Q
Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

DETECTING MALICIOUS SOCIAL BOTS USING CLICK STREAM SEQUENCES

M. RAMAKRISHNA

M. Ramakrishna, Assistant Professor CSE, Vaagdevi College Of Engineering(Autonomous), India

V. Manaswini, UG Student, CSE, Vaagdevi College Of Engineering(Autonomous), India

M. Vineeth, UG Student, CSE, Vaagdevi College Of Engineering(Autonomous), India

P. SaiKumar, UG Student, CSE, Vaagdevi College Of Engineering(Autonomous), India

S. SaiKumar, UG Student, CSE, Vaagdevi College Of Engineering(Autonomous), India

Q
Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

DETECTING MALICIOUS SOCIAL BOTS BASED ON CLICK STREAM SEQUENCES

ABSTRACT

Twitter is another web application assuming double parts of online person to person communication and microblogging. Clients speak with one another by distributing text-based posts. The prevalence and open design of Twitter have pulled in an enormous number of computerized programs, known as bots, which give off an impression of being a twofold edged sword to Twitter. Genuine bots create a lot of amiable tweets conveying news and refreshing channels, while vindictive bots spread spam or malignant substance. All the more strangely, in the center among human and bot, there has arisen cyborg alluded to either bot-helped human or human-helped bot. To help human clients in distinguishing who they are cooperating with, this paper centers around the grouping of human, bot, and cyborg accounts on Twitter. We first lead a bunch of enormous scope estimations with an assortment of more than 500,000 records. We notice the distinction among human, bot, and cyborg as far as tweeting conduct, tweet substance, and record properties. In light of the estimation results, we propose an arrangement framework that incorporates the accompanying four sections: 1) an entropy-based part, 2) a spam location segment, 3) a record properties segment, and 4) a chief. It utilizes the blend of highlights extricated from an obscure client to decide the probability of being a human, bot, or cyborg. Our trial assessment exhibits the viability of the proposed characterization framework.

1. INTRODUCTION

TWITTER is a mainstream online person to person communication and microblogging device, which was delivered in 2006. Striking straightforwardness is its particular element. Its people group cooperates by means of distributing text-based posts, known as tweets. The tweet size is restricted to 140 characters. Hashtag, in particular words or expressions prefixed with a # image, can amass tweets by point. For instance, #Justin Bieber and #Women's World Cup are the two moving hashtags on Twitter in 2011 [1]. Image @ followed by a username in a tweet empowers the direct conveyance of the tweet to that client. Not at all like generally on the web interpersonal interaction destinations (i.e., Facebook and MySpace), Twitter's client relationship is coordinated and comprises of two closures, companion and adherent. For the situation where the client An adds B as a companion, A will be a devotee of B while B is a companion of A. In Twitter terms, A follows B (specifically, the

accompanying relationship is unidirectional from A to B). B can likewise add An as his companion (specifically, following back or restoring the follow), yet isn't needed. At the point when An and B follow one another, the relationship gets bidirectional. From the outlook of data stream, tweets stream from the source (creator) to endorsers (supporters). All the more explicitly, when a client posts tweets, these tweets are shown on both the creator's landing page and those of his supporters. As revealed in August 2011, Twitter has pulled in 200 million clients and produced 8.3 million Tweets for every hour [2]. It positions the tenth on the best 500 site list as indicated by Alexa in December 2011 [3]. In November 2009, Twitter accentuated its incentive as a news and data network by changing the inquiry over the tweet input discourse box from "What are you doing" to "What's going on." To a few degree, Twitter has changed from an individual microblogging website to a data distributing scene. Numerous conventional ventures have utilized Twitter as another media channel. We have seen fruitful Twitter applications in business advancement [4], client support [5], political battling [6], and crisis correspondence.

