VISVESVARAYA TECHNOLOGICAL UNIVERSITY

BELAGAVI-590018, KARNATAKA.

A PROJECT SYNOPSIS

On

"SPAM ACCOUNT PREDICTOR USING MACHINE LEARNING"

Submitted in Partial Fulfillment for the requirement of VII Semester

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE & ENGINEERING

Submitted By:

Diksha Bhardwaj	**1SG19CS029**
Keshav Chandra Ray	**1SG19CS047**
Kumar Swapnil	**1SG19CS051**
Manas Mishra	**1SG19CS055**

Under the Guidance of

Hemalatha K
Assistant Proffessor

Department of Computer Science and Engineering

(Accredited by NBA)

SAPTHAGIRI COLLEGE OF ENGINEERING

(Affiliated to Visvesvaraya Technological University, Belagavi& Approved by AICTE, New Delhi.)

ISO 9001-2015 & 14001-2015 Certified, Accredited by NAAC with 'A' Grade

14/5, Chikkasandra, Hesarghatta Main Road

Bengaluru – 560057.

2022-2023

TITLE OF THE PROJECT

Spam Account Predictor using Machine Learning

ABSTRACT

For millions of users, using social media is one of the most popular ways to share information and receive updates on their friends and other people they are familiar with. People spend their social contact time in OSNs for information exchange on birthdays and other social political topics through text, photographs, emoticons, and videos due to a lack of physical engagement caused by different geographical places and times. Researchers have used machine learning algorithms to classify spam detection as an issue in order to automatically detect spam. Therefore machine learning algorithms such as neural network ,random forest algorithm and support vector algorithm have been employed to identify spam users on social media platforms.

INTRODUCTION

In today's society, social media plays an important role in everyone's life. The general purpose of social media is to connect with friends, share news, etc. The number of users on social media is increasing dramatically. Instagram has recently gained huge popularity among social media users. With over 1 billion active users, Instagram has become one of the most widely used social networking sites. Following the emergence of Instagram on social media, people with a good number of followers were called Social Media Influencers. These communications promoters have now become the catalyst for a business organization to advertise their products and services.

The widespread use of social media has been a blessing in disguise. Using social media to fraud online, the spread of false information is increasing rapidly. Fake accounts are a major source of false information on social media. Business organizations that invest heavily in Sum from social media should know whether the next acquisition of that account is natural or not. Therefore, there is a widespread need for a false accounting tool, which can accurately determine whether an account is fake or not. In this paper, we use phase algorithms for machine learning to detect false accounts. The process of obtaining a fake account depends largely on factors such as the level of involvement and the activity.

STATEMENT OF THE PROBLEM

Provide an overview and steps pictorial representation where we have already available data set which is required to be On the social interaction platform such as tweeter or facebook there we can consider the set of m users N={n1,n2, n3, n4,…..nk}Each user tries to send some message that comprise some words. Those words can be considered as bag of words for identification of spam and non-spam users as per the labelled data available on the platform available by the legitimate users. Let the profile of user nk is vk the objective of the problem is to classify the user nk is spammer or malicious or not. Mathematically the set can be defined as .

S: nk◊{malicious user(spammer), legitimate user(non-spammer) To identify the user as spammer first step is to identify the features of the tweeted text which contains certain words which can help in the identification of spam content. These contents can be further segregated in the words those can be termed as features for the data segregation. Thereby to build the given set the features can be given for identification of malicious user and non-malicious users as W={w1,w2,w3,…… wm} from S for profile vk.

WHY IS THE PARTICULAR TOPIC CHOSEN?

Web Scraper: Web Scraper is used to extract data from a website. When a user pastes a link of a social media Account, Using OutWit hub, a Web scraper tool, we extract necessary pieces of information from the social media site.

Detection of Fake Accounts: In this step, we combine all the data we extracted from the website. In this paper we mainly focus on engagement rate, artificial activity and spam comments. The data collected using web scraper is used to compute the values for the factors mentioned above.

