IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10417

Twitter Bot Detection

Jison M Johnson[1], Prince John Thekkadayil[2], Mansi D Madne[3], Atharv Nilesh Shinde[4], N Padmashri[5]

Student, Computer Department, Fr. Conceicao Rodrigues Institute of Technology, Navi Mumbai, India[1-4]

Asst. Professor, Computer Department, Fr. Conceicao Rodrigues Institute of Technology, Navi Mumbai, India[5]

Abstract: Today, social media platforms are being utilized by a gazillion of people which covers a vast variety of media. Among this, around 192 million active accounts are stated as Twitter users. This discovered an increasing number of bot accounts are problematic that spread misinformation and humor, and also promote unverified information which can adversely affect various issues. So in this paper, we will detect bots on Twitter using machine learning techniques. A web application where we can verify if the account is a bot or a genuine account. We analyze the dataset extracted from the Twitter API which consists of both human and bot accounts. We analyze the important features like tweets, likes, retweets, etc., which are required to provide us with good results. We use this data to train our model using machine learning methods Decision Trees and Random Forest. For linking our model with the web content, we used the flask server. Our result on our framework indicates that the user belongs to a human account or a bot with reasonable accuracy.

Keywords: Machine learning, Twitter, bot detection, Random forest.

I. INTRODUCTION

Twitter is a social networking site which has one of the most rapidly growing user base. It allows users to express their opinions, discuss current affairs and share news. Governments, organizations, and individual people are actively attempting to persuade or influence the users of social media by spreading propaganda with large networks of bot accounts. The users can follow people whom they know and can spread their contacts. Twitter is a great place for interaction and to meet new people. Twitter was released in 2006 and it turned out to be one of the most popular social networking and microblogging sites. The distinctive feature of Twitter is its simplicity. It allows users to interact through text-based posts, known as tweets. The tweets can be grouped into topics by using a Hashtag, which are words or phrases prefixed with a hashtag symbol. When a user posts tweets, these tweets are displayed on the user's homepage and to his/her followers. In recent times bots generate more internet traffic than human users. A bot is a code that does automated tasks. On social media, the existence of bots is quite noticeable. It is estimated that more than 50 million Twitter accounts are bots. Many bots are easy to distinguish as a bot that copies human behaviour and tries to spread information. But it's difficult to classify an account as a bot or human when it mimics like a human user. Bots can be used for plenty of purposes, many of which provide services to users. Bots can be classified as “good” or “bad” depending upon their use and purpose. These ‘social spambots’ can serve a variety of purposes but can be very difficult to detect, even by human observers. Bad bots don’t identify themselves to the online servers they access, while good bots declare and identify themselves. Around 60% of internet bot traffic can be classified as bad and the other 40% is classified as good. The ability to identify bots as “good” or “bad” on social networking sites is important for healthy information exchange. Many corporations and organizations have used Twitter as a media channel for communication. We have seen successful use of Twitter in the fields of marketing, customer service, election campaign, and in public relations, the rapid growth in user base and the open nature of Twitter makes it easy to get exploited from automated programs, which are known as bots. Like existing bots in other web applications and social media, bots have been common on Twitter. Twitter does not examine strictly automation. It only requires the CAPTCHA image during registration. A bot can do many human tasks after getting the login credentials so Twitter doesn't need to detect whether the user is a bot or not.

II. STUDY OF THE SYSTEM

A. Twitter and Bots

Twitter bots are the accounts that are automated (controlled by software). They are made to perform tasks similar to those of normal users like tweeting and following other users. But their main purpose is tweeting and retweeting some specific tweets which are based on a specific situation. Not all bots are harmful. Some of them are helpful. Bots are used in passing messages like broadcasting some news, sharing content that might be informative, and also used to make automated replies to messages or queries posted in several applications. But there is a flip side too. There are

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10417

some harmful activities done with the help of these bots. These bots are used to spread misleading information and false news about a certain situation. These bots are used for spamming an account or also for breaching and violating someone's privacy.

Twitter bots tend to perform or act like human beings. It remains in stealth mode. These bots may like your tweets and the content you post. Or they can also be used to bully someone, intimidate and also persuade people with some false information. Twitter bots are used on a large scale by cybercriminals to send malware to different users. We need to be careful and ignore these links sent by these kinds of suspicious accounts and be far away from touching malware. Twitter bots are also being used in political propaganda. And eventually, it may influence the election results. The groups may use these bots to spread discontent or panic. These bots can affect the elections, financial section, healthcare community, etc.