The developing client populace and open nature of Twitter have made itself an ideal objective of abuse from computerized programs, known as bots. Like existing bots in other web applications (i.e., Internet visit [7], online journals [8] and internet games [9], bots have been basic on Twitter. Twitter doesn't assess carefully on robotization. It as it were requires the acknowledgment of a CAPTCHA picture during enrollment. In the wake of acquiring the login data, a bot can perform most human assignments by calling Twitter APIs. More curiously, in the center among people and bots have arisen cyborgs, which allude to either bot-helped people or on the other hand human-helped bots. Cyborgs have gotten normal on Twitter. After a human registers a record, he may set robotized programs (i.e., RSS channel/blog gadgets) to post tweets during his nonattendance. Occasionally, he partakes to tweet and collaborate with companions. Not quite the same as bots which extraordinarily use computerization, cyborgs join qualities of both manual and mechanized conduct. Robotization is a twofold edged sword to Twitter. On one hand, authentic bots create a huge volume of favorable tweets, similar to news and blog refreshes. This conforms to the Twitter's objective of turning into a news and data organization. Then again, pernicious bots have been incredibly misused by spammers to spread spam. The meaning of spam in this paper is spreading malignant, phishing, or spontaneous business content in tweets. These bots arbitrarily add clients as their companions, anticipating a couple of clients to follow back.1 thusly, spam tweets posted by bots show on clients' landing pages.

Captivated by the engaging content, a few clients may tap on connections and get diverted to spam or vindictive sites.2 If human clients are encircled by vindictive bots and spam tweets, their twittering experience falls apart, and at last the entire Twitter people group will be harmed. The target of this paper is to describe the robotization highlight of Twitter accounts, and to arrange them into three classifications, human, bot, and cyborg, as needs be. This will assist Twitter with dealing with the local area better and assist human clients with perceiving who they are tweeting with.

In the paper, we first lead a progression of estimations to portray the distinctions among human, bot, and cyborg regarding tweeting conduct, tweet content, and account properties. By creeping Twitter, we gather over 500,000 clients and in excess of 40 million tweets posted by them. At that point, we play out a nitty gritty information examination, and discover a set of valuable highlights to group clients into the three classes. In view of the estimation results, we propose a computerized characterization framework that comprises of four significant

1. the entropy segment utilizes tweeting stretch as a proportion of conduct intricacy, and recognizes the intermittent and normal planning that is a marker of robotization;

2. the spam discovery segment utilizes tweet substance to check whether text designs contain spam or not3

3. the record properties segment utilizes valuable account properties, for example, tweeting gadget cosmetics, URL proportion, to recognize deviations from typical; and

4. the chief depends on Random Forest, and it utilizes the mix of the highlights created by the over three segments to classify an obscure client as human, bot, or cyborg.

We approve the viability of the grouping framework through our test informational collection. We further apply the framework to order the whole informational index of more than 500,000 clients gathered, and hypothesize the current creation of Twitter client populace based on our order results.

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

The rest of this paper is coordinated as follows: Area 2 covers related work on Twitter and online social networks. Segment 3 subtleties our estimations on Twitter. Area 4 portrays our programmed grouping framework on Twitter. Area 5 presents our test results on characterization of people, bots, and cyborgs on Twitter. At last, Section 6 finishes up the paper[10].

2.LITERATURE SURVEY

The presence of bots has been felt in numerous parts of online media [11]. Twitter, one illustration of online media, has particularly felt the effect, with bots representing an enormous segment of its clients. These bots have been utilized for malevolent errands, for example, spreading bogus data about political applicants and expanding the apparent prominence of superstars. Moreover, these bots can change the aftereffects of normal examinations performed via online media [12]. It is significant that scientists and experts have devices in their weapons store to eliminate them. Approaches exist to eliminate bots, anyway they center around accuracy to assess their model at the expense of review. This implies that while these methodologies are quite often right in the bots they erase, they at last erase not many, hence numerous bots remain. We propose a model which expands the review in distinguishing bots, permitting a scientist to erase more bots. We assess our model on two genuine online media datasets and show that our location calculation eliminates a greater number of bots from a dataset than current methodologies [13].

