e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

DETECTING MALICIOUS BOTS USING MACHINE LEARNING : A REVIEW

Akolkar Vishwa*1, Gadekar Ankita*2, Patil Pooja*3, Pawar Surbhi*4

*1,2,3,4Computer Science & Engineering, Vidya Pratishithan's Kamalnayan Bajaj Institute of Engineering and Technology, Baramati, India.

ABSTRACT

Social bots are considered the foremost common quite malware in social platform. they will produce fake messages, spread rumours, and even manipulate public opinions. social bots are used to perform automated analytical services and provide users with improved quality of service. However, malicious social bots have also been used to disseminate false information and this will end in real-world consequences one among the best challenges for bot detection in social media is in understanding what social bots can do and analyze the quantitative features of their behavior. This model distinguished normal users from social bots. This paper proposes an approach to detect the twitter bots using machine learning algorithms. We Compare K-NN Algorithm, SVM Algorithm, Naive Bayes Algorithm, Random Forest Algorithm, Decision Tree Algorithm and custom algorithm.The best learning model will be applied on test data.

Keywords: Online social network, Social bots, User behavior, Supervised Learning.

I. INTRODUCTION

Social media bots are machine-controlled programs use have interaction in social media. These bots behave in an either partly or absolutely autonomous fashion, and are typically designed to mimic human users. Whereas benevolent social media bots exist, several social media bots are employed in dishonest and wicked ways. Some estimates suggest that these malicious bots structure a large share of all accounts on social media. While these terms are typically used interchange- ably, chatbots are bots which will severally hold a speech communication, whereas social media bots don't have to be compelled to have that ability. Chatbots are able to answer user input, however social media bots don't ought to know a way to converse. In fact, several social media bots don't communicate exploitation language at all, they only perform additional straightforward interactions like providing 'follows' and 'likes'. Social media bots conjointly exist on a way larger scale than chatbots, due to the extent of human management needed. A chatbot typically needs someone or perhaps a team of individuals to take care of its functionality. On the opposite hand, social media bots are a lot of easier to manage, and ofttimes hundreds of or perhaps thousands of social media bots are managed by one person.[10]

Some social media bots offer helpful services, like weather updates and sports scores. These 'good' social media bots square measure clearly known intrinsically and therefore the those who act with them recognize that they're bots [9], but an oversized range of social media bots square measure malicious bots disguised as human users. Malicious social media bots will be used for variety of functions like a artificially amplifying the popularity of a person or movement, Influencing elections, Manipulating financial market, Amplify phishing attacks, Spreading spam, etc.[11]

Therefore, it's necessary to spot and eliminate malicious social bots on on-line social networks. One of the best challenges for bots detection in social media is in understanding what modern social bots will do and analyze the quantitative features of their behavior. Most current detection strategies of malicious social bots analyze quantitative characteristics of their behavior. These bots will simply mimic social bots.

II. RELATED WORK

F. Morstatter et.al [6] have explore the matter of finding bots on social media. They start by grouping 2 datasets, each with different labeling mechanisms. Then they have a tendency to still propose a bot detection technique that optimizes the F1 score of the model, which considers recall additionally to precision. The datasets they have a tendencyto check this technique were labeled through different processes.

Y. Zhou et al [7] presents a unique system, ProGuard, to automatically detect malicious OSN accounts that participate in online promotion events. ProGuard leverages 3 classes of features including general behavior, virtual-currency assortment, and virtual-currency usage. Experimental results based on labeled data collected from Tencent QQ, a world leading OSN company, have demonstrate the detection accuracy of ProGuard, that has

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

achieved a high detection rate of 96.67% given a particularly low false positive rate of 0.3%.

M. Al-Qurishi et al [2] They tried a unique approach relating to the method of data extraction and classification to contextualize large-scale networks in correct manner. They also collected a big range of user profiles from Twitter and YouTube, together with around thirteen million channel activities. In depth evaluations were conducted on real-world datasets of user activities for each social networks. The analysis results show the effectiveness and utility of the proposed approach. The main goal of this analysis was to present an integrated system with analytic ability to sight malicious activities in OSNs.

