International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 3 ǁ March 2023 ǁ PP. 442-445

Detection of Malicious Social Bots

Prof. Ravindranath R C Assistant Professor
Computer Science and Engineering DepartmentGlobal Academy of Technology Bangalore, India
1. Tejashwini C *Computer Science and Engineering Department Global Academy of Technology Bangalore, India*
2. Vatsala M *Computer Science and Engineering DepartmentGlobal Academy of Technology Bangalore, India*

Abstract*— *Social bots are the programs which does the task autonomously. These malevolent social bots perform the various phishing activities such as creating false identities, acts like a follower andmakes to believe that they are genuine users. Moreover, several malevolent attacks are executed by social bots, such as spreading junk content, generating false personalities and also performs social violence. When a person wants to share contents via URL their arises need to shorten the URL in order to share the information with other users which may involve malevolent activities such as redirecting to malicious sites, so it becomes very vital to distinguish between malevolent and real user. Detection of malicious social bots is done by extracting URLcharacteristics. Malicious social bot detection algorithm contains two parts, direct trust which is done using Bayes theorem, which is used calculate the probabilities with uncertainty and indirect trust using DST, which combines bits of information to calculate the probability of occurrence.

Keywords*— *Malevolent, Social bots, and Detection

Date of Submission: 10-03-2023 Date of acceptance: 23-03-2023

I. INTRODUCTION

Malicious social bot imitates to be legitimate user. Moreover, several malevolent attacks are executed by social bots, such as spreading junk content, generating false personalities and also performs social violence. When a person wants to share contents via URL their arises need to shorten the URL in order to share the information with other users which may involve malevolent activities such as redirecting to malicious sites so it is vital to distinguish between malevolent and real user.

Various methods have been seen in detecting spam. These methods use features which can be manipulated very easily in order to not get identified as malevolent URL which inspired us to ruminate the learning techniques to control temporal data arrangements. We have devised an model to detect malicious social bots, which analyses malevolent behavior by considering URL features which can identify malevolent URL even when it can redirected to other sites, Analyze the malevolent behavior of the participant by seeing URL-based structures such as relative position URL,URL redirection, frequency and junk content in the URL and thenevaluate the trustworthiness of the tweets.

Detection of Malicious Social Bots

Online users can read tweets, post tweets, scroll through the timeline all these data will be collected and stored and from these data certain features will be extracted such as lexical properties of URL, domain length, special characters of URL which in turn will distinguish between malicious and legitimate users. Malicious social bot detection algorithm contains two parts, direct trust which is done using Bayes theorem, which is used calculate the probabilities with uncertainty and indirect trust using DST, which combines bits of information to calculate the probability of occurrence and distinguish malevolent user and real user.

II. LITERATURE SURVEY

"Detecting malicious social bots based on clickstream sequences" which was published inyear 2019. A method of detecting malevolent social bots, based on the conversion likelihood of clickstream sequences and semi-supervised clustering.

"Adaptive deep Q-learning model for detecting social bots and influential users in online social network" which was published in year 2019. A deep Q-network architecture by incorporating a Deep Q- Learning model based on apprising function.

"A neural network-based ensemble approach for spam detection in Twitter" which was published in year

2018.Incorporated several deep learning models based on CNNs.

III. METHODOLOGY

I. Data Collection:

This first step in Detection of Malicious Social Bots is collection of data.
In our case data is taken from Kaggle. This dataset contains three different columns:
ID, Label and URL. Label specifies whether the given URL is malicious or not in the given dataset.

II. Pre-processing:

The following steps in pre-processing are: URL features will be extracted and then will be split into tokens by using tokenizer.

III. Feature Selection:

A classification algorithm is used in feature selection. In this case we are using Logistic regression. It is a classification algorithm which can be used for fraud detection. When the data contains binary output Logistic regression is usually used.

IV. Applying Algorithms

A. Random Forest Algorithm: It is made upon a decision tree to expand the accurateness significantly. Randomforest produces many naïve decision trees and uses the "majority vote" system to determine on what label to send. Classification is done based on label which has received more votes whereas Average prediction is final prediction in regression task.

