AN ALGORITHM FOR DETECTING MALICIOUS PROGRAMS BASED ON SPATIOTEMPORAL FEATURES

[1]D. Sasikanth, [2]D. Srinivas

[1,2]Dept. of CSE, Kakinada Institute of Engineering & Technology., Matlapalem, Talarevu Mandal, Corangi, E.G.dt, AP, India

ABSTRACT:

Major raise in the volume of user data (e.g., user generated data) in online social networks, there have been endeavored to plan better approaches for gathering and analyzing such big data. Social bots have been utilized to perform computerized analytical services and give users with improved quality of service. We intend to detect malicious social bots on social network platforms, by (1) proposing the transition probability features between user clickstreams based on the social situation analytics; and (2) designing an algorithm for detecting malicious social bots based on spatiotemporal features. A tale technique for identifying malicious social bots, including the two features selection based on the transition probability of clickstream sequences and semi-supervised clustering, is introduced in this work. This strategy not just examines change probability of user behavior clickstreams but also considers the time feature of behavior.

KEYWORDS: big data, social bots, transition, clickstreams

1] INTRODUCTION:

In online informal organizations, social bots are social records constrained via mechanized projects that can perform comparing tasks dependent on a set of procedures [1]. The expanding utilization of cell phones (e.g., Android and iOS devices) also added to an increase in the frequency and nature of user connection through social networks. It is confirmed by the huge volume, velocity and variety of data generated from the large online social network user base. Social bots have been generally sent to upgrade the quality and proficiency of gathering and examining data from social network services. For instance, the social bot SF QuakeBot [2] is intended to produce tremor reports in the San Francisco Bay, and it can examine seismic tremor related information in social networks in real-time. Be that as it may, popular opinion on informal communities

and enormous user information can also be mined or disseminated for malicious or nefarious purpose [3]. In online social networks, programmed social bots can't speak to the genuine cravings and expectations of ordinary people, so they are normally viewed malicious ones. For instance, some fake social bots accounts made to copy the profile of an ordinary user, take user information and compromise their protection [4], scatter pernicious or counterfeit data, malicious comment, promote or advance certain political or philosophy plan and purposeful publicity [7], and impact the securities exchange and other cultural and efficient business sectors [8]. Such exercises can unfavorably affect the security and steadiness of person to social networking platforms.

2] LITERATURE SURVEY:

2.1]E. Van Der Walt,***et al***

There are a developing number of individuals who hold accounts via social media platforms (SMPs) yet conceal their character for malicious purposes. Unfortunately, very little research has been done to date to detect fake identities created by humans, especially so on SMPs. Conversely, numerous models exist of situations where fake accounts created by bots or PCs have been detected successfully using machine learning models. On account of bots these AI models were dependent on employing engineered features, such as the "friend-to-followers ratio. "These highlights were designed from attributes, for example, "friend-count" and "follower-count, "which are directly available in the account profiles on SMPs.

The exploration talked about in this paper applies these equivalent designed features to a set of fake human accounts in the hope of advancing the successful detection of fake identities created by humans on SMPs.

2.2] Z. Zhang,***et al***

The previous decade has seen the rise and progress of multimedia social networks (MSNs), which have dangerously and hugely expanded to enter each edge of our lives, recreation and work. In addition, portable Internet and versatile terminals empower users to admittance to MSNs at whenever, anyplace, for the benefit of any personality, including job and group. In this manner, the connection practices among users and MSNs are getting more extensive and confounded. This paper principally broadened and improved the circumstance examination structure for the particular social area, named as SocialSitu, and further proposed a novel calculation for users'

expectation serialization investigation dependent on exemplary Generalized Sequential Pattern (GSP). We utilized the enormous volume of user behaviors records to investigate the continuous grouping mode that is important to foresee user goal.

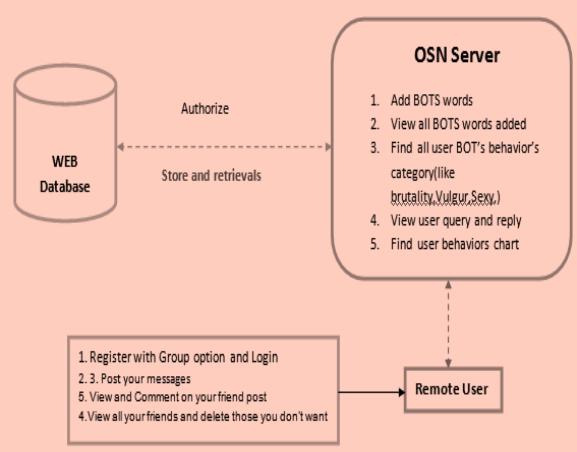
3] PROBLEM DEFINTION:

User behavior is the most immediate indication of user plan, as various users have various propensities, inclinations, and online behavior. we might have the option to mine and break down data covered up in user's online behavior to profile and recognize various users. However, we additionally should be aware of situational factors that may assume a job in changing user's online conduct. As such, user conduct is dynamic and its condition is continually changing i.e., outer noticeable environment of utilization setting and the hidden condition in user data.