S. Barbon [5] They have proposed an algorithm for classifying users as being human, a legitimate bot, or a malicious bot in OSNs. The algorithm was based on Discrete Wavelet Transform to obtain a pattern of writing style embedded in post contents. Experiments are conducted by classifiers with 2 totally different datasets: single and miscellaneous theme, it absolutely was determined that the planned technique yields the high average classification accuracies of 94.47% for each datasets. Considering the results, the text-based model they developed, provides promising accuracies in classifying the user based on its writing style.

III. SYSTEM ARCHITECTURE

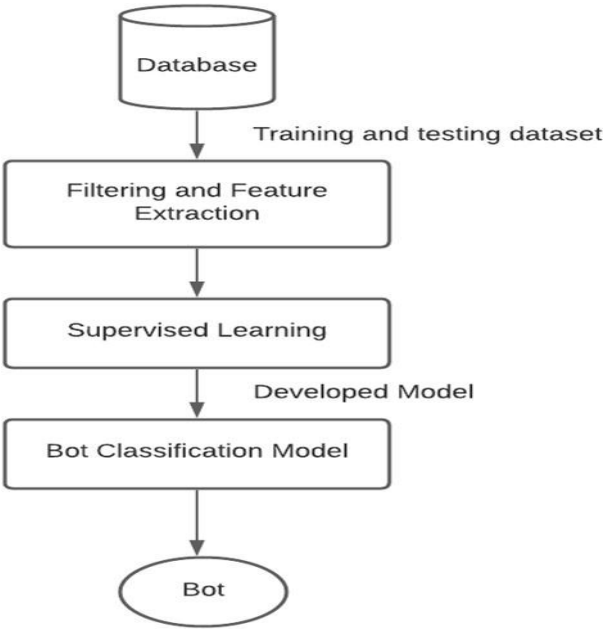

Fig. 1. System Architecture

IV. MACHINE LEARNING BASED BOT DETECTION

Machine learning is a field of computer science and subset of artificial intelligence (AI), that has ability to automatically learn and improve from experience without being explicitly programmed. It involves the study and construction of techniques that enable computers to self-study supported the input data to solve specific problems. Machine learning focuses on the development of computer programs which will access information and use it to learn for themselves.

Based on the learning strategies, machine learning techniques are usually divided into three main categories: supervised learning, unsupervised learning and semi-supervised learning. supervised learning may be a variety of learning within which training data is labeled. The machine can "learn" from the labeled patterns to create the classifier and use it to predict labels for new data. In contrast, unsupervised learning is a variety of learning within which training data has not been labeled. In this form, the machine can learn by analyzing the data characteristics to construct the classifier. And Semi- supervised learning is the hybrid approach between supervised and unsupervised learning. Each method of machine learning has its own advantages, disadvantages and applications.

In this paper, we only examine the effectiveness of supervised learning techniques in bot detection and also the next section in short describes the common supervised machine learning algorithms, together with k-nearest neighbor(kNN), decision tree, suport vector machine(SVM), random forest, and Naive Bayes.[8][11]

A. Supervised Machine Learning Techniques

1) K-NN Algorithm

- K-Nearest Neighbour is one among the best Ma- chine Learning algorithms supported supervised Learning technique.
- K-NN rule assumes the similarity between the new case/data and obtainable cases and place the new case into the class that's most almost like the obtainable classes.
- K-NN rule stores all the obtainable information and classifies a replacement information supported the similarity. this suggests once new information seems then it are often simply classified into a well suite class by mistreatment K- NN rule.
- K-NN rule are often used for Regression also as for Classification however principally it's used for the Classification issues.

2) SVM

- Support Vector Machine or SVM is one in all the foremost common supervised Learning algorithms, that is employed for Classification in addition as Regression issues. However primarily, it's used for Classification issues in Machine Learning.
- The goal of the SVM rule is to make the simplest line or call boundary that may segregate n- dimensional house into categories. This best callboundary is termed a hyperplane.
- SVM chooses the acute points/vectors that facilitate in making the hyperplane. These extreme cases area unit referred to as as support vectors, and therefore rule is termed as Support Vector Machine.