Artificial Activity: Normal social media activities such as liking, commenting and sharing turns into an artificial activity when the frequency of the above mentioned are very high.

OBJECTIVE AND SCOPE OF THE PROJECT

Objective:

On the basis of algorithms discussed in the last section. A data set of Tweets containing the text messages and their categorization labeling was taken with total 6000 tweets text which are already labelled as spam or malicious and ham or non-malicious. The following steps carried out for the experimenting with given data set with python 3.7 environment.
In today's online social networks there have been a lot of problems like fake profiles, online Impersonation, etc. To date, no one has come up with a feasible solution to these problems. In this project, I intend to give a framework with which the automatic detection of fake profiles can be done so that the social life of people become secured and by using this automatic detection technique we can make it easier for the sites to manage the huge number of profiles, which can't be done manually.

Scope:

Recent times have seen a surge in the reach and popularity of social media. Many social media platforms boast of subscribers in the millions. Like they say, with the good… comes the bad. Along with catching the fancy of genuine subscribers, online social networks have also caught the attention of bad actors. Bots and malicious accounts make up for a significant chunk of the user base. Fortunately, just like real users, fake users also leave trails in data enabling detection of these unwanted and potentially dangerous accounts.

In a large scale OSN, a bad actor can create dozens to thousands of malicious accounts. Making a prediction about each account, as most fake user detection techniques do, may not be scalable or efficient. In such a situation, Cluster level detection is desirable. Legitimate clusters of users show diversity in profile patterns whereas groups of fake accounts created by a single actor show similar distribution and frequency of attributes. Hence, engineering features to describe the whole cluster allows for detection of clusters of fake accounts.

METHODOLOGY

Supervised Machine Learning Classification algorithm named Logistic Regression is user to analyze the Twitter. Logistic regression provide greater accuracy as it is a binary classifier over other multiclass classification algorithms/classifiers namely Random Forest, Decision tree, K-nearest neighbor algorithms. Since this work is based on multiclass classification, but the Logistic Regression classifier is a binary classifier, this work uses a principle named one Vs Rest (OVR) to classify the multiclass classification problem. The natural language is the language used by people for every day communication. NLP applies computational techniques to analyze and synthesize the natural language. In this research, the text is the tweet posted by the person.

The Models used are:

- Random Forest Classifier
- Decision Tree Classifier
- Support Vector Machine(SVM)
- Artificial Neural Network

POSSIBLE OUTCOMES

Since we can anticipate spam or unwelcome users on social media sites and shield other users from scams and spam, this will improve and safeguard social interactions. In a sense, we are creating a secure atmosphere for everyone.

REFERENCES

[1]. Fake Social Profile Detection Using Machine Learning – Er. Ashpreet Kaur, Dr. Abhinav Bhandari
[2]. Spam detection Framework using ML Algorithm - Vinodhini. M, Prithvi. D, Balaji. S
[3]. Fraudulent Account Detection using Machine Learning and Data Science – J. Sucharitha, S. Srivarshini, V. Anusha
[4]. Detecting Fake Acconts in Media Application Using Machine Learning – Gayathri A, Radhika S, Mrs. Jayalakshmi S.L.
[5]. Deep learning for Hate Speech detection in Tweets – Pinkesh Bajdjatiya, Shashank Gupta, Manish Gupta, Vasudeva Varma
[6]. Detecting Fake accounts on Social Media Using Machine Learning Algorithms - Dr. K. Sreenivasa Rao, Dr. G. Sreeram, Dr. B. Deevena Raju .
[7]. Fake Account detection using Machine Learning and Data Science – S.P. Maniraj, Harie Krishnan G, Surya T, Pranav R.
[8]. Fake Profile Identification in Online Social Networks - Siva Nandini, P. Bhaya Anjali, K. Devi Manaswi