International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

DETECTION OF MALICIOUS SOCIAL BOT USING DEEP LEARNING

Poonguzhali E[1], Agila M[2], Haripriya K[2], Pavithra R[2], Thelagavathe S[2]

[1]Assisstant Professor, Sri Manakula Vinayagar Engineering College, Puducherry
[2]Sri Manakula Vinayagar Engineering College, Puducherry

Abstract - *Malicious social bots are a very common issue in online social networks. These malicious social bots are being used for a number of purposes such as artificially amplifying the popularity of a person or movement, influencing elections, manipulating financial markets, amplifying phishing attacks, spreading spam, and shutting down free speech. Therefore detection of these bots in online social networks is of great importance. Social media platforms are unable to apply more stringent requirements for account creation because for a variety of reasons such as it may prevent some legitimate users from signing up, it will lack the ability to maintain some anonymity for protestors under oppressive regimes, it may cause inconvenience to real users(CAPTCHAs are a good deterrent against bots, but it causes inconvenience for the humans). So alternatively machine learning algorithms were used to detect these malicious social bots. In this paper, we have proposed a faster RCNN algorithm and ResNet algorithm in order to increase the accuracy of detection.*

Key Words*: *Malicious social bot, Phishing, online social network, faster RCNN, ResNet

1.INTRODUCTION

Social media has played a more important role in our daily life. With billions of users producing and consuming information every day, it is a natural extension that people turn to this medium to read and disseminate news. Social media bots are programs that vary in size depending on their function, capability, and design and can be used on social media platforms to do various useful and malicious tasks while stimulating human behaviour. Some social media bots provide useful services, such as weather updates and sports scores. These good social media bots are clearly identified as such and the people who interact with them know that they are bots. However a large number of social media bots are malicious bots disguised as human users. These bots cause users to lose trust that social media platforms can deliver news honestly, as they become suspicious that the stories they see at the top of their feeds were "pushed" there by manipulative bots. With so many people turning to social media, malicious users like bots have begun to sway the conversations in whatever direction their creators want .These malicious bots have been used for malicious tasks such as spreading false information about political candidates , inflating the perceived popularity of celebrities, deliberately pushing down the messages of protestors and activists, illicitly advertising by spamming the social web with links to commercial websites and influencing financial markets in an attempt to manipulate the direction of stock prices. Furthermore, these bots can change the results of common analyses performed on social media. Some of the common attack methods of social media bots are: sleeper bots-they remain dormant for long periods of time, then wake up to launch their attack of thousands of posts in a short period of time(perhaps as a spam attack),and then return to a dormant state, trend jacking -use of top trending topics to focus on an intended audience for targeting purposes, watering hole attack-attacker guesses or observes which websites an organization often uses and infects one or more of them with malware, hashtag hijacking-use of hashtags to focus an attack(e.g. spam ,malicious links)on a specific audience using the same hashtag and click farming or like farming-inflate fame or popularity on a website through liking or reposting of content via click farms. Bot detection is an important task in social media. Twitter, a popular social media platform, is plagued by automated accounts. Some studies estimated that around 15% of the accounts on Twitter Operates Automatically or Semiautomatically. One reason which might have stimulated the rise of the number of bots is the characteristics of Twitter. Moreover, it is worth mentioning that a bot on Twitter is regarded as a credible source of information. In addition to this, bot operated accounts can be 2.5 times more influential than human operated accounts. Malicious bots have been able to influence measures on Twitter, including the trending topics. These bots can also influence statistics performed on Twitter data, such as the top hashtags and the most important users in the data. Traditionally, the detection of malicious social bots are done through the usage of blacklisting methods. These are essentially lists of URLs collected by anti-virus groups which are known to be malicious. While these methods are fast (requiring a simple database lookup), and are expected to have low False Positive rates, a major shortcoming is that they fail against newly generated URLs. This is a severe limitation as new URLs are generated everyday. To address these limitations, there have been several attempts to solve this problem through the use of machine learning.