3) Naive Bayes Algorithm

- The Naive Thomas bayes formula is comprised of two words Na¨ıve and Bayes, which might be delineated as Naive : it's referred to as Naive as a result of it assumes that the incidence of an explicit feature is freelance of the incidence of alternative options. like if the fruit is known on the bases of color, shape, and taste, then red, spherical, and sweet fruit is recognized as an apple. therefore every feature separately contributes to spot that it's an apple whilenot counting on one another.
- Naive Bayes formula may be a supervised learning formula, that relies on Bayes theorem and used for resolution classification issues.
- It is primarily used in text classification that has a high-dimensional training dataset.
- Naive Bayes Classifier is one in all the easy and handiest Classification algorithms that helps in building the quick machine learning mode Naive man of science formula could also be a supervised learning formula, that depends on man of science theorem and used for resolution classification problems.ls that may create fast predictions.

4) Random Forest Algorithm

- Random Forest could be a in style machine learning formula that belongs to the supervised learning technique. It may be used for each Classification and Regression issues in metric capacity unit.
- it's supported the construct of ensemble learning, that could be a method of mixing multiple classifiers to resolve a posh drawback and to enhance the performance of the model.
- Random Forest could be a classifier that contains variety of call trees on varied subsets of the given dataset and takes the common to enhance the prophetic accuracy of that dataset.
- Instead of wishing on one call tree, the random forest takes the prediction from every tree and sup- ported the bulk votes of predictions, and it predicts the ultimate output.
- The larger range of trees within the forest ends up in higher accuracy and prevents the matter of overfitting.

5) Decision Tree Algorithm

- Decision Tree may be a supervised learning tech- nique which will be used for each classification and Regression issues, however largely it's most popular for determination Classification issues. it's a tree-structured classifier, wherever internal nodes represent the options of a dataset, branches represent the choice rules and every leaf node represents the result.

- In a decision tree, there are two nodes, that are the decision Node and Leaf Node. Decision nodes used to build any decision and have multiple branches, whereas Leaf nodes are the output of these decisions and don't contain from now on branches.
- The decisions or test are performed on the idea of features of the given dataset.
- It is a graphical illustration for obtaining all the potential solutions to a problem/decision supported given conditions.
- It's known as a decision tree because, the same as a tree, it starts with the root node, that expands on more branches and constructs a tree-like structure.
- A decision tree merely asks an issue, and supported the solution (Yes/No), it more split the tree into subtrees.

V. EXPERIMENT AND EVALUATION

A. Experimental Dataset

To study and understand the behavior of social bots in comparison to human behavior in social networks, it is essential to maintain datasets that consist of both human and bot accounts.

Attributes	Description
id	The integer representation of the unique identifier for this Tweet.
id str	string representation of the unique identifier for this Tweet.
screen name	Name a user chooses to use when communicating with othersonline.
location	The user-defined location for this account's profile
url	A URL provided by the user in association with their pro-file.
description	The user-defined String describing their account.
followers count	The number of followers this account currently has.
friends count	The number of users this account is following.
created at	The UTC date-time that the user account was created on Twitter
listed count	The number of public lists that this useris a member of.

Favorite count	The number of Tweets this user has liked in theaccount's lifetime.
verified	When true, indicates that the user has a verified account
Status count	The number of Tweets (including retweets) issued by the user.
lang	Language of the Tweet text
Status	The text of the status update.
default profile	When true, indicates that the user has not altered the theme or background of theiruser profile.
default profile image	When true, indicates that the user has not altered the theme or background of theiruser profile.

B. Data Pre-Processing/ Data Cleaning

Before jumping to the subtle methods, there are some very basic data cleaning operations that you just probably shouldto perform on each single machine learning project.

Data Cleaning plays a crucial role in the field of Data Managements, Data Analytics and Machine Learning. Data Cleaning means that the method of identifying the incorrect, incomplete, inaccurate, irrelevant or missing a part of the data and then modifying, replacing or deleting them according consistent with the need. Data cleaning is considered a foundational component of the basic data science. When you start to work contains missing values. one the simple things to do in data cleaning is to remove or delete rows with missing values.

One of the important step of fixing errors in your dataset is to find incomplete values and fill them out. Most of the data that you may have, it can be categorized. In such type of cases, it is best to fill out your missing values based on different categories or create entirely new categories to includethe missing values.