B. Machine learning

Machine learning is the field that provides computers the capability to learn without the need for any explicit coding. It's one of the latest and exciting technologies that are there in the market today. This field helps computers or machines to reach one step closer to being a human, with the ability to learn. There are three types of machine learning which are: supervised machine learning, unsupervised machine learning, and semi-supervised machine learning.

In supervised machine learning, the systems are given or are exposed to a large labelled dataset. For example, a handwriting recognition system. A supervised machine learning system would be able to understand the cluster of shapes and pixels that is associated with the numbers and thus, able to recognize or classify the numbers based on the above categorization. The system will be able to recognize the numbers like 4, or 5, or 9, etc. But for this to happen, we require a dataset that's labelled with these classifications of numbers.

In unsupervised machine learning, it looks to identify patterns in data by trying to find the similarity between the data. Clustering is an example of unsupervised machine learning. For example, google showing news that is similar to each other. The algorithm looks for similarities and groups the data accordingly detection is now one of the important tasks to be performed while spamming detection. So, for this purpose machine learning techniques are used.

C. Related Works

Methodologies studied by us led us to know that mainly there are two approaches: one is by language modelling and the second is using the attributes of an account.

Twitter is a rapidly growing social networking site. It allows us to share contents, or news and it also allows us to connect with other people or the society. Governments, organizations, and individual people are actively attempting to persuade or influence the users of social media by spreading propaganda with large networks of bot accounts. The users can follow people whom they know and can spread their contacts. Twitter is a great place for interaction and to meet new people.

The second type of approach found was using the attributes of an account. This approach used attributes either from Twitter API itself or from some other data source like the CRESCI dataset. In this approach, they were working with an assumption that bot accounts will be fundamentally different from human accounts in some aspects. Then these attributes were used in different algorithms like the Naive Bayes algorithm, decision tree algorithm, random forest algorithm. Problems related to these methods were as given. First, in some cases, the boundary separating the bot account and human account is not sharp. Second, sometimes, too many features are used and for some of these algorithms, fewer features or attributes were used. Third, in one of the models, they had to add a boosting algorithm to increase the accuracy value.

III. DESIGN OF THE SYSTEM

A. Requirement Analysis

i. Hardware Requirement

- RAM 8+GB
- Active internet connection
- CPU with 1.5GHz

ii. Software Requirement

- Operating System: Windows 10/Windows 7
- Language: Python 3.8
- Software: Jypter Notebook/Google Notebook
- Modules: Pandas, Numpy, Scikit-Learn, Matplotlib Web
- Server (Back-end): Flask/Django/Cloud

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

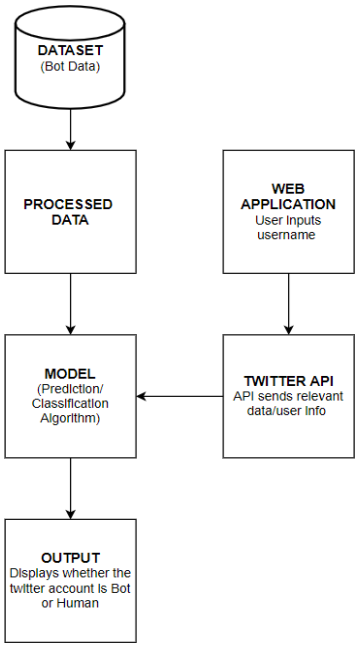
DOI 10.17148/IJARCCE.2021.10417

- Front end: HTML, CSS, Bootstrap.

B. System Architecture

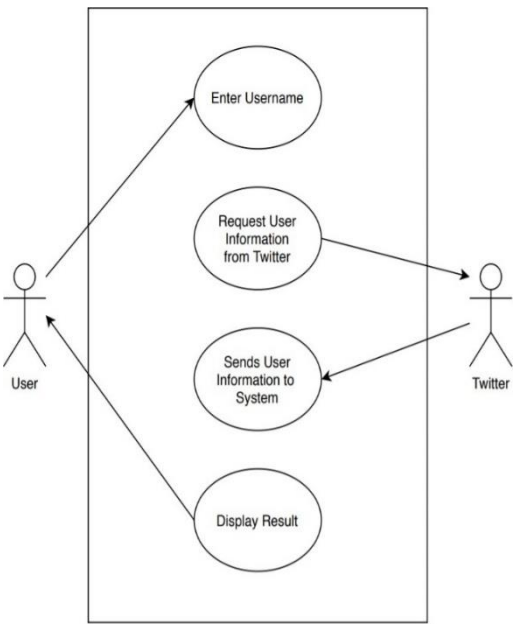
i.Block Diagram

A block diagram is a specialized, high- level flowchart used in engineering. It is used to design new systems or to describe and improve existing ones. Its structure provides a high-level overview of major system components, key process participants, and important working relationships.



ii.Use case Diagram

Use case diagrams are used to gather the requirements of a system including internal and external influences. These requirements are mostly design requirements. Hence, when a system is analyzed to gather its functionalities, use cases are prepared and actors are identified. When the initial task is complete, use case diagrams are modelled to present the outside view.



IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

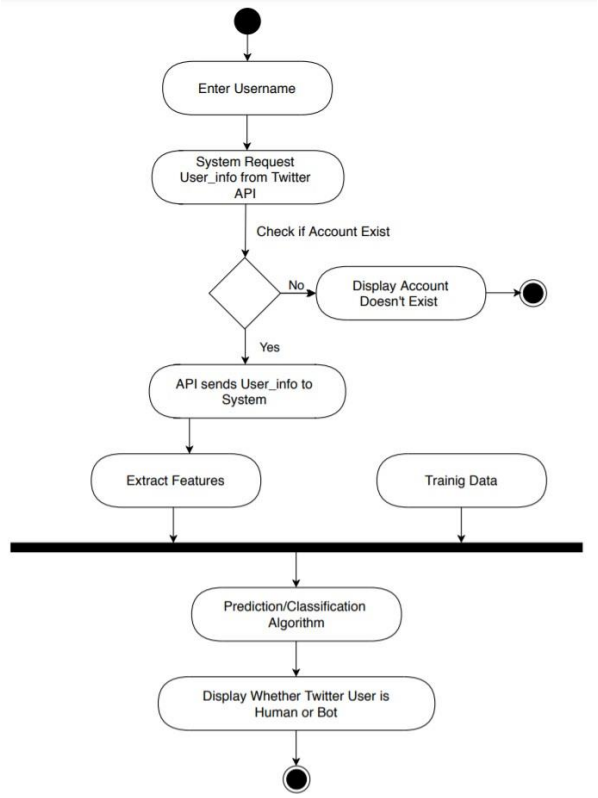
International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10417

iii.Activity Diagram

Activity Diagrams describe how activities are coordinated to provide a service which can be at different levels of abstraction.



IV. IMPLEMENTATION

A. Dataset

The dataset consisted of a total of 16 attributes. Some of these attributes were binary, some numerical and some were descriptive. The 19 attributes or columns were:

1) id
2) id_str
3) Screen name
4) Location
5) Description
6) Url
7) Follower's count
8) Friends count
9) Listed count
10) Created at
11) Favorites count
12) Verified
13) Statuses count
14) Lang
15) Status
16) Default profile
17) Default profile image
18) Has extended profile Name
19) Name

Out of these 19 attributes, we have selected only nine at- tributes, which were: screen name, name, description, status, verified, followers count, friends count, statuses count, and listed count. Listed count refers to the popularity of that account.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10417

B. Feature Selection

Out of these 9 attributes, screen name, name, description, status, verified and listed count are binary attributes. And the rest are numerical values. Apart from listed count and verified attributes, other attributes were made as binary-valued by comparing them with some words. We found that there were a set of words that were found to be there in the descriptive fields of a bot account.
Some of those words are bot, prison, paper, follow me, tweet me, swag, bang, b0t, magic, face, wizard, etc. So, if any of these words are present in those above-mentioned descriptive fields, then there is a high chance of that account being classified as a bot.

C. Model

To build our model, we first trained our dataset on different algorithms to find the most optimum algorithm to go forward with. The algorithms used were as follows:

1) Decision tree
2) Logistic regression
3) KNN classifier
4) SVM classifier
5) Kernel SVM
6) Naive Bayes
7) Random Forest

The dataset was trained on these seven different algorithms. Before passing the dataset to these algorithms, the dataset was pre-processed. Then the most efficient algorithm was selected to be the model for our system. We found the most efficient and accurate algorithm was the random forest algorithm. Random forest is a collection of decision trees. It generally provides higher accuracy than the normal decision tree as was observable in our experiment too. It used different attributes like friends count, followers count, listed count, etc. to predict the result as a bot or a genuine account. Eighty percentage of the dataset was used to train the model and the rest twenty percentage to test the trained model.
It was found that the most important attribute in the list of 9 attributes is the 'verified' attribute. Most of the time, the model predicted the account as a bot whenever the verified attribute was 'FALSE'. It's not necessary for accounts specified as 'FALSE verified' to be a bot and vice versa. Also, most of the bot accounts predicted were not popular. That's because these bot accounts generally remain in a stealth mode.
The model built using the random forest algorithm was quite efficiently able to predict the account as a bot or a genuine account.

