International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Detection of Malicious Bots in Twitter Using Machine Learning Algorithms

Mr R Mathiyalagan [1], Shaik Shoaib Akthar [2] , Somanna Ms[3] , Shaik Jaffar[4] , S Radha Krishna [5], Shamanth H[6]
[6]Assistant Professor [1] , UG Students [2,3,4,5,6]
Computer Science Department, Presidency University, Bengaluru, Karnataka, India

ARTICLEINFO

Article History:

Accepted: 01 May 2023
Published: 23 May 2023

Publication Issue
Volume 9, Issue 3
May-June-2023

Page Number
216-222

ABSTRACT

Unwanted social bots have become more pervasive as robotized social entertainers because of the development of web administrations and the ubiquity of online informal organizations (OSN) like Facebook, Twitter, LinkedIn, and so on. These players can assume a variety of malevolent roles, such as intruders into human discussions, con artists, imposters, spreaders of false information, manipulators of the stock market, astroturfers, and any content polluters (spammers, virus spreaders, etc.). Social bots are undeniably quite important on social networks. The RNN algorithm feeds the output of the previous step as input to the current step in order to detect these harmful social bots in social networks. Comparing this algorithm to all other machine learning algorithms, it has a high detection accuracy rate. Therefore, this study examines detection strategies within a methodological category, highlights the possible risks of malevolent social bots, and suggests lines of future research.

Keywords : RNN, malicious social bots, online social networks (OSNs).

I. INTRODUCTION

Everyday life is becoming increasingly dominated by social media. Given the billions of clients who produce and consume data consistently, it just seems OK that individuals could utilize this medium to peruse and share the news. Computer programs known as "social media bots" are capable of influencing human behavior while carrying out a wide range of beneficial and harmful activities on social media platforms. Web-based entertainment bots shift in size contingent upon their ability, plan, and capability. Some social media bots offer services like weather updates and sports scores. Clients who interface with these proficient virtual entertainment bots know about this since they can rapidly distinguish them in that capacity. In any case, numerous virtual entertainment bots take on the appearance of real individuals and spread infections. Users lose faith in the ability of social media platforms to accurately relay news as a result of these bots, and they become suspicious that the press releases at the top of their feeds were "pushed" there by dishonest bots. Malicious individuals, such as bots, have begun to steer online debates in the direction that their creators prefer as a result of the growing number of people who use social media.

These exploitative bots have been utilized to spread bogus data about political competitors, misrepresent big names' apparent ubiquity, smother activists' and protestors' messages, take part in unlawful promoting by flooding web-based entertainment with connections to for-benefit sites and slow down monetary business sectors to attempt to change stock costs. Additionally, these bots have the power to change the results of successive social media inspections. In order to stop these malicious activities in social media we are using RNN algorithm. It is an artificial neural network with a sequential information structure. These algorithm uses previous step output in order to get the output for present or current step. RNNs are loop based networks that enable data preservation.

In order to imitate human activity on social media sites, automated accounts are known as social bots. It may be used to propagate false information or promote products, among other things. It is crucial to identify dangerous social bots since they may significantly affect information distribution and user experience on websites like twitter. Utilizing recurrent neural networks is one method of spotting dangerous social bots on Twitter (RNNs). An artificial neural network called an RNN is ideally suited for handling sequential data. B. An online Twitter feed of tweets. We can identify the traits of a social bot by teaching an RNN on a dataset of tweets. Using this information, we can categorize new tweets as being created by bots or by humans.

The issue of employing RNNs to identify dangerous social bots on Twitter may be solved in a number of ways. RNNs are a popular method for determining if a tweet was sent by a machine or a person. It is founded on a variety of characteristics taken from tweets.

These traits might include the usage of certain hashtags, the inclusion of links to other websites, or the regularity of posting. Then, using these characteristics, an RNN can be taught to forecast whether a class belongs to a bot or a person.

Another way to identify risky social bots on Twitter is to use RNNs to analyze tweet content rather than their attributes. For example, an RNN could be prepared to classify tweets composed by bots or others in light of the language they use. This contrasts with the tone of the tweet. Utilizing RNNs makes it easy to identify dangerous Twitter social bots and reduce their influence. On Twitter, automated accounts known as malicious social bots are used to spread spam, false information, or propaganda. They are also known as "malicious Twitterbots." There are many reasons why a malicious social bot could be created and used on Twitter. Common reasons include.

