Automated Bot Detection

Dr. Pushpalatha S Nikkam, Amogh Belavigi, Divyank Rahate, Ananya Shanbhag, Shreyas Desai

Department of Information Science and Engineering, SDM College of Engineering and Technology, Dharwad, Karnataka

Date of Submission: 24-05-2023 Date of Acceptance: 05-06-2023

Abstract— In online social networks, the audience size commanded by an organization or an individual is a critical measure of that entity's popularity, and this measure has important economic and/or political implications Such efforts to measure the popularity of users or exploit knowledge about their audience, which is complicated by the presence of chatbots on these networks. Twitter is an online social networking site that is gaining popularity in the blink of an eye. The increase in popularity has also led to an increase in the number of chatbots, which can easily manipulate the interests of Twitter users. We propose a system to distinguish between a human user and a bot. However, we observe that human behavior is more complex than that of bots. Analysis of the profile of the Chatbots reveals their distinct behavior, i.e., the tweets are in favor of a few selected topics, and the interval of the tweets is uniform.

Keywords: Twitter, chatbots, hashtags, online social networking sites.

I. INTRODUCTION

The social networking phenomenon has grown tremendously over the last twenty years. During this rise, the different types of social networking sites have created many online activities. It instantly attracts the interest of a large population, and users increasingly depend on the credibility of the information exposed on online social networks. On the other hand, online social networking sites suffer from an expanding number of fake accounts, and also a huge number of chatbots that are being created that do not match any real human accounts. These chatbots are trained to present a particular set of instructions like spreading fake news, web ratings, and spam. Twitter spreads information to a large group of users who are active in real-time. There are two types of events. The first type expresses the events that are discovered to be fake. Some examples of these events are False news announced by politicians or rumors that are spread among the public for different reasons. The second type expresses the events that seem to be fake; some Examples of these events are tweets that provide conflicting contents or tweets that do not have any evidence of correctness. One of the main problems with social media is scammers, as they can use chatbots for different targets. One of these targets would be spreading rumors that may affect a determined business or even society as a whole larger segment.

For instance, one political party spreads false news and makes controversial statements about the other political parties. In order to prevent negative influences on people, the idea presented is to analyze the tweets and detect and stop the chatbots from carrying out malicious or deceiving activities. and alter people's ideologies by spreading negativity, the aim is to detect chatbots. and report it to Twitter.

II. LITERATURE SURVEY

There are a number of such incidents that have actually proven the fact that Twitter is being misused. One such latest incident was the rise in Twitter followers of an Indian politician [1].

From politicians and nation-states to terrorist groups, several organizations have been reported to run specific campaigns to influence opinions on social media that create risk. freedom of expression. Many researchers are turning to machine learning techniques. distinguish between real and fake users. So, it is necessary to identify and remove the "effect". "Bots" are realistic, automated identities that illegally alter conversations on websites such as Twitter. and Facebook before they become too influential. Different teams in the DARPA robotics challenge used different techniques to find chatbots on Twitter. SentiMetrix was the first team to figure out all the chatbots. They used different approaches, such as tweet syntax, Tweet semantics, temporal behavioral characteristics, and user profile characteristics proved to be the case. effective approaches [2]. These methods have proven to be the most effective. The paper [3] describes phishing.

III. MOTIVATION

Powered by advanced algorithms, we protect the authenticity and integrity of Twitter. In the realm of tweets and hashtags, we fight automated accounts that spread misinformation. Please help us by reporting suspicious accounts and sharing your findings.

Together, we can create a path to a more authentic social media experience. Let us be relentless, steadfast, and unwavering in our commitment to protect the integrity of Twitter. Together, we'll reveal the shadows, reveal the truth, and make sure Twitter remains a thriving place for authentic conversations.

IV. PROPOSED WORK

The proposed system aims to identify fake chatbots on Twitter among other users and restrict their impact on people's behavior on social media. An online social networking site where there are more than 319 million active users. of numerous chatbots that try to gain human attention over a particular topic or deviate pollute and dominate the genuine expression of people over social media. Proposed system functionalities are achieved by first extracting the Twitter network, i.e., the data being posted on Twitter by the Twitter users, like the Twitter handle, tweet location, and date the tweet was posted. Twitter API (Application Programme Interface), also known as Tweepy, is an option provided to developers by Twitter that grants us permission to extract the Twitter data, but to extract the data, one must first have a Twitter account and a blank application created on the Twitter application developer site, which helps in data extraction. where the user's Twitter handle is filtered by using the screen name feature, and again with the help of the Twitter API, we find out the followers for that particular Twitter handle extracted, and for that Twitter handles again, the followers are identified. This process is carried out All these screen names, or the Twitter handles extracted, are stored on a graph that is drawn, and a network is established between the Twitter handles. nodes identified from this network and clustered based on the parent Twitter handle or the tweets to which the user has reacted, the behavior of the particular Twitter handle, the content of all the common nodes or Twitter handles that contribute to the network and help a topic of genuine users, and the bots and the bot accounts or the Twitter handles responsible for the creation of bot accounts and reporting them to Twitter.