If the missing values are significantly less, then removing or deleting missing values may be the proper approach. You'll have to be very sure that the data you are deleting does not include information that is present in the alternative rows of the training data. Handling missing values is incredibly vital as a result of if you leave the missing values as it is, it's going to have an effect on your analysis and machine learning models. So, you wish have to make sure that whether your dataset contains missing values or not. If you find missing values in your dataset you must have to handle it.

One of the vital step is to find incomplete values and fill them out. Most of the data that you may have can be categorized. In such cases, it's best to fill out your missing values based on different categories or create entirely new categories to include the missing values.

After properly finishing Data Cleaning steps, we'll have a robust dataset that avoids several of the foremost

common difficulties. This step should not be rushed as because it proves very helpful in the further method. Having clean data can ultimately increase overall productivity of your project .

C. Feature Selection/Extraction

Feature extraction is a method of dimensionally reduction by which an initial set of raw data is reduced to additional manageable groups for processing. Feature extraction is the name for strategies that select and /or mix variables into features, effectively reducing the amount of data that has to be processed, whereas still accurately and fully describing the initial data set.

The process of feature extraction is beneficial when you need to reduce the number of resources required for process while not losing necessary or relevant information. Feature ex- traction also can reduce the amount of redundant information for a given analysis.

There are three kinds of feature selection techniques inmachine learning- [3]

1) Filter Method-

This methodology uses the variable ranking technique in order to select the variables for ordering and here, the selection of features is independent of the classifiers used. By ranking, it means that how much useful and vital every feature is predicted to be for classification. It essentially selects the subsets of variables as a pre-processing step severally of the chosen predictor. In filtering, the ranking methodology can be applied before with datasets, you'll realize that almost all of the dataset classification for filtering the less relevant features. It carries out the feature selection task as a pre-processing step that contains no induction rule.

Some examples of filter methods -

- Chi-Square Test: generally, this technique is used to check the independence of two events.
- Variance Threshold: It is an approach wherever all features are removed whose variance doesn't meet the precise threshold. By default, this technique removes features having zero variance. The assumption made using this technique is higher variance features are doubtlessly to contain a lot of information.
- Information Gain: Information gain or IG measures what proportion of information a feature provides concerning the class.

2) Wrapper Methods-

The wrapper methods produce many models that are having completely different subsets of input feature variables. Later the chosen features that end in the most effective performing model in accordance with the performance metric.

3) Embedded methodology-

This methodology tries to mix the efficiency of both the previous ways and performs the selection of variables in the method of training and is typically specific to given learning machines. This methodology essentially learns that which feature provides the utmost to theaccuracy of the model.

D. Supervised Learning

In supervised learning, the training data provided to the machines work because the supervisor that teaches the machines to predict the output properly. It applies an equivalent thought as a student learns in a supervision of the teacher. Supervised learning is a method of providing input data as well as correct output data to the machine learning model. The aim of a supervised learning algorithm is to find out a mapping function to map the input variable(x) with the output variable(y).

Classification algorithm is a supervised Learning technique that's used to determine the class of new observations on the basis of training data. In Classification, a program learns from the given dataset or observations and then classifies new observation into variety of categories or groups. Such as, Yes or No, 0 or 1, Spam or Not Spam, cat or dog, etc. classescan be referred as targets/labels or categories.[10][11]

Some supervised classification algorithms we can used toclassify the users into malicious/benign are as follows:

1) K-Nearest Neighbour (KNN)
2) Support Vector Machine (SVM)

3) Naive Bayes Algorithm
4) Random Forest Algorithm
5) Decision Tree Algorithm

E. **Own Classifier Algorithm**

Some typical characteristics of bots on Twitter include:

- Several Twitter bots have a comparatively recent creation date.
- Several bot user names contain numbers, sometimes which can indicate automatic name generation.
- The account primarily retweets content, instead of tweeting original content.
- The account's tweet frequency is over an human user may feasibly accomplish.
- The account may have a high number of followers and even be following a lot of accounts; conversely, some bot accounts are recognizable as a result of they send lot of tweets however only have some followers.
- Several bots tweet an equivalent content as alternative users at roughly the same time.
- Short replies to alternative tweets may also indicate machine-controlled behavior.
- There's typically no biography, or no photo, related to bot Twitter accounts.