Spamming: Malicious Twitter bots can be used to send a lot of spam messages or links to websites in an effort to promote a product or service.

Misinformation: Threatening Twitter bots can be used to spread counterfeit or deluding information to affect general appraisal or control the web-based conversation.

Propaganda: Malicious Twitter bots can be used to spread false information or advance a specific political objective.

Disinformation: Twitter bots that are malicious can be used to spread false information, which is information that is sent with the intention of deceiving or misleading others.

Influence: Vindictive Twitter bots can be utilized to attempt to impact the internet-based discussion or to control popular assessment by flooding virtual entertainment with counterfeit records or computerized messages.

There are several approaches that can be taken to overcome malicious social bots on Twitter using machine learning and specifically using Recurrent Neural Networks (RNNs). Some potential approaches include.

Bot detection: By studying the patterns of activity and behavior of the relevant accounts, RNNs may be applied to create models that can detect and identify dangerous Twitterbots.

Designing highlights: RNNs can be used to determine the most relevant variables, such as the substance of tweets, the frequency of tweeting, and so on, that can be used to distinguish between true and false data.

Classification: After the relevant properties have been discovered, RNNs can be used to build models that can classify accounts based on their behavior and activity on the site as genuine or malicious.

Error detection: RNNs might be utilized to detect deviations or odd examples of conduct that can highlight the presence of a noxious Twitterbot.

Filtering: Models made with RNNs can be used to exclude or flag potentially malicious accounts or content for further examination.

It is important to note that overcoming malicious social bots on Twitter is a complex task that requires a combination of technical and non-technical approaches. In addition to using machine learning techniques like RNNs, it is also important to have policies and procedures in place to identify and address malicious activity on the platform.

II. RELATED WORKS

Bot detection in social media: A Machine Learning approach (2019)

On this project, the authors proposed a machine learning approach for detecting bots on social media platforms. The proposed method uses features such as user behavior, content, and network features to detect bots. They used a Twitter dataset to evaluate the proposed method. The advantages are high accuracy in bot detection, ability to handle multiple types of bots, and efficient feature selection. The limitations are the need for labeled training data and the sensitivity of the proposed method to changes in social media platform policies.

Anomaly Detection and Bot Identification in Social Networks (2019)

On this project, the creators proposed a strategy for recognizing bots in interpersonal organizations in view of their odd way of behaving. Anomalies in the behavior of social media users can be identified using the proposed method, which makes use of machine learning and graph analysis techniques. They used a Facebook dataset to evaluate the proposed method. The advantages are high accuracy in bot detection, ability to handle different types of bots, and the ability to detect emerging bot threats. The limitations are the need for labeled training data and the sensitivity of the proposed method to changes in social network behavior.

Detecting Malicious Bots in Social Media Using Machine Learning (2020)

The creators of this study suggested employing machine learning to identify dangerous bots on social media networks. The proposed strategy employs user behavior, network topology, and user profiles as characteristics to identify bots.

They tested the suggested approach using a dataset from Twitter. The benefits include the capacity to handle many bot kinds, high accuracy in bot verification, and real-time bot detection. The constraints include the requirement for labeled training data and the requirement to routinely update the model to address new bot threat scenarios.

A Machine Learning Approach for Malicious Bot Detection on Social Media (2021)

The creators of this study suggested using machine learning to identify dangerous bots on social media networks. The recommended method detects bots by utilizing elements including user behavior, content, and network properties. They used a Twitter dataset to evaluate the proposed method. The advantages are high accuracy in bot detection, ability to handle different types of bots, and the ability to detect bots in real-time. The limitations are the need for labeled training data and the need to update the model periodically to handle emerging bot threats.

A Review of Machine Learning Approaches for Email Spam Filtering (2019)

In this project, the authors review various machine learning approaches for email spam filtering. They categorize the approaches into three groups: rule-based,

content-based, and hybrid. They discuss the advantages and disadvantages of each approach and compare their effectiveness. The authors also present a detailed analysis of the datasets used for evaluating these approaches. The advantages of rule-based methods include easy maintenance, while the disadvantages include low accuracy due to limited rules.