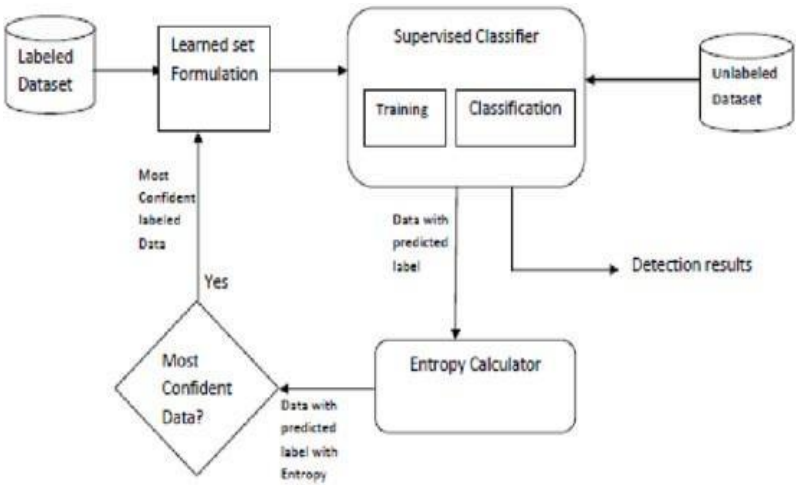
B. CNN (Convolution Neural Network):
CNNis a subclass of Machine Learning. this is oneof various artificial neural network models that makes of data sets. It is used for image identification.

V. Connection Part

Flask is a Web Application Flask in python. HTML and CSSare used with flask which presents the contenton the web page. Conditions for placement ofhtml elements is given by CSS. Inputs can begiven by users. After receiving the input, values from the html elements are taken by the flask functions and data frame is created, based on which the model is trained and basedon the output received various web page which tells whether the URL is malevolent or not.