2. BOTS

Internet bots, also known as web robots, WWW robots or simply bots, are software applications that run automated tasks over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web spidering, in which an automated script fetches, analyzes and files information from web servers at many times the speed of a human. Each server can have a file

called robots.txt, containing rules for the spidering of that server that the bot is supposed to obey. In addition to their uses outlined above, bots may also be implemented where a response speed faster than that of humans is required (e.g., gaming bots and auction-site robots) or less commonly in situations where the emulation of human activity is required.

3. RELATED WORK

In [1] Sneha Kudugunta, Emilio Ferrara (2018) proposed a deep neural network based on contextual LSTM (Long Short-Term Memory) architecture allowing the use of both tweet content and metadata to detect bots at the tweet level. The contextual features are extracted from user metadata and fed as auxiliary input to LSTM deep nets processing the tweet text. From a single tweet, the model can achieve an extremely high accuracy exceeding 96% AUC.They also proposed methods based on SMOTE (Synthetic Minority Oversampling Technique) that yield a near perfect user-level detection accuracy (> 99% AUC) to enhance existing datasets by generating additional labeled examples. Both these methods use a very minimal number of features that can be obtained in a straightforward way from the tweet itself and its metadata. The system outperforms previous state of the art while leveraging a small and interpretable set of features yet requiring minimal training data.

In [2] Mohammed AL - Janabi, Ed de Quincey, Peter Andras (2017) proposed a supervised machine learning classification model to detect the distribution of malicious content in online social networks (ONSs). The multi-source features have been used to detect social network posts that contain malicious Uniform Resource Locators (URLs). These URLs could direct users to websites that contain malicious content, drive-by download attacks, phishing, spam, and scams. For the data collection stage, the Twitter streaming application programming interface (API) was used and Virus Total was used for labelling the dataset. A random forest classification model was used with a combination of features derived from a range of sources. The random forest model without any tuning and feature selection produced a recall value of 0.89. After further investigation and applying parameter tuning and feature selection methods, however, we were able to improve the classifier performance to 0.92 in recall.

In [3] Chongzhen Zhang, Yanli Chen, YangMeng (2020) proposed A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques. We propose a novel intrusion detection framework to improve classification capabilities. Simultaneously, the retraining of the classifier in the classification module is realized through the database module and the feedback module so as to ensure the high accuracy rate of the classification module continuously. We developed a novel classification method by combining SAE and RF. Our approach realizes the potential of effective representation and dimensionality reduction to improve the classification results for traditional ML algorithms in binary and multiclass classification. We take full use of the characteristics of the SAE model, combined with the feature library in the database module, to restore the flow before compression, which can be used for post event analysis and forensics. We evaluate our proposed framework using the CICIDS2017 dataset and give the training and testing times. Compared with different methods in the related work using the same dataset, we have achieved the best value in the binary and multiclass classification.

In [4] Sylvio barbon JR,Gabriel F.C.Campos,Gabriel M.Tavares(2018) proposed a Detection of Human, Legitimate Bot, and Malicious Bot in Online Social Networks Based on Wavelets. The proposed approach was modeled in five steps: Acquisition, Profiling Setup, Features Extraction, Feature Selection, and Classification. Our model is suitable to any OSN, i.e., the Acquisition step can be adapted according to each OSN API. Classification step is also flexible. In this work, we adopted Random Forests (RFs) as classifiers. This choice was based on works such as Singh et al. (2014) and del Río et al. (2014), which reported good results by applying RFs in big data environments and Igawa et al. (2016) that treats specifically bots on OSNs. We have proposed an algorithm for classifying authors as being a human, a legitimate robot, or a malicious robot, in OSNs. The algorithm was based on Discrete Wavelet Transform to obtain a pattern of writing style embedded in post contents. Experiments have been conducted by classifiers with two different datasets: single and miscellaneous theme. It was observed that the proposed method yields the high average classification accuracies of 94.47% for both datasets. Considering the results, the text-based model we have developed gives promising accuracies in classifying the user type based on its writing style. We believe that the proposed algorithm can be very helpful to combat frauds in OSN. Further exploration of different machine-learning approaches can yield more interesting results.