Online interpersonal organizations (OSNs) [14] slowly incorporate monetary abilities by empowering the utilization of genuine and virtual money. They fill in as new stages to have an assortment of business exercises, for example, online advancement occasions, where clients can get virtual money as remunerations by taking an interest in such occasions. Both OSNs and colleagues are altogether concerned when assailants instrument a bunch of records to gather virtual money from these occasions, which make these occasions inadequate and bring about critical monetary misfortune. It happens to extraordinary significance to proactively identifying these noxious records before the online advancement exercises and accordingly diminishes their need to be remunerated. In this paper, we propose a novel framework, in particular ProGuard [15], to achieve this goal by deliberately incorporating highlights that describe accounts from three viewpoints including their overall practices, their reviving examples, and the utilization of their money. We have performed broad trials dependent on information gathered from the Tencent QQ, a worldwide driving OSN with

worked in monetary administration exercises. Trial results have shown that our framework can achieve a high discovery pace of 96.67% at a low bogus positive pace of 0.3%.

In a quality based encryption [16], the client is related to help of certain ascribes and their capacities for encryption and unscrambling of the information. The current strategies dependent on property based encryption have discovered that if client's entrance structure incorporates a lot of quality data marked as Don't Care, at that point the encryption matching activity has low figuring proficiency and ciphertext data excess [17]. In this paper, we have proposed a progressive multi-authority trait put together encryption with respect to prime request gatherings to handle these issues. Our encryption method has a polycentric characteristic approval framework dependent on an AND entryway access structure, with a bound together trait file set up by each property authority all through the framework, to shape a parallel tree, i.e., quality access tree. The state estimation of the parent hub can be controlled by the condition of its youngster hub in a trait access tree. The quality based encryption set up as such is hypothetically demonstrated to successfully diminish [18] the estimation sum for unscrambling and pack the excess data in the ciphertext however much as could be expected. Our encryption procedure has a hypothetical and pragmatic importance in the arrangement of "huge universe"constructions [19].

Social bots are viewed as the most well-known sort of malwares in social stage. They can deliver counterfeit messages, spread bits of gossip, and even control popular assessments. As of late, huge social bots are made and broadly spread in social stage, they carry negative impacts to public and netizen security. Bot identification means to recognize bots from human and it gets an ever increasing number of considerations as of late. In this paper, we propose a conduct upgraded profound model (BeDM) [20] for bot recognition. The proposed model views client content as transient content information rather than plain content to remove idle worldly examples. Besides, BeDM wires content data and conduct data utilizing profound learning strategy. To the most awesome aspect our insight, this is the primary preliminary that applies profound neural organization in bot location [21] . Trials on genuine world dataset gathered from Twitter likewise exhibit the viability of our proposed model.

The previous decade has seen the development and progress of sight and sound informal organizations (MSNs), [22] which have dangerously and massively expanded to infiltrate each side of our lives, relaxation and work. Besides, portable Internet and versatile terminals empower clients to admittance to MSNs at whenever, anyplace, for the benefit of any character, including job and

gathering. In this way, the collaboration practices among clients and MSNs are getting more extensive and muddled. This paper fundamentally expanded and improved the circumstance examination system for the particular social area, named as SocialSitu, and further proposed a novel calculation for clients' goal serialization investigation dependent on exemplary Generalized Sequential Pattern (GSP) [23]. We utilized the gigantic volume of client practices records to investigate the continuous succession mode that is important to foresee client expectation. Our examination chose two general sorts of aims: playing and sharing of media, which are the most well-known in MSNs, in view of the goal serialization calculation under various least help limit (Min_Support) [24]. By utilizing the clients' infinitesimal practices examination on goals, we found that the ideal personal conduct standards of every client under the Min_Support, and a client's personal conduct standards are diverse because of his/her character varieties in a huge volume of meetings information.