Using some of the above characteristics of bots we can create method/algorithm to find bot users from dataset.

In that method/algorithm we can also check

- If the user is verified, then it is normal user otherwise bot.
- If listed count is greater than 16000, then it is bot otherwise normal user.
- If the name or screen name contains "bot" or some malicious words or the words that normal user never use, then that user consider as bot.

VI. CONCLUSION

This paper presents an overview of bot detection using machine learning. Bot detection is a massive challenge in network security management. There are many methods and techniques that have been used to track bot activities and detect them. These technique might be not totally applicable for new generations of bots, but this method can effectively detect bot accounts on social platforms. We develop a novel methodology based on machine learning and supervised learning algorithms that can detect bots from a large and imbalanced dataset. This methodology is not specific to any particular type of bot characteristics, rather it can detect any type of bots.

In future research, further behaviors of malicious social bots will be considered and therefore the projected detection approach are extended.

ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my teachers such as our Prof. Shinde Sir, our Project Guide Prof. Kokare Sir our Honorable HOD Dr. Takale Mam as well as our principal Dr. R. S.Bichkar Sir who gave us the golden opportunity to work on the topic " Detecting Malicious Bots in Social Media Accounts ", which also helped us in doing a lot of Research and we came to know about so many new things, we are really thankful to them. Secondly we would also like to thank our parents and friends who helped us a lot in this. And we hope our Project will be helpful to detect the bot users.

V. REFERENCES

[1] M. Sahlabadi, R. C. Muniyandi, and Z. Shukur, "Detecting abnormal behavior in social network Websites by using a process mining technique," J. Comput. Sci., vol. 10, no. 3, pp. 393-402, 2014.

[2] M. Al-Qurishi, M. S. Hossain, M. Alrubaian, S. M. M. Rahman, and A. Alamri, "Leveraging analysis of user behavior to identify malicious activities in large-scale social networks," IEEE Trans. Ind. Informat., vol. 14, no. 2, pp. 799-813, Feb. 2018

[3] Jianyu Miao, Lingfeng Niub, "A Survey on Feature Selection, " Information Technology and Quantitative Management (ITQM 2016).

[4] Phillip G. Efthimion1, Scott Payne1, Nick Proferes2, "Supervised Machine Learning Bot Detection

Techniques to Identify Social Twitter Bots ", Master of Science in Data Science, Southern Methodist University,6425 Boaz Lane, Dallas, TX 75205, 2018.

[5] S. Barbon, Jr., G. F. C. Campos, G. M. Tavares, R. A. Igawa, M. L. Proença, Jr., and R. C. Guido, "Detection of human, legitimate bot, and malicious bot in online social networks based on wavelets," ACM Trans. Multimedia Comput., Commun., Appl., vol. 14, no. 1s, Feb. 2018, Art. no. 26.

[6] F. Morstatter, L. Wu, T. H. Nazer, K. M. Carley, and H. Liu, "A new approach to bot detection: Striking the balance between precision and recall," in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining, San Francisco, CA, USA, Aug. 2016, pp. 533-540.

[7] Y. Zhou et al., "ProGuard: Detecting malicious accounts in social network based online promotions," IEEE Access, vol. 5, pp. 1990-1999,2017.

[8] Xuan Dau Hoang and Quynh Chi Nguyen, "Botnet Detection Based On Machine Learning Techniques Using DNS Query Data"

[9] C. K. Chang, "Situation analytics: A foundation for a new software engineering paradigm," Computer, vol. 49, no. 1, pp. 24-33, Jan. 2016.

[10] Efthimion, Phillip George; Payne, Scott; and Proferes, Nicholas (2018), "Supervised Machine Learning Bot Detection Techniques to Identify Social Twitter Bots," SMU Data Science Review: Vol. 1 : No. 2 , Article5.

[11] Ranjana Battur, Nagaratna Yaligar, " Twitter Bot Detection using Machine Learning Algorithms, " International Journal of Science and Research (IJSR) ISSN: 2319-7064 ResearchGate Impact Factor (2018): 0.28 — SJIF (2018): 7.426

[12] C. Cai, L. Li, and D. Zengi, "Behavior enhanced deep bot detection in social media," in Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI), Beijing, China, Jul. 2017, pp. 128-130.