Predicting the Malicious User for Mobile Application

1st K.Elavarsi
Assistant Proffesor, CSE
S.A. Engineering college
Chennai, India

2nd R. Vaishnavi
Computer Science and Engineering
S.A. Engineering college
Chennai, India

3rd P. Pooja
Computer Science and Engineering
S.A. Engineering college
Chennai, India

4th G.Vigneshwari
Computer Science and Engineering
S.A. Engineering college
Chennai, India

***Abstract* -Nowadays people used to communicate with the help of social media networks. There are various kinds of online networking. In olden days people used to communicate with the help of mail. But many social media have evolved. For example Facebook, Twitter etc. In this social media many social bots have evolved, those bots used to spread false information about political candidates and degrade the character of the popular celebrities. The result of common analysis can also be changed by the bot in social media. The social media collects the user's data which is confidential that can also be hacked by the malicious bot. The collection of data which increases the features of the application and improves the quality of service. The bugs can also be fixed, Due to malicious bot there are several threats to people. They need to be identified and removed. Identifying the malicious bot is a tedious task.. One of the techniques is to analyze the character and behavior of the malicious bot. There are several methods and algorithms are used to find the malicious bot. Here we are using the distinctive method to identify the malicious bot. It includes feature selection supported by the transition probability of click stream sequence and semi supervised clustering. These are the techniques included in this paper.**

Keywords-mobile application, collecting datasets, identifying the frequent clicks, block the hacker bots.

I. INTRODUCTION

Nowadays the users are using mobile phones frequently and there is the nature of using social media applications that are liked by the users. It has been proved that social media applications are used to find more people in it, and as well as they can gather more information about everything. The social media application is a massive network where all data will be stored and retrieve the information whenever in need. This has been done by using reinforcement of standard and the efficiency for collecting the data and analyzing the stored information in social media. The social bot uses a short form intended to get earthquake reports with the help of entry Bay. It is used to analyze the earthquake information which is related to social networks. In different research they utilize different techniques to secure the online informal organizations. In online networks we have a huge number of clients which will share their data and that will be stored in a database. The users can access the social media for liking, commenting and sharing their posts with their friends. The fake accounts will be created by the malicious user so that they can steal the user information and compromise their privacy. The malicious user uses bots for doing their three actions (ie liking, commenting and sharing) within a fraction of seconds, but normal users cannot access the three actions at a time but only a single task can be done by them. The social networks will collect all the datasets of all the users who are accessing the social media accounts in it. After collecting the datasets we need to clean the data who accessed the single task, and then we need to give an identification number to the unlearned datasets. The users accessed multiple tasks at a time that will be

checked by using transition probability with the help of zero's and one's, the normal user will be shown as zero and the malicious bot user will be shown as one. The malicious bots can do their task dynamically. Based on the user activity we can easily differentiate who is the normal user and the malicious user. Each user has different behavior by accessing the social media application.

Ⅱ. SYSTEM MODEL

Fig 1: Working of Architecture

Ⅲ. METHODOLOGY

Data Collection

The user's data is collected on the server side. The cyvod technique website, ios and android application in it. The click stream sequence is obtained with data burying point. If one wants to build a website of their own they can use technology called burying for collecting data in a realistic environment. The other way to obtain data is to call corresponding API for building websites.

Experimental Design

The social bots can do a single task at a time, but malicious bots can do multiple tasks at a time. The malicious bots can perform mixed tasks. For example The normal user can access the social media application for liking, commenting and sharing their post to their friends. But malicious users can access all the three within a fraction of seconds by using transition probability. It will predict the normal user as zero and the malicious bot user as one , with the help of this we can identify who is the normal user and the malicious bot user.

Ⅳ. MALICIOUS SOCIAL BOTS DETECTION

Data cleaning: The data cleaning is used for increasing the speed access time and storage in the mobile. It is also used to clean our short term actions in our mobile.

Data processing: The data processing is used to select the data from the user's social media application, and then those data's are labeled as 1 and malicious user is labeled as -1. This can be done by using clustering.