Content-based methods offer high accuracy by analyzing the content of the email, but they may be susceptible to feature selection bias. Hybrid approaches combine rule-based and content-based methods to improve accuracy and reduce false positives. The authors conclude that machine learning approaches are effective in email spam filtering and that hybrid approaches are the most promising due to their high accuracy and low false positive rates. They also identify several areas for future research, including improving feature selection and exploring new approaches such as deep learning.

III. METHODOLOGY

Proposed system:

Detecting malicious bots on Twitter using a recurrent neural network (RNN) architecture involves several steps. Here is a diagram that outlines the process:

- **Data collection:** The first step is to collect data from Twitter. This includes both bot and human accounts.
- **Data preprocessing:** The collected data is then preprocessed, which involves cleaning and formatting the data to ensure it is suitable for analysis.
- **Feature extraction:** Next, features are extracted from the data. These features are used to train the RNN model and include things like tweet frequency, tweet content, and account activity.
- **RNN training:** The RNN model is then trained using the extracted features. The model is trained to differentiate between bot and human accounts based on the extracted features.
- **Model evaluation:** Once the RNN model is trained, it is evaluated to determine its accuracy in detecting bot accounts. This involves testing the model on a separate dataset that was not used during training.
- **Bot detection:** Finally, the trained RNN model is used to detect malicious bot accounts on Twitter. The model analyzes the features of each account and determines if it is a bot or human account.

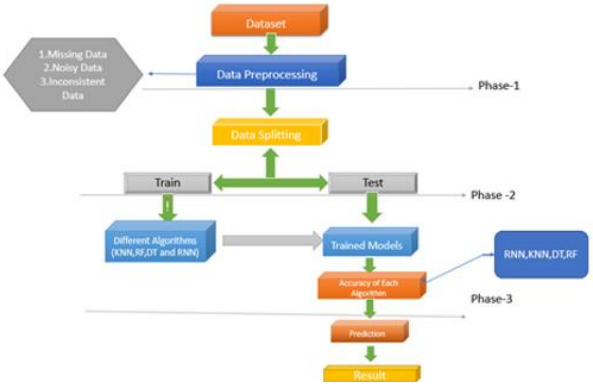

Fig. Physical model

In order to detect malicious social bots in twitter with better accuracy rate we proposed a RNN algorithm which is an artificial neural network with a sequential information structure. They are referred to as recurrent because they execute the same function on each sequence element, with the outcome depending on prior calculations. RNNs are loop based networks that enable data preservation.

IV. IMPLEMENTATION

The project has implemented by using below listed algorithm.

KNN:

- One of the most straightforward AI calculations, in light of the regulated learning technique, is K-Closest Neighbor.

- The K-NN technique puts the new case in the class that is most tantamount to the accessible classifications, in all actuality the new case/information and the current cases are comparable.
- The K-NN algorithm saves all of the data that is available and uses similarity to classify new data. This intends that by conveying the K-NN strategy, new information might be rapidly and precisely arranged into a reasonable class.
- Although the K-NN method can be utilized for both classification and regression tasks, classification tasks are where it is most frequently used.
- Because it is a non-parametric algorithm, K-NN does not make any fundamental assumptions about the data. It is also known as a lazy learner algorithm because it does not immediately learn from the training set. All things being equal, while ordering information, it stores the dataset and makes a move on it.
- The KNN algorithm simply saves the dataset during the training phase, and when it receives new data, it places it in a category that is very similar to the new data.

Random Forest:

First, N decision trees are combined to generate the random forest, and then predictions are made for each tree that was produced in the first phase. The stages listed below can be utilized to demonstrate the working process.

Step 1: Pick K data points at random from the training set.

Step 2: Create the decision trees linked to the subsets of data that have been chosen.

Step 3: Select N for the size of the decision trees you wish to construct.

Repeat steps 1 and 2 in step 4.

Support Vector Machine (SVM):

The primary function of the SVM is to find an ideal hyperplane for various unique cases in a high-dimensional space. Multiple hyperplanes exist to realize this paradigm. This procedure is dependent on the support vector, which is the data that corresponds to the ideal choice surface and is located closest to the closed surface. It carries out classification by generating a hyperplane to divide the data and planning the input vectors into a high-dimensional space. This approach is mostly used to resolve non-convex, unconstrained minimization problems and quadratic programming problems. The SVM is the classifier process's most successful technique.