In [5] Greeshma Lingam, Rashmi Ranjan Rout and DVLN Somayajulu(2018) proposed a Detection of Social Botnet using a Trust Model based on Spam Content in Twitter Network. We first present a trust model based on spam content for determining the trust value among participants in Twitter network. Further, a social botnet detection algorithm has been proposed by incorporating a trust model for identifying a trustworthy path in Twitter network. We analyze the malicious behavior of n participants (in Twitter network) for social botnet detection through a direct trust computation. The indirect trust is evaluated based on the recommended one-hop neighboring participants. If the direct observation is only considered then there could be an ambiguity in evaluating trust value. In this paper, Dempster-Shafer theory (DST) has been adopted to combine multiple supporting evidences that are provided by multiple one-hop neighboring participants. This theory is based on important concept called belief. We propose a social botnet detection algorithm by incorporating trust model in order to detect the social bots in Twitter network. , the performance of the proposed model is analyzed by incorporating direct and indirect trust parameters.

In [6] Xia Liu, (2019) proposed a big data approach to examining social bots on Twitter. In this section, we present details on the Twitter data set, sampling, sentiment analysis and econometric modeling. We explain why Twitter is a uniquely valuable social network for investigating social bots and discuss the importance of the sample data in understanding information distortion and diffusion by bots. As sentiment analysis plays a pivotal role in quantifying unstructured big data in this study, we introduce maximum entropy, the steps in training and testing of the Examining social bots based on the metrics for evaluating model accuracies. In the end, we present important findings on social bots from an econometric analysis of the weekly panel data set. Twitter is a viable platform to study social bots and big data of user-generated content, further insights from other platforms, such as Facebook, will broaden our understanding of how social bots can impact information quality and virality. Second, sentiment analysis is a helpful tool for automatically classifying textual big data, but it has some inherent limitations due to the complexities and intricacies of human language.

In [7] Linhao Luo, Xiaofeng Zhang, Xiaofei Yang and Weihuang Yang(2019) The proposed Deepbot contains two components: a trained Twitter bot classifier and a Web interface developed using Web service for public access. 3.1. Twitter Bot Classifier The Twitter bot classifier is proposed based on a deep neural network model to determine whether the input tweet is posted by a bot or not. To represent the textual features of tweets, first, we embed the tweets into vectors using the Global Vectors for Word Representation (GloVE) [8]. This pre-trained word embedding matrix is denoted as E ∈ R|e|×|V |, where |e| denote the length of each word after embedding and |V | is the total number of vocabulary V. Let D denote the number of words in the i-th tweet (Si). Then, each tweet Si could be embedded as a matrix S RD×|e| by replacing all the words with the corresponding word vector v in E. The proposed Deepbot customizes the Bi-directional Long Short Term Memory (Bi-LSTM) [12] to analyze the input tweets and automatically extracts the important textual features. By doing so, it can largely save the manual cost for feature selection and is helpful to build a robust feature space for the learning of a more accurate classifier. To allow users to access this Twitter bot classifier through the Internet, we provide a public accessible interface developed using Web service. This interface allows a user to upload the tweet and returns the classification result (probability that the tweet is posted by a bot or not) to that user. For the server side, we use Flask, a micro framework developed in Python, to return JSON data generated by the Deepbot. The proposed Deepbot consists of two components which is the bot classifier and the Web interface. In the near future, we will further enhance the model classification ability by designing a more sophisticated deep neural network structure and try to make the Web system of Deepbot to support the high concurrency access.

In [8] Heng Ping , Sujuan Qin (2018) proposed A Social Bots Detection Model Based on Deep Learning Algorithm. In this paper The DeBD detection method consists of three parts: social bot detection based on tweet joint features, social bot detection based on tweet metadata temporal features and features fusing. In the first part, the user tweet is transformed into a word embedding and concatenate them. Then CNN is used to extract the feature of the tweet content and the relationship between them. In the second part, we treat the metadata of the user tweets as temporal information represented by social users rather than purely digital features. Counting the user's temporal information for a period of time and using it as an input to the LSTM neural network. The experimental results of these two parts shows that the proposed DeBD is effectiveness for detecting bot. CNN and LSTM focus on different aspects of tweet features, and fuse the extracted features of CNN and LSTM. Although the social bot detection based on deep learning achieves nearly perfect accuracy on different data sets, it requires a large amount of tweet information from the user. In the future work, we can use the user tweets and information to detect social bots as little as possible while ensuring high detection rate.

