MAT JOURNALS

Journal of Computer Science Engineering and Software Testing
e-ISSN: 2581-6969
Volume 5 Issue 2

Performance Analysis of Machine Learning Algorithms in SMP: A Case Study of Twitter

S Varsha[1], Prathiba P S[1], Deepika N[1], Neha Janghel[1], D V Ashoka[2]
[1]UG Students, [2]Professor
[1,2]Department of ISE, JSS Academy of Technical Education, Bangalore, Karnataka, India
Email: *prathibaupadhya97@gmail.com*
DOI: *http://doi.org/10.5281/zenodo.3268439*

Abstract

The number of people using Social Media Platform (SMP) is increasing day by day. A few users may hide their identity with malicious intentions. Previous research has detected fake accounts created by bots using machine learning concepts. These ML concepts used engineered features such as the 'following-to-followers ratio' which is generally available in their accounts. In previous studies these similarly clustered features were applied to the machine learning models for detection of fake and real accounts. In the recent research the behavioural features like the sentient of the tweet posted on twitter is considered along with the parameters. Here, the ML models are also trained to use engineered features depending on behavioural data.

Keywords: *Botometer, bots, fake account, MLclassifiers, NLP, social media platform, tweepy*

INTRODUCTION

Overview of Social Media

Social media is a collection of online platforms and tools thatenables people for content-sharing, collaboration, interaction, expressing ones experiences and perspectives by facilitating online communication between groups of people.

Billons of people all over the world make use of social media to communicate with family and friends, develop their interest, and learn new things and for entertainment.

Social media platform (SMP) was originated as a tool that was mainly used by people to interact with friends and family but was later adopted by businesses to widen the knowledge in specific field, build professional network, gain customer feedback, and elevate your brand.

Blogs, micro-blogs, wikis, social networking sites, photo-sharing sites, instant messaging, video-sharing sites, virtual world, widgets, podcasts are some of the forms of Social media. Some popular social media are:

Facebook

Facebook is friend, community and interest-basedSMP that allow registered users to generate profiles, post photos and videos, send messages and to be in contact with their friends.
It is a popular free website which is available in 37 different languages.

Twitter

It is a micro blogging site that enables us toconverse, share and communicate by typing short postscalled 'tweets'initially, that had a limit of 140 characterswhereas in2017, it increased its limit to 280 characters. Ahash tag(#) isused to index topics or keywords on

Twitter that enables user to easily track the topics of their interest. It can be included anywhere in a tweet that allows people to follow their interested topics, categorize tweets and help in twitter search.

Instagram
It is a widespread photo-sharing applicationthat is integrated with other SMP. During its course more filters and features were included: photo maps, mobile photo pages, and web profiles.

Similar popular Medias are Tumblr, LinkedIn and Pinterest. But in contrast, SMP is becoming a target for spammers and scammers as the powerful application of social network is often misused by malevolent attackers who extract sensitive private data of naive users. Some commonly observed threats and methods of attacks are:

Social Engineering: Here the attacker tries to establish trustwith targeted individual. Once it is establishes, attacker starts to ask specific private information.

Targeted Phishing Attack: These attacks mainly aim atstealing money or confidential information where chances of success are high.

Site Compromise: Here attacker compromises site withmalicious code which directs users to provide their personal information.

Social media used for spreading spam and malwares: Cyber criminals use short URLs which are difficult to identify if it is pointing to malicious or legitimate site.

Fake Accounts: Fake accounts are the most commonly usedmethod for performing data harvesting attack on a larger scale where malicious actor create profiles which imitates real or fictitious persons. Fake accounts can either be created by bots or humans or cyborg. Bots usually target largePerformance analysis of machine learning algorithms in SMP: A case study of Twitter2group whereas, human fake account tends to target specific individuals.

Few malicious intent of fake account generation are:
To change individual or group's action and perception. Spread rumours or false news and malwares. Defaming ones character.Polarizing ones opinions. Improvising popularity.

Various machine learning techniques have been applied to identify fake accounts generated by both bots and humans.

RELATED WORK

During real-world occurrences, particularly crisis events, online social media plays a significant role in today's world. The use of real-world social media has both beneficial and negative impacts on culture. It can be used favourably by officials as effective disaster management and negatively to spread rumours or false news during the crisis. Gupta H Lamba focuses on the role of SMPs like Twitter in spreading false catastrophe images like Hurricane Sandy (2012) by characterizing and defining the spread of fake images. It was found that ten thousand unusual unique tweets were spread on Twitter, consisting of false pictures of Hurricane Sandy. Characterization was introduced to acknowledge patterns of impact; spatial and social reputation for the production of fake pictures, resulting in the reality that 86% of tweets circulating the fake pictures were initial retweets and therefore very restricted tweets. Classification models were used to distinguish Hurricane Sandy's fake and true pictures. Using the classification of Decision Tree, 97 percent precision was acquired by anticipating false pictures from true. This showed that it is possible to identify true and fake pictures published on Twitter using automated methods.