V. RESULTS AND DISCUSSION:

The suggested work is implemented in Python 3.6 using the sklearn library, pandas, matplotlib, and other necessary tools. The study will take into account the bot detection dataset that was acquired from Kaggle. Utilized were machine learning algorithms like RNN, KNN, SVM and Random Forest. To forecast the bot detection, these machine learning methods were employed. We developed the code by using all the four algorithms to get better accuracy among all the algorithms. The outcome demonstrates that RNN produces better accuracy among those four algorithms. RNN produces 99.866, whereas KNN, SVM, Random Forest produces 92.110, 95.900, 93.900 respectively.

The following images will visually depict the process of our project.

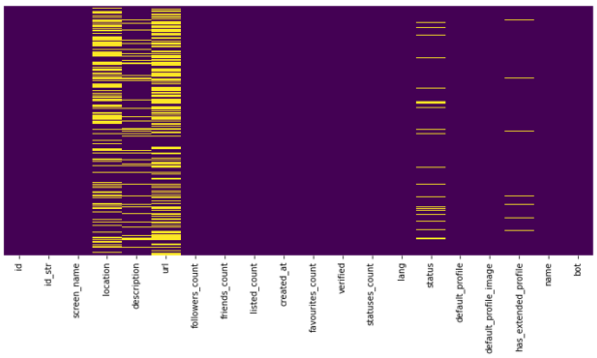

Fig 4.1. Heat map of training dataset

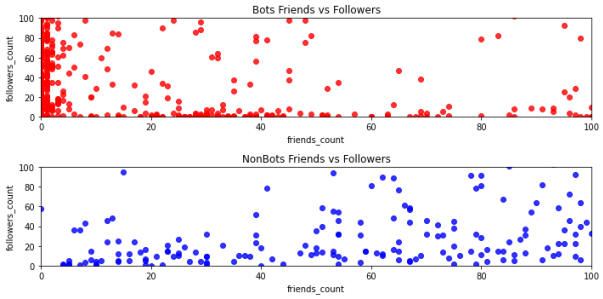

Fig 4.2. Bots and Non-Bots in Followers

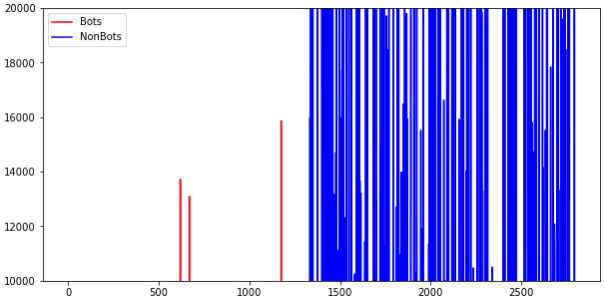

Fig 4.3. Bots and Non Bots

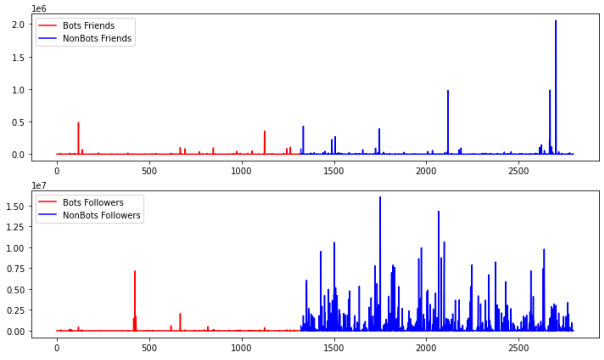

Fig 4.4. Bot and Original Accounts

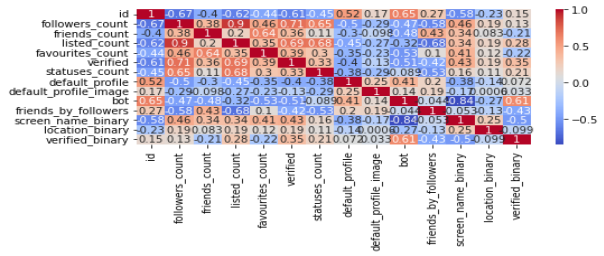

Fig 4.5. Seaborne Heat map for Visualizing Data

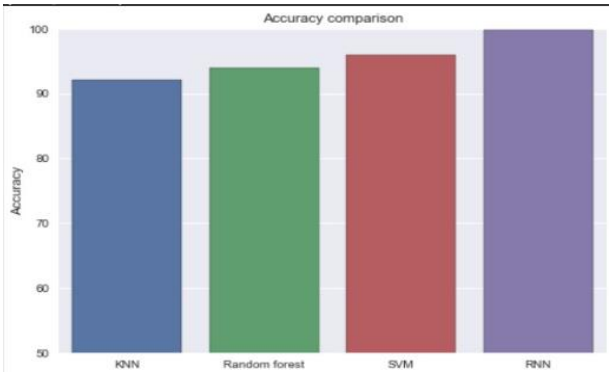

Fig 4.6. Accuracy comparison between RNN and other algorithms

	Agorithms	accuracy
0	KNN	92.110
1	Random forest	93.900
2	SVM	95.900
3	RNN	99.866

Fig 4.7. accuracy

VI. CONCLUSION

In conclusion, the use of RNN for detecting malicious bots in Twitter is a promising approach to combat bot activity and maintain the integrity of the platform. RNN models are suitable for analyzing sequential data such as tweets and can learn to recognize patterns and characteristics of bot-generated tweets. However, it requires a large labeled dataset of tweets, which should be preprocessed before feeding into the RNN model. The trained RNN model can be used to classify new tweets as either human-generated or bot-generated. Although there are still challenges and limitations to this approach, such as handling variations in bot activity and the possibility of adversarial attacks, it shows great potential in improving the detection and mitigation of malicious bots on Twitter. As Twitter