In [9] Peining Shi,Zhiyong Zhang (2019) proposed Detecting Malicious Social Bots Based on Clickstream Sequences. We proposed a novel method to accurately detect malicious social bots in online social networks. Experiments showed that transition probability between user clickstreams based on the social situation analytics can be used to detect malicious social bots in online social platforms accurately. In future research, additional behaviors of malicious social bots will be further considered and the proposed detection approach will be extended and optimized to identify specific intentions and purposes of a broader range of malicious social bots. Data cleaning: data that are clicked less must be cleaned to remove wrong data, obtain accurate transition probability between clickstreams, and avoid the error of transition probability caused by fewer data. Data processing: some data are selected randomly from the normal user set and social bots set to the label. Normal user account is labeled as 1, and the social bots account is labeled as −1. Seed users are classified as the category of clusters. Feature selection: in the spatial dimension: according to the main functions of the CyVOD platform, we select the transition probability features related to the playback function: P(play,play) , P(play,like) , P(play,feedback) , p(play,comment) , P(play,share) and P(play,more) ; in the time dimension: we can get the inter-arrival times (IATs). Because if all transition probability matrixes of user behavior are constructed, extremely huge data size and sparse matrix can increase the difficulty of data detection. Semi-supervised clustering method: first, the initial centers of two clusters are determined by labeled seed users. Then, unlabeled data are used to iterate and optimize the clustering results constantly. Obtain the normal user set and social bots set: the normal user set and social bots set can be finally obtained by detecting. 6) Result evaluation: we

evaluate results based on three different metrics: Precision, Recall, and F1 Score (F1 is the harmonic average of Precision and Recall, F1 = 2 ·

Precision·Recall Precision+Recall). In the meantime, we use Accuracy as a metric and compare it with the SVM algorithm to verify the efficiency of the method. Accuracy is the ratio of the number of samples correctly classified by the classifier to the total number of samples.

In [10] Rashmi Ranjan Rout, Greeshma Lingam, and D.

V. L. N. Somayajulu (2019) This article presents an LAMSBD algorithm by integrating a trust computational model with a set of URL-based features for MSBD. In addition, we evaluate the trustworthiness of tweets (posted by each participant) by using the Bayesian learning and DST. Moreover, the proposed LA-MSBD algorithm executes a finite set of learning actions to update action probability value (i.e., probability of a participant posting malicious URLs in the tweets). The proposed LA-MSBD algorithm achieves the advantages of incremental learning. Two Twitter data sets are used to evaluate the performance of our proposed LA-MSBD algorithm. The experimental results show that the proposed LA-MSBD algorithm achieves up to 7% improvement of accuracy compared with other existing algorithms. For The Fake Project and Social Honeypot data sets, the proposed LA-MSBD algorithm has achieved precisions of 95.37% and 91.77% for MSBD, respectively. Furthermore, as a future research challenge, we would like to investigate the dependence among the features and its impact on MSBD.

4. PROPOSED METHODOLOGY

To overcome the restrictions of techniques we have introduced the deep learning technique dependent of Faster RCNN and RNN Using Twitter API we can post tweets including hash tag for particular topic. We generate Twitter data set to differentiate between human and bots. The tweets can be posted by registered users or by computer program. Computer programs are designed in such a way that they continuously tweet from some account on particular topic on behalf or against it for some neutral tweets. Usually when normal users tweet or reply to a particular topic the frequency of tweets will be normal. We will train the data sets using RCNN based algorithm. The input will be processed using RCNN to find out the sentiments. To detect if it is a human generated or not we will check the time interval of the Accounts suppose its within 10 minutes. If it is more than 8-10 minutes then it was suspected. We will also analyze the type of treats that has been posted from a user account. In the course of identification of human account deception large corpus of data is obtained. This data is recycled since it will contain information that do not contribute to the end results. The data is mined, impure data is removed and then stored in a database. This data is applied to machine learning models and results are obtained. Our proposed approach for detecting malicious social bot in twitter network using deep learning was modelled in five modules

1. Acquisition and Profiling setup
2. Data Bootstrap
3. Feature Extraction
4. Feature Preprocessing
5. Training Classifiers.