4] PROPOSED APPROACH:

We mean to detect malicious social bots on social organization stages continuously, by (1) proposing the change probability highlights between user clickstreams dependent on the social circumstance analytics; and (2) structuring a algorithm for detecting malicious social bots dependent on spatiotemporal highlights To check the exactness of the strategy, the support vector machine model dependent on transition probability, the semisupervised clustering technique dependent on blended element, the supervised clustering strategy dependent on transition probability, and the semi-supervised clustering technique dependent on quantitative component are built up in similar informational data set. Social situation analytics can be used to acquire the external observable environment of applied scenarios and the hidden environment of user information in time.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

IDENTIFIER:

The IDENTIFIER has to login by using valid user name and password. Identifier find all social bot user behavior. Identifier can view the optimized result.

DATA COLLECTION:

In the realistic environment, for your own website, we can use the buried technology to get the corresponding data; for other

websites, we need to get the data by working with the website or by calling the corresponding. In the real social network platform, many platforms use the burying technology to obtain the user's behavior data.

OSN SERVER:

The OSN Server has to login by using valid user name and password. OSN Server can add some BOTS words to the database and view the all words added by him and based on that negative words admin can find all users behavior and also produce chart for that behavior words.

USER:

There are n numbers of users are present. User should register with group option before doing some operations. Login successful he will do some operations like view profile details, Search friends based on keyword or friends name, view the friend requests, post message with image to all friends. Find posts of friends and comment on that posts.

7] ALGORITHM:

DETECTION ALGORITHM FOR MALICIOUS SOCIAL BOTS:

Input: The log set of users' click stream sequence

Output: Normal user set, Social bot user set

Step 1: Refers to the users click stream sequence

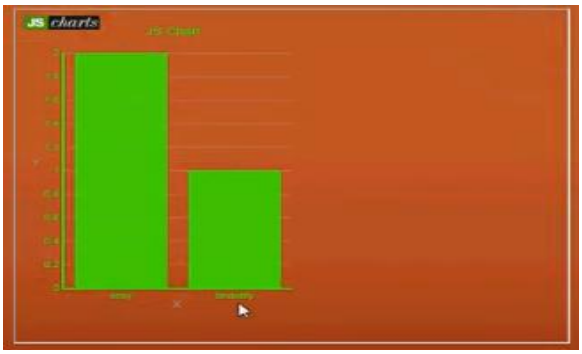
Step 2: generate the user's intent sequence sets

Step 3: Calculate the transition probability like, comment, share etc.,

Step 4: identify the user behaviors based on comments.

Step 5: divide the normal user and social bot user.

.8] RESULTS:



The user behavior, if any user uses the malicious words it calculated as social bot. In these graphs we will identify the user behavior.

9] CONCLUSION:

We proposed a new technique to recognize malicious social bots in online social

organizations. Investigations indicated that progress probability between user clickstreams dependent on the social circumstance analytics can be utilized to detect malicious social bots in online social stages accurately.

10] EXTENSION WORK

We will use supervised learning algorithm and extra behaviors of malicious social bots will be additionally thought of and the proposed detection approach will be stretched out and upgraded to identify specific aims and purposes of a more extensive scope of malicious social bots.

11] 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 network Websites 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 socialnetwork-based online promotions,’’ IEEE Access, vol. 5, pp. 1990–1999, 2017.

[10] Z. Zhang, C. Li, B. B. Gupta, and D. Niu, ‘‘Efficient 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.

[11] C. Cai, L. Li, and D. Zengi, ‘‘Behavior enhanced deep bot detection in social media,’’ in Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI), Beijing, China, Jul. 2017, pp. 128–130.

[12] C. K. Chang, ‘‘Situation analytics: A foundation for a new software engineering paradigm,’’ Computer, vol. 49, no. 1, pp. 24–33, Jan. 2016.

[13] Z. Zhang, R. Sun, X. Wang, and C. Zhao, ‘‘A situational analytic method for user behavior pattern in multimedia social networks,’’ IEEE Trans. Big Data, to be published. doi: 10.1109/TBDATA.2017.2657623.

[14] S. Barbon, Jr., G. F. C. Campos, G. M. Tavares, R. A. Igawa, M. L. Proença, Jr., and R. C. Guido, ‘‘Detection of human, legitimate bot, and malicious bot in online social networks based on wavelets,’’ ACM Trans. Multimedia Comput., Commun., Appl., vol. 14, no. 1s, Feb. 2018, Art. no. 26.

[15] J. Y. Park, N. O’Hare, R. Schifanella, A. Jaimes, and C.-W. Chung, ‘‘A large-scale study of user image search behavior on the Web,’’ in Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst., Seoul, South Korea, 2015, pp. 985–994.

Mr. D. Sasikanth is a student of Kakinada Institute of Engineering & Tech., Coringa, East Godavari Dist, AP. Presently he is pursuing his M.Tech [Software Engineering] from this college and he received his B.Tech from Kakinada Institute of Engineering & Technology, affiliated to JNT University, Kakinada in the year 2016. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr. D. Srinivas B.Tech., M.Tech is associate professor in Kiet Engineering College. He has 10 years of teaching experience. His area of interest includes Data mining, Networking, Bioinformatics and data science