continues to be a critical platform for communication and information sharing, efforts to combat bot activity are crucial to maintain the integrity and trust of the platform.

VII.REFERENCES

[1]. Xie, K., Yang, L., & Liu, C. (2021). Bot detection in social media: A survey. Journal of Network and Computer Applications, 186, 103031.

[2]. Lee, C., Lee, J., & Lee, K. (2020). Detection of social bots on social media: A survey. ACM Computing Surveys (CSUR), 53(4), 1-34.

[3]. R. Alqurashi and A. Mahmood are the authors. Techniques for spotting malicious bots in social networks online: a summary. 94, 101870, Computers & Security.

[4]. Jung, J., Park, H., and Lee, J. (2018). A review on the discovery of pernicious records in virtual entertainment. 14(5), 1005-1018, Journal of Information Processing Systems.

[5]. Wang, X., Yang, Y., Li, Y., & Jiang, C. (2020). A review on malicious bot detection in social networks. Journal of Ambient Intelligence and Humanized Computing, 11(9), 3839-3850.

[6]. Fardoun, H. M., & Al-Rahmi, W. M. (2019). Social bot detection: A review. IEEE Access, 7, 141906-141922.

[7]. Nguyen, T. T. H., Nguyen, L. V., & Hwang, D. (2020). A comprehensive survey of social bot detection using machine learning. Future Generation Computer Systems, 102, 1269-1284.

[8]. Chavoshi, N., &Hamooni, H. (2017). Twitter's detection of malicious social bots: An AI approach. Diary of Canny Data Frameworks, 49(3), 541-566.

[9]. "Detecting Malicious Bot Accounts in Online Social Networks Using SVM and Random Forests" by Hani Alshahrani and Ali Almohammad.

[10]. "Detecting Malicious Accounts in Social Networks Using a Multi-Objective Optimization Algorithm" by Wei Hu, Yunchao Tian, and Fei Wang.

[11]. "Detecting Malicious Accounts in Social Networks Using Convolutional Neural Networks" by Han Liu, Xuefeng Li, and Wei Wang.

Cite this article as :

Mr R Mathiyalagan, Shaik Shoaib Akthar, Somanna Ms, Shaik Jaffar, S Radha Krishna, Shamanth H, "Detection of Malicious Bots in Twitter Using Machine Learning Algorithms", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.216-222, May-June-2023.