The success and popularity of an online social network is a result of the number of audience/users the organization has commanded. [4] Here, Twitter is taken as

the prime focus of the case study with 62 million public accounts. The author states that the study of its broad spectrum of users is a difficult task because of the presence of fake accounts. They have used profile-based approach for recognizing fake accounts by considering and studying their activities such followers to following count, last profile updated time, their profile name etc. Web crawling is used for gathering twitter data using Twitter Rest API.

Further using map-reduction and pattern recognition techniques fake profiles are identified.
The social media life and the personal life are social media users are intertwined in an irreversible way[6]. These users spend a quality time on social media and it's the source of their news or any real time information is found online. Since the people blindly believe the credibility of the information published by these sources we need to eliminatethe chances of such scammers uploading fake news from a fake account. The method used for eliminating fake accounts in this paper consists of two main steps, The first step is to determine the main factors that influencing a correct detection of fake accounts.

The second step is applying a classification algorithm that uses the determined attributes in step one from accounts for discovering the fake accounts.

This research mainly aims to propose the minimum set of attributes that helps us to detect the fake users with highest accuracy.

Zi Chu primarily focuses on the functionality of the social media giant Twitter in an attempt to classify the users as human, bot and cyborg users.[5] Twitter is also used as a tool for microblogging where the user can write their blog or tweet in less than 140 words. They can use @Username for addressing other user and #Hashtag conveying some tweet corresponding a topic with the #.

User relationship in twitter consists of two end i.e., following and followers. Cyborg is human created accounts but aremaintained by bots which has similar characteristics to both human and bot account. This work follows this mechanism that uses entropy measures, which helped in determining that humans are having high entropy due to their complex timing behaviour, whereas bots and cyborgs have low entropy.

C. Xiao describes cluster of fake identities created by the same user [3].Supervised machine learning pipeline is the main method used where complete group of accounts is classified as legitimate or malicious. Registration date and registration IP address are the factors to be considered to create groups. The main elements used in this model are statistics on areas of user-created text such as name, email address, company, etc.

Tayfun Tuna explains about Social network analysis (SNA) in [7], i.e., nothing but measuring and mapping of flow of relationship among peoples, groups, organizations, URLs and other linked data entities. The graphical representation of SNA consists of nodes and links between the nodes.

Where nodes symbolize the people or groups and links demonstrate relationships or flows among the nodes. SNA's provide mathematical and visual analysis of human relationships. SNA's have wide range of applications that includes data aggregation and mining, user attribute and behaviour analysis, community-maintained source funding, location based communication analysis, recommender systems development and entity resolution. SNA is

used in intelligence, law enforcement activities, understanding online behaviour by individuals, organizations, and between websites.

The understanding of user characteristics about behavioural patterns in social networks is momentous as these patterns can contribute useful evidence about the people behaviours in addition to the online interactivity. These observations can be Performance analysis of machine learning algorithms in SMP: A case study of Twitter3used to describe the main problems from sociological and psychological health viewpoint.

There is a lot of curiosity shown in the recognition of malicious accounts from SMP. For example, Twitterbots [8] are those who send automated posts on twitter. These bots posts contents that ranges from helpful or malicious. Twitter bots send tweets periodically. It replies to instances of particular sayings in user messages. They are specialized for various purposes that can be informative, useful or dangerous. Here, we use tweet sentiment feature in both bot and human account to identify bots.

Previous work mostly stresses on the semantic characteristic of tweet sentiment. In this work, [8] they have used tweet sentiment to analyse public view. Here the sentiment was used for account authentication and classification.

On a daily basis huge number of comments is generated in YouTube but not all activities are legitimate. Any user action that tries to post fake contents, or theatrically increasing the YouTube's activity metrics over a redirected link, are termed as illegitimate activity.

Main contribution of this work [9] is to detect fake contents from the real ones posted on YouTube. Spammer seeds face the problem of identifying fake social engagement in a way with the aim of finding beings that have alike pattern of behaviour known as seeds.

IMPACT OF FAKE ACCOUNTS

Bots, also well-known as spiders, crawlers, etc., are used to carry out repeating and iterative tasks in a search engine comes regularly in the form of malware. They get the total control of website or a computer.

Useful Bots are used to collect data. Bots in such pretexts are called web crawlers. A good use of bots is automate communication with messengers, catboats, etc.

Malicious bots are known as self-propagating malware it corrupts its host. Harmful effects of Bots in SMPs It contributes in creation of fake accounts. It helps in increasing follower count, retweeting on behalf of a person, or posts, likes, or comments for a cost. It helps the competitors of a particular company to promote false and negative reviews of a company to taint its reputation.

They promote spreading of fake news. A type of bots called as Spam bots attract the users to phishing links and scam the users.The loading time and performance of websites can slow down the by bots.

PROPOSED METHODOLOGY

Create of twitter application, obtain the authentication keys and obtain tweet in JSON format. Using tweepy library to create connection with twitter and to extract tweets from twitter.