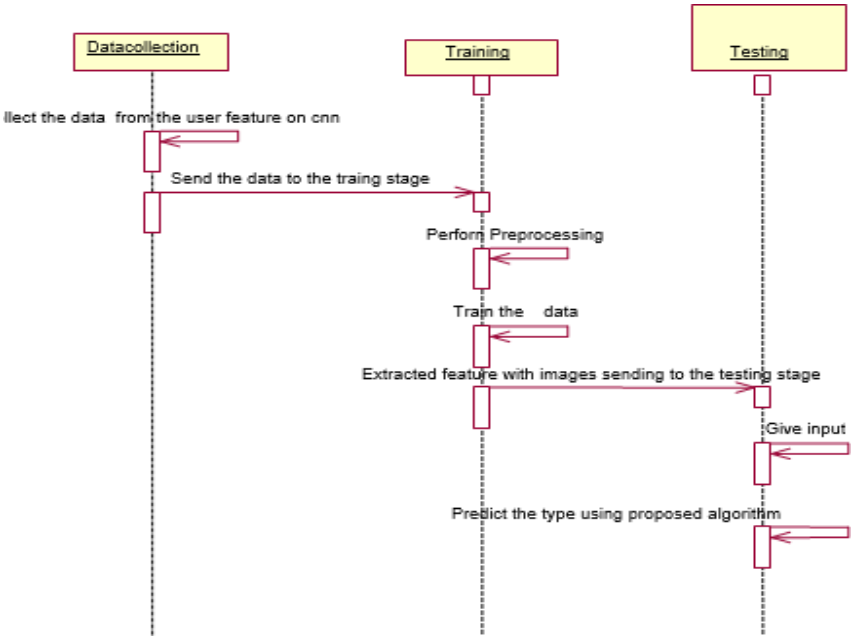
System Design

1. System Architecture

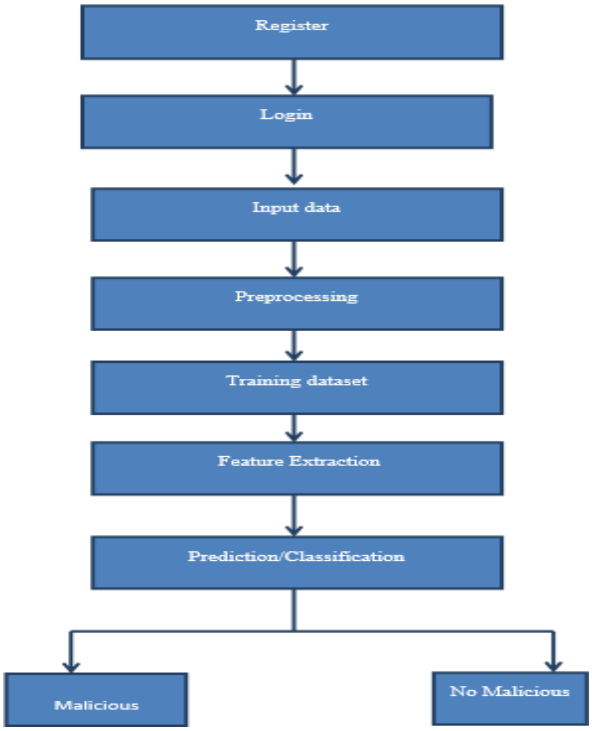


The labelled data is taken from the dataset. Training is done using the labelled data. Testing is done using unlabeled. Output from the testing is taken and is inserted to labelled data. The "learned set formulation" facilitates to eliminates redundancy in labelled data and controls size. Entropy is used for assortment of specific data from test data and which filters test data and add to training set and then data will be finally classified whether it is malicious or not.

2. Sequence Diagram:

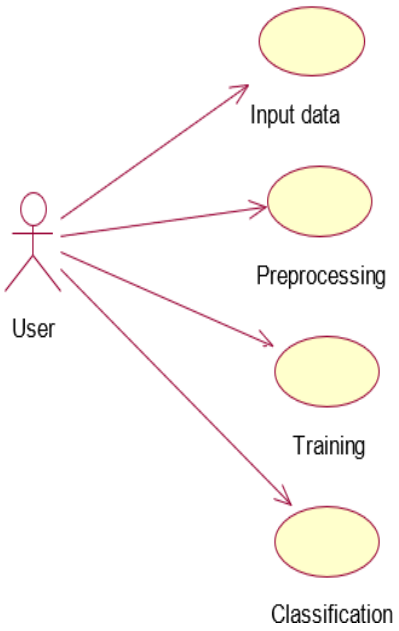


3. Data Flow Diagram



The data flow diagram (DFD) explains the flow of the system. As user enters the system it asks for the user to register and then login. After providing the input, it will be pre-processed (The following steps in pre-processing are: URL features will be extracted and then will split tokens by using vectorizer.), and the system will be trained and the URL features will be extracted after whichthe system classifies whether the given URL as input is maliciousor not.

4. Use Case Diagram:



This diagram delivers graphical outline of the system functionality. System asks user for input, it will be pre-processed, and the system will be trained, and the URL features will be extracted after whichthe system classifies whether the given URL as input is malicious or not.

IV. EXPECTED RESULTS

Considering the results of the Existing papers we proposed model using Bayesian learning and DST. Given the input, system will classifywhether the URL is malicious or not. Malicious social bot detection algorithm contains two parts, direct trust which is done using Bayes theorem, which is used calculate the probabilities with uncertainty and indirect trust using DST, which combines bits of information to calculate the probability of occurrence.

V. CONCLUSIONS

The malicious activities of applicants are examined by extracting the URLcharacteristics, such as relative position URL, URL redirection, frequency, and junk content in the URL. Malicious social bot detection algorithm incorporates two factors, direct trustwhich is done using Bayes, theorem and indirect trust using DST. Malicious social bot detection algorithm contains two parts, direct trust which is done using Bayes theorem, which is used calculate the probabilities with uncertainty and indirect trust using DST, which combines bits of information to calculate the probability of occurrence.

REFERENCES

[1]. P. Shi, Z. Zhang, and K.-K.-R. Choo, "Detecting malicious social bots based on clickstream sequences," IEEE Access, vol. 7, pp. 28855–28862, 2019.
[2]. G. Lingam, R. R. Rout, and D. V. L. N. Somayajulu, "Adaptive deep Q-learning model for detecting social bots and influentialusers in online social networks," Appl. Intell.,vol. 49, no. 11, pp. 3947–3964, Nov. 2019.
[3]. D. Choi, J. Han, S. Chun, E. Rappos, S. Robert, and T. T. Kwon, "Bit.ly/practice: Uncovering content publishing and sharing through URL shortening services," Telematics Inform., vol. 35, no. 5, pp. 1310– 1323, 2018.
[4]. S. Madisetty and M. S. Desarkar, "A neural network-based ensemble approach for spam detection in Twitter," IEEE Trans.Comput. Social Syst., vol. 5, no. 4, pp. 973–984, Dec. 2018.
[5]. H. Gupta, M. S. Jamal, S. Madisetty, and M. S. Desarkar, "A framework for real-time spam detection in Twitter," in Proc. 10th Int.Conf. Commun. Syst. Netw. (COMSNETS),Jan. 2018, pp. 380–383.