Our model is suitable to any online social network such as twitter, Acquisition step can be adapted according to twitter API- Tweepy. Classification step is also flexible. In this work we adopted FASTER REGIONS CONVOLUTION NEURAL NETWORK and RESNET which is reported good results by applying in big data environments that treats specifically bots on online social network such as twitter. The proposed approach pipeline: Acquisition and Profiling Setup, Data Bootstrap Feature Extraction, Feature Preprocessing and Classification. Each user, we need to create a user profile. The labelling followed the rules consolidated in related works:

—Malicious bots: automated accounts with spamlike content, usually redundant and repetitive;

—Legitimate bots: automated accounts with harmless content, usually posted with the use of auxiliary software;

—Human: non-automated accounts with intelligent and original content.

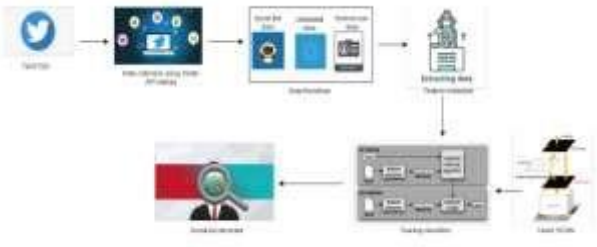


Fig 1: proposed framework

1. ACQUISITION AND PROFILING SETUP

The acquisition step consists of getting data from an OSN to create a textual data set. Our model requires the collected textual set to be grounded on one main subject .This is requirement is necessary, because wavelet-based text mining takes analysis of signalized key terms to obtain any further knowledge. In case the dataset is not grounded on one main term, we suggest the extraction of relevant terms. The use of a supervised deep-learning approach, we need a l dataset to induce a method. The text of each user is concatenated cumulatively following the profile-based

paradigm and a textual repository with several users' posts. This step is called Profiling Setup and provides the data that will be processed to obtain the feature vector that describes each class.

2. DATA BOOTSTRAP

Data Bootstrap Consists of Social Bots, unlabeled Data normal user data which contains all the details each of them such as network, user, making friends, content, tweeting and emotion, the attribute where can we detect malicious social bots.

3. FEATURE EXTRACTION

This phase which aims to collect relevant information about the malicious bots. This includes information such as presence of the URLs in a blacklist, features obtained from the URL String, information about the host, the content of the website such as HTML and JavaScript, popularity information, etc., gives an example to demonstrate various types various types of information that can be collected from an online social network to obtain the feature representation.

4. FEATURE PREPROCESSING

In this phase, the unstructured information about the data is appropriately formatted, and converted to a numerical vector so that it can be fed into Deep learning algorithms. For example, the numerical information can be used as is, and Bag-of-words is often used for representing textual or lexical content.

5. TRAINING CLASSIFIERS

We propose a general framework used for online classification and offline training. A classification problem consists of taking an input vector with data and deciding. It follows a supervised learning process based on training from instances of each class the most important learning feature is the generalization: the algorithm should produce sensible output for inputs that were not encountered during learning.

EXPLORATORY DATA ANALYSIS

1) Identifying missingness & imbalance in the data
2) Feature extraction
3) Feature engineering
4) Dropping unnecessary attributes

Heatmap shows us all the missing values in the yellow and all the filled values which are not missing is shown in the purple. The location description in URL see our maximum null values as we can see in these yellow bars while status has extended profile and some of the missing values.

