. Buntain and J. Golbeck, ''Automatically identifying fake news in popular Twitter threads,'' in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Nov. 2017, pp. 208–215.
[11] C. Chen, J. Zhang, Y. Xie, Y. Xiang, W. Zhou, M. M. Hassan, A. AlElaiwi, and M. Alrubaian, ''A performance evaluation of machine learning-based streaming spam tweets detection,'' IEEE Trans. Comput. Social Syst., vol. 2, no. 3, pp. 65–76, Sep. 2015.
[12] G. Stafford and L. L. Yu, ''An evaluation of the effect of spam on Twitter trending topics,'' in Proc. Int. Conf. Social Comput., Sep. 2013, pp. 373–378

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details