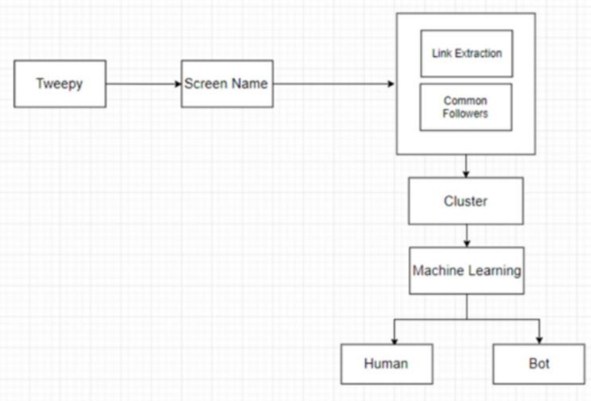
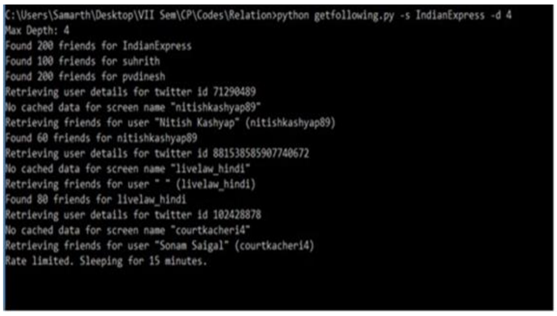


Fig.1 Flow Diagram of Process

V. EXPERIMENTAL RESULT

This project was tested in real-time using ML, which helped the user bifurcate between the real human user and a bot, created by an organization to promote its product and influence the person or bot. can be made by a real human user with the bad intention of stealing a person's data. After analyzing the bot and the user, the security concerns will be eradicated as the Differentiation is clearly visible between a person and a bot, and the user will be saved from major cybercrime such as phishing, hacking, or security breaches of the organization or the firm that holds the majority of data regarding the employees and the workers of that organization or firm.



```
C:\Users\Samarth\Desktop\VII Sem\CP\Codes\Relation>python getfollowing.py -s IndianExpress -d 4
Max Depth: 4
Found 200 friends for IndianExpress
Found 100 friends for suhrith
Found 200 friends for pvdinesh
Retrieving user details for twitter id 71290489
No cached data for screen name "nitishkashyap89"
Retrieving friends for user "Nitish Kashyap" (nitishkashyap89)
Found 60 friends for nitishkashyap89
Retrieving user details for twitter id 881538585907740672
No cached data for screen name "livelaw_hindi"
Retrieving friends for user " " (livelaw_hindi)
Found 80 friends for livelaw_hindi
Retrieving user details for twitter id 102428878
No cached data for screen name "courtkacheri4"
Retrieving friends for user "Sonam Saigal" (courtkacheri4)
Rate limited. Sleeping for 15 minutes.
```

Fig.2 Result of the Project

VI. CONCLUSION

Twitter is a very influential social networking site that may manipulate people's ideologies quite easily, so it is very important that we detect chatbots doing malicious deeds and make sure it's reported to Twitter. [3]. During this process of detecting and reporting chat, With bots, there might arise some divergent results that are considered to be exceptions.

REFERENCES

[1]. Himanshu. Rajput. "social media and politics in india: a study on twitter usage among indian political leaders.". ajms/article/view/159.

[2]. Azaria A. Durst S. Kagan V. Galstyan A. Lerman K. Zhu L. Ferrara E. Flammini A. Subrahmanian, V.S. and F. Menczer. “"The DARPA Twitter bot challenge."". pages 38–46, 2016.

[3]. Kempers L. Shafahi, M. and H. Afsarmanesh. “"Phishing through social bots on Twitter"". In Big Data (Big Data), 2016 IEEE International Conference, pages 3703–3712.

[4]. Stavrakas Y. Mathur, V. and . Singh, S. “"Intelligence analysis of Tay Twitter bot"". In Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference , pages 231–236, 2016.

[5]. Hossein Hamooni Chavoshi, Nikan and Abdullah Mueen. “"DeBot: Twitter Bot Detection via Warped Correlation"". In ICDM , pages 817–822, 2016.

[6]. Vadim Kagan Dickerson, John P. and V. S. Subrahmanian. . "using sentiment to detect bots on twitter: Are humans more opinionated than bots?". Advances in Social Networks Analysis and Mining (ASONAM), 2014 IEEE/ACM International Conference on. IEEE, pages 620–627, 2014.

[7]. Di Pietro R. Petrocchi M. Spognardi A. Tesconi M. Cresci, S. "fame for sale: efficient detection of fake twitter followers.". pages 56–71, 2015.