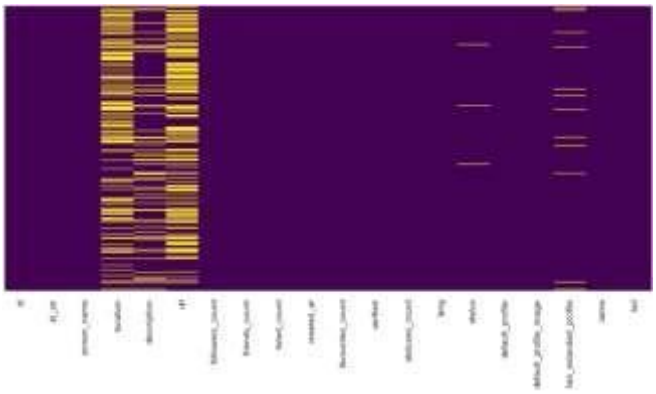
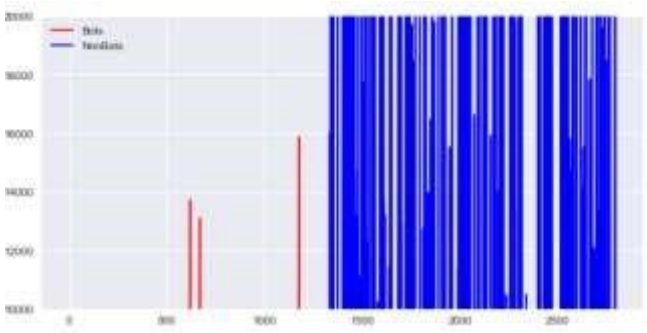
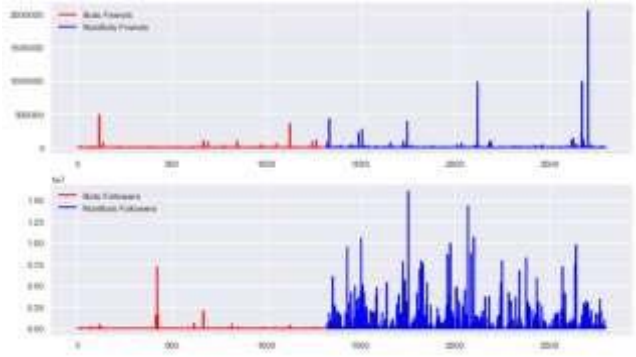


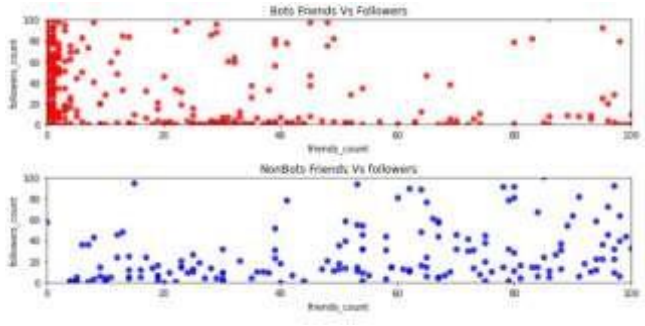
Fig 2 : heatmap(missingness of data)



Our next step was identifying the imbalance of being the data we found that whenever the listed count is between 10,000 to 20,000. Listed count is listed between 10,000 to 20,000 then there is a chance of 5% bots is detected remaining 95% non bots is detected.



We found that bots have maximum followers but have less friends. So followers and friends is the good indication attributes of bots and non bots. Similarly for the case of verified attributes as well.



Next we identified feature independence using spearman correlation. From the Pearson correlation and spearman correlation matrix we found that no correlation between the attributes of status count, id, default profile, default profile image. Hence it should not consider feature to detect malicious bots or non bots.There is strong correlation between the attributes verified, friends count, followers count hence it is considered to detect malicious bots or not.