In online informal communities (OSNs) [24], spam beginning from companions and colleagues lessens the delight of Internet surfing as well as purposes harm to less security-sharp clients. Earlier countermeasures battle OSN spam from various points. Because of the variety of spam, there is not really any current technique that can autonomously identify the greater part or the vast majority of OSN spam. In this paper, we experimentally investigate the printed example of an enormous assortment of OSN spam. A moving finding is that the dominant part (63.0%) of the gathered spam is produced with basic formats. We hence propose removing formats of spam identified by existing strategies and afterward coordinating messages against the layouts toward exact and quick spam location. We actualize this understanding through Tangram, an OSN spam sifting framework that performs online review on the surge of client produced messages. Tangram naturally separates OSN spam into fragments and uses the sections to develop formats to channel future spam. Test results show that Tangram is profoundly precise and can quickly create layouts to choke recently arose crusades [25]. In particular, Tangram recognizes the most pervasive format based spam with 95.7% genuine positive rate, though the current layout age approach distinguishes just 32.3%. The combination of Tangram and its helper spam channel accomplishes a general precision of 85.4% genuine positive rate and 0.33% bogus.

The Turing test found out if one could perceive the conduct of a human from that of a PC calculation. Today this inquiry has unexpectedly gotten exceptionally significant with regards to online media, where text imperatives limit the expressive force of people, and genuine motivations

proliferate to create human-mirroring programming specialists called social bots. These slippery elements fiercely populate online media biological systems, regularly going unnoticed among the number of inhabitants in genuine individuals. Bots can be benevolent or hurtful, targeting convincing, spreading, or deluding. Here we examine the attributes of present day, modern social bots, and how their quality can imperil online environments and our general public. We at that point talk about current endeavors focused on location of social bots in Twitter. Attributes identified with content, organization, assessment, and transient examples of movement are imitated by bots and yet can help separate manufactured practices from human ones, yielding marks of designed social altering.

The Social Mediator discussion was made to connect the holes between the hypothesis and practice of web-based media innovative work. The articles are expected to advance more noteworthy consciousness of new bits of knowledge and encounters in the quickly developing space of web-based media, some of which may impact points of view and approaches in the more settled territories of human-PC cooperation. Each article in the discussion is comprised of a few short commitments from individuals addressing alternate points of view on a specific subject. Past portions of this discussion have woven together assorted points of view on the ways that online media is changing connections among various partners in the domains of medical care and government. The current article features a portion of the ways social robots (socialbots) [25]- - programs that work self-rulingly on informal communication destinations - are changing connections inside those locales, and how these changes may all the more comprehensively impact connections among individuals and associations later on. A new article in Communications of the ACM called "The Social Life of Robots" announced that "analysts have begun to investigate the prospects of 'social' machines equipped for cooperating with insignificant human oversight" [26]. That article enlightens late improvements including collaborations among people and robots in the actual world; this article centers around the associations among people and robots in the virtual world. Our creators are investigating and extending the wildernesses of planning, sending, and dissecting the conduct and effect of robots working in online informal communities, and they have welcomed various other frontierspeople to share a portion of their bits of knowledge, encounters, and future assumptions for social mechanical technology.

Online informal communities (OSNs) continuously incorporate monetary capacities by empowering the use of genuine and virtual money. They fill in as new stages to have an assortment of

business exercises, for example, online advancement occasions, where clients can get virtual money as remunerations by taking an interest in such occasions. Both OSNs and colleagues are fundamentally concerned when aggressors instrument a bunch of records to gather virtual cash from these occasions, which make these occasions incapable and bring about critical monetary misfortune. It is the fate critical to proactively identifying these malevolent records before the online advancement exercises and thusly diminishes their need to be compensated. In this paper, we propose a novel framework, to be specific ProGuard, to achieve this goal by efficiently coordinating highlights that describe accounts from three points of view including their overall practices, their energizing examples, and the use of their money. We have performed broad trials dependent on information gathered from the Tencent QQ, a worldwide driving OSN with worked in monetary administration exercises. Test