V. RESULTS

The model required for this project aims to predict whether a given Twitter account is a genuine user or a bot and also to have the best accuracy. For this reason, we implemented various types of classification algorithms and selected the one with the maximum accuracy score. The below table shows the algorithms and their accuracy scores.

Algorithms	Accuracy Rate	Misclassification Rate	True Positive Rate
Decision Tree	85.00%	15.00%	86.03%
Logistic Regression	71.85%	28.15%	94.14%
KNN Classifier	83.71%	16.29%	85.67%
SVM Classifier	67.28%	32.72%	93.50%
Kernel SVM	69.28%	30.72%	91.11%
Naive Bayes	62.14%	37.86%	96.22%
Random Forest	85.25%	14.75%	83.50%

As it is clear from the table that random forest has the highest score hence we used random forest in our model. The model uses 9 attributes which are mentioned in the implementation section for prediction. All these attributes for a given account are extracted using Twitter API. Compared against bots our model is 85.28% accurate, with a misclassification rate of 14.72% The true positive rate of this model for bots is 83.5%. This was done with a total dataset of 2,748 total accounts; 1,361 bots and 1,387 real accounts.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10417

VI. CONCLUSION

Our end goal is to build a system for Twitter users to identify whether an account is a bot or not. To achieve this goal, we have designed and implemented a system that takes an account's username as input and classifies it as a human user or a bot. The Random Forest classification algorithm was used to build the model which gives an accuracy rate of 85.28%. Our idea is to allow the users to check whether the information from an unverified and unknown source is a bot or not before blindly spreading it without more research. Spambots are usually used to influence people's opinions on various topics with misinformation and rumors. By having this system, we can prevent such influence.

ACKNOWLEDGMENT

The Success of the project involves high technical expertise, patience, and massive support of the guide, which is possible when team members work together. We take this opportunity to express our gratitude to those who have been instrumental in the successful completion of this project. We would like to show our appreciation to **Mrs. N Padmashri** for their tremendous support and help, without them this project would have reached nowhere. We would also like to thank our project coordinator **Mrs. Rakhi Kalantri** for providing us with regular inputs about documentation and project timeline. A big thanks to our **HOD Dr. Lata Ragha** for all the encouragement given to our team. We would also like to thank our principal, **Dr. S. M. Khot**, and our college, Fr. C. Rodrigues Institute of Technology, Vashi, for giving us the opportunity and the environment to learn and grow.

REFERENCES

[1]. Przybyła, Piotr. (2019). Detecting Bot Accounts on Twitter by Measuring Message Predictability .https://www.aclweb.org/anthology/R191065.pdf
[2]. de Andrade, Norberto & Rainatto, Giuliano & Lima, Fonttamara & Silva Neto, Genésio & Paschoal, Denis. (2019). Machine Learning and Bots detection on Twitter. International Journal of Science and Research (IJSR). 8. 001-011.
[3]. Ranjana Battur & Nagaratna Yaligar: Twitter Bot Detection using Machine Learning Algorithms https://www.ijsr.net/archive/v8i7/ART20199245.pdf
[4]. Jurgen Knauth: Language-Agnostic Twitter Bot Detection
[5]. M. Kantepe and M. C. Ganiz, "Preprocessing framework for Twitter bot detection," 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 2017, pp. 630-634, doi: 10.1109/UBMK.2017.8093483.
[6]. Wetstone, Jessica and Sahil R. Nayyar. “I Spot a Bot: Building a binary classifier to detect bots on Twitter.” (2017). http://cs229.stanford.edu/proj2017/final-reports/5240610.pdf
[7]. Chavoshi, Nikan, H. Hamooni and A. Mueen. “On-Demand Bot Detection and Archival System.” Proceedings of the 26th International Conference on World Wide Web Companion (2017): n. pag. https://api.semanticscholar.org/CorpusID:8175106
[8]. Abou Daya, Abbas & Salahuddin, Mohammad & Limam, Noura & Boutaba, R. (2020). BotChase: Graph-Based Bot Detection Using Machine Learning. IEEE Transactions on Network and Service Management. PP. 10.1109/TNSM.2020.2972405. https://www.researchgate.net/publication/338779142_BotChase_Graph_Based_Bot_Detection_Using_Machine_Learning