Fig : 3 Pearson correlation matrix

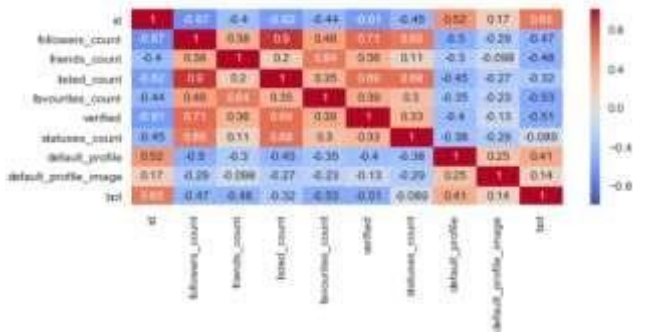


Fig: 4 spearman correlation matrix

We cannot perform correlation for categorical attributes so we will take screen name, name description, status into feature engineering verified, listed count for feature extraction. To perform the feature Engineering we created a bag of word models which identifies whether an account on twitter is a bot or not. So we have a screen name, name description in status into a binary using counts vectorizer algorithm. Then we have done some feature extraction and the listed count binary wherever it is about 20,000 we have false and taken all these values and created new feature then we have implemented classifier algorithm. We have taken the bag of word model to approach create some vectors some other feature like the bus feed in the description and identify that earlier that it is a real user the listed count and predicted the remaining values and identified malicious bots.

Receiver operating characteristics:

1) False Positive Rate

2) True Positive Rate

A Receiver operating characteristics curve or ROC curve is a graphical plot that illustrates the diagnostics ability of a binary classifier system False positive ratio is the probability of falsely rejecting the null hypothesis probability that an actual positive will test The corpus is cleaned from all the bot accounts since the aim is only to identify the deceptive human accounts. Even after filtering the corpus can contain few fake human accounts and bot accounts. Extra 15,000 deceptive were manually created as though they were created by humans & not bots and added to the corpus for research purposes.

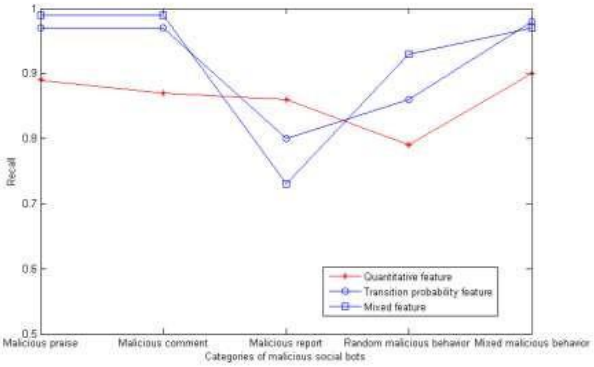


Fig: 5 Recall of detection methods based on different features for different types of malicious social bots.

According to psychology humans lie about these things on social media their name, age, gender, image and location. The accounts created were rich with these attributes. The now two different available dataset are tested for similarity. The tests performed are the Mann-Whitney-U test which says if the two sets are similar and The Chi-Square Test to test if the datasets are independent of each other.

6. CONCLUSION

The prevalence of sophisticated bots on social media platforms such as Twitter, the need for improved, inexpensive bot detection methods is apparent. We proposed a Faster RCNN and Resnet algorithm allowing us to use both tweet content and metadata to detect bots at the tweet level. Our model can achieve an extremely high accuracy exceeding 97% .The proposed algorithm executes a finite set of learning actions to update action accuracy value. Faster-RCNN is used to extract the feature of the tweet content and the relationship between them. The proposed algorithm achieves the advantages of incremental learning. Twitter data sets are used to evaluate the performance of our algorithm. The experimental results show that the algorithm achieves improvement of accuracy compared with other existing algorithms.

7. REFERENCES

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.

[1] G. Lingam, R. R. Rout, and D. V. L. N. Somayajulu, "Adaptive deep Q-learning model for detecting social bots and influential users in online social networks," Appl. Intell., vol. 49, no. 11, pp. 3947–3964, Nov. 2019.

[2] 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.

[3] S. Madisetty and M. S. Desarkar, "A neural networkbased ensemble approach for spam detection in Twitter," IEEE Trans. Comput. Social Syst., vol. 5, no. 4, pp. 973–984, Dec. 2018.

[4] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection using hyperlinks information," J. Ambient Intell. Hum. Comput., vol. 10, no. 5, pp. 2015–2028, May 2019.

[5] T. Wu, S. Liu, J. Zhang, and Y. Xiang, "Twitter spam detection based on deep learning," in Proc. Australas. Comput. Sci. Week Multiconf. (ACSW), 2017

[6] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection using hyperlinks information," J. Ambient Intell. Hum. Comput., vol. 10, no. 5, pp. 2015–2028, May 2019.