In the process of detection of fake accounts the account data is accumulated with the help of official twitter API. The data undergoes the process of data mining and the extracted data is cleaned and filtered from unwanted contents.

The cleaned data is stored which is later applied to the trained ML models. Initially a specified number of user's data is extracted with the help of users data is extracted with the help of given tag word. Then the latest 200 tweets of these users are also extracted.

The sentiment of the cleaned data is determined using Sentiment analysis. Natural language processing estimates the total count of positive, negative and neutral tweets among the selected tweets.

After Natural language processing the dataset obtained is called featured dataset. The ML classifier is used to train the dataset so as to classify fake and genuine twitter accounts. The Classifier is initially trained with Kaggle dataset and later the featured dataset is fed as an input to classifier for classification of fake and real accounts. Bot and non-bot accounts can be detected and classified using botometer API.

Classification results are analysed and obtained results are fed to visualization tool for effective visual display of result which may consists of graphs and tabular comparisons.

EXPECTED RESULT

After the analysis of the dataset contents using ML classifier, the results can be visualized using visualization tools like Power BI, Tableau, etc.

Here, the output is viewed in form of a dash board containing tables and graphs. Here the graph plotted represents the number of fake accounts v/s number of real accounts. This can also be represented in tabular form. Further part of the results is still under research work.Performance analysis of machine learning algorithms in SMP: A case study of Twitter4AuAhmed El Azab, Amira M. Idrees, Mahmoud A. Mahmoud, Hesham Hefny

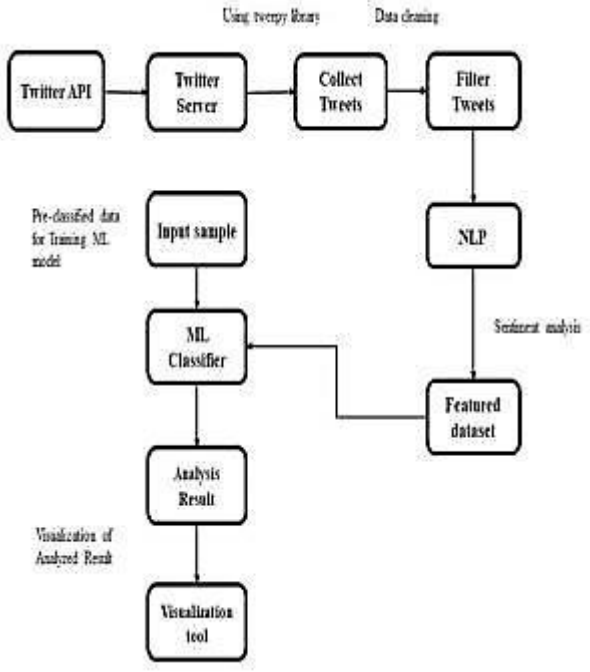

Figure 1: *Architecture of the proposed methodology.*

CONCLUSION

The main inspiration for this work was the chaos caused by the fake accounts in the SMPs. It is necessary to detect these and reduce its malicious effect. There are various solutions proposed for their detection and this work is one such derived solution by referring much work. Future

work would be to enrich the corpus of the fake accounts by doing in-detail research about their characteristics and behavior tendencies.

REFERENCES

1. Using Machine Learning to Detect Fake Identities:Botsvs Humans.
2. Faking Sandy: Characteristics and identifying Fake Images on Twitter during Hurricane Sandy.
3. Detecting clusters of fake accounts in online social networks.
4. Profile characteristics of fake Twitter accounts(SuprajaGurajala, Joshua S White, Brian Hudson, Brian R Voter and Jeanna N Matthews).
5. Zi Chu, Steven Gianvecchio, Haining Wang, and SushilJajodia, "Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?.
6. Fake Account Detection in Twitter Based on Minimum Weighted Features.
7. User Characterization for Online Social NetworkAuthor: Tayfun Tuna, EsraAkbasAhmetAksoy, M. Abdullah CanbazUmitKarabiyik, Bilal GonenRamazanAyguna.
8. Using Sentiment to Detect Bots on Twitter: Are Humans more Opinionated than Bots?.
9. Author: John P. Dickerson,VadimKagan, V.S. Subrahmanian.
10. In a World That Counts: Clustering and Detecting Fake Social Engagement at ScaleAuthor: Yixuan Li, Oscar Martinez, Xing Chen, Yi Li, John E. Hopcroft.
11. Fame for sale: Efficient detection of fake Twitter follower.
12. Author: S. Cresci, M. Petrocchi, R. Di Pietro, A. Spognardi, M. Tesconi.

Cite this article as: *S Varsha, Prathiba P S, Deepika N, Neha Janghel, & D V Ashoka. (2019). Performance Analysis of Machine Learning Algorithms in SMP: A Case Study of Twitter. Journal of Computer Science Engineering and Software Testing, 5(2), 17–22. http://doi.org/10.5281/zenodo.3268439*