Feature selection: In future selection, some of the features social media applications are used. Those features are listed as follows comments , like, share, play, feedback. The time interval will be identified from these actions of the features the user performs.

Semi-supervised clustering method: The center point of 2 sets of clusters are used to identify the user. Then from the identified clusters, the data which are not in the characteristics (unlabeled) are removed . The unlabeled comes under a supervised method .

Obtain the normal user set and social bots set:By completing all the above steps , who are all the normal users and who are all the malicious bot is obtained.

Ⅴ. RELATED WORK

[1]BEDM (Behavior enhanced deep model)is used to identify the fake accounts. With the help of Deep learning methods, BEDM find the Malicious users in Social media applications.

[2]The online social network the trace of post, comments and like are performed by the users in social media applications. The users will differentiate the malicious & normal users social media applications.

[3]This identifies the malicious bot users who are spreading rumors about some incidents. And also to identify who are creating fake accounts in social media applications.

[4]The functions of attributes . The normal & malicious user is based on their attributes and

also we learned how to have a low amount of calculation process.

[5]It is used to identify the accounts of the malicious user in the social media applications. Based on the online activities, like transferring of money, shopping through online.

VI. CONCLUSION

The distinctive method is included to detect malicious bot in social media application. The transition probability between click stream and user helps to identify the malicious bot accurately in social media.

VII. FUTURE ENHANCEMENT

The current project deals with only limited datasets which are already collected. It has to be enhanced. The results are not more accurate, it has to be developed with more accuracy. This detects malicious bots with only a small number of tagged users. Detecting the malicious bot goes difficult when numbers of users get increased. It has to be overcome by upcoming projects. The time used for identifying the frequent clicks and malicious bot has to be decreased.

REFERENCES

[1] F. Morstatter, L. Wu, T. H. Nazer, K. M. Carley, and H. Liu, ``A new approach to bot detection: Striking the balance between precision and recall," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining*, San Francisco, CA, USA, Aug. 2016, pp. 533_540.

[2] C. A. De Lima Salge and N. Berente, ``Is that social bot behaving unethically?" *Commun. ACM*, vol. 60, no. 9, pp. 29_31, Sep. 2017.

[3] M. Sahlabadi, R. C. Muniyandi, and Z. Shukur, ``Detecting abnormal behavior in social networkWebsites by using a process mining technique," *J. Comput. Sci.*, vol. 10, no. 3, pp. 393_402, 2014.

[4] F. Brito, I. Petiz, P. Salvador, A. Nogueira, and E. Rocha, ``Detecting social network bots based on multiscale behavioral analysis," in *Proc. 7th Int. Conf. Emerg. Secur. Inf., Syst. Technol. (SECURWARE)*, Barcelona, Spain, 2013, pp. 81_85.

[5] T.-K. Huang, M. S. Rahman, H. V. Madhyastha, M. Faloutsos, and B. Ribeiro, ``An analysis of socware cascades in online social networks," in *Proc. 22nd Int. Conf. World Wide Web*, Rio de Janeiro, Brazil, 2013, pp. 619_630.

[6] H. Gao *et al.*, ``Spam ain't as diverse as it seems: Throttling OSN spam with templates underneath," in *Proc. 30th ACSAC*, New Orleans, LA, USA, 2014, pp. 76_85.

[7] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, ``The rise of social bots," *Commun. ACM*, vol. 59, no. 7, pp. 96_104, Jul. 2016.

[8] T. Hwang, I. Pearce, and M. Nanis, ``Socialbots: Voices from the fronts," *Interactions*, vol. 19, no. 2, pp. 38_45, Mar. 2012.

[9] Y. Zhou *et al.*, ``*ProGuard*: Detecting malicious accounts in social network- based online promotions," *IEEE Access*, vol. 5, pp. 1990_1999, 2017.

[10] Z. Zhang, C. Li, B. B. Gupta, and D. Niu, Ef_cient compressed ciphertext length scheme using multi-authority CP-ABE for hierarchical attributes," *IEEE Access*, vol. 6, pp. 38273_38284, 2018. doi:10.1109/ACCESS.2018.2854600.