[7] J. Echeverria and S. Zhou, "Discovery, retrieval, and analysis of the'star wars' botnet in twitter," in Proc. 2017 IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining 2017, 2017, pp. 1–8.

[8] A. Dorri, M. Abadi, and M. Dadfarnia, "SocialBotHunter: Botnet detection in Twitter-like social networking services using semisupervised collective classification," in Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Intl Conf Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), Aug. 2018, pp. 496–503.

[9] M. Agarwal and B. Zhou, "Using trust model for detecting malicious activities in Twitter," in Proc. Int. Conf. Social Comput., Behav.-Cultural Modeling, Predict. Springer, 2014, pp. 207–214. [27] G. Lingam, R. R. Rout, and D. V. L. N. Somayajulu, "Detection of social botnet using a trust model based on spam content in Twitter network," in Proc. IEEE 13th Int. Conf. Ind. Inf. Syst. (ICIIS), Dec. 2018,

[10] A. Moayedikia, K.-L. Ong, Y. L. Boo, and W. G. S. Yeoh, "Task assignment in microtask crowdsourcing platforms using learning automata," Eng. Appl. Artif. Intell., vol. 74, pp. 212–225, Sep. 2018.

[11] G. Lingam, R. R. Rout, and D. Somayajulu, "Learning automatabased trust model for user recommendations in online social networks," Comput. Electr. Eng., vol. 66, pp. 174–188, Feb. 2018.

[12] Manju, S. Chand, and B. Kumar, "Target coverage heuristic based on learning automata in wireless sensor networks," IET Wireless Sensor Syst., vol. 8, no. 3, pp. 109–115, Jun. 2018.

[13] G. Wang, X. Zhang, S. Tang, C. Wilson, H. Zheng, and B. Y. Zhao, "Clickstream user behavior models," ACM Trans. Web, vol. 11, no. 4, Jul. 2017, Art. no. 21.

[14] Y. Liu, C. Wang, M. Zhang, and S. Ma, "User behavior modeling for better Web search ranking," Front. Comput. Sci., vol. 11, no. 6, pp. 923–936, Dec. 2017.

[15] 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.

[16] A. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2017. [2] N. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system," Procedia Computer Science, vol. 89, pp. 213–217, 2016.

[17] H. Wang, J. Gu, and S. Wang, "An effective intrusion detection framework based on SVM with feature augmentation," Knowledge-Based Systems, vol. 136, pp. 130–139, 2017.

[18] I. M. Akashdeep, I. Manzoor, and N. Kumar, "A feature reduced intrusion detection system using ann classifier," Expert Systems with Applications, vol. 88, pp. 249–257, 2017.

[19] Y. Chuan-Long, Z. Yue-Fei, F. Jin-Long et al., "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.

[20] M. Lopez-Martin, B. Carro, and A. SanchezEsguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," Expert Systems with Applications, vol. 141, Article ID 112963, 2019.

[21] H. He, X. Sun, H. He, G. Zhao, L. He, and J. Ren, "A novel multimodal-sequential approach based on multi-view

features for network intrusion detection," IEEE Access, vol. 7, pp. 183207–183221, 2019.

[22] P. Sun, P. Liu, Q. Li et al., "DL-IDS: extracting features using CNN-LSTM hybrid network for intrusion detection system," Security and Communication Networks, vol. 2020, Article ID 8890306, 11 pages, 2020.

[23] A. Ramachandran, N. Feamster, and D. Dagon, "Revealing Social bot Membership Using DNSBL Counter-Intelligence," Proc. USENIX Second Workshop Steps to Reducing Unwanted Traffic on the Internet (SRUTI '06).

[24] B. McCarty, "Social bots: Big and Bigger," IEEE Security & Privacy Magazine, vol. 1, no. 4, pp. 87-90.

[25] C.T. News, Expert: Social bots No. 1 Emerging http://www.cnn.com/2006/TECH/internet/01/31/f urst/internet.

[26] D. Dagon, C. Zou, and W. Lee, "Modeling Social bot Propagation Using Time Zones," Proc. 13th Ann. Network and Distributed System Security Symp. (NDSS '06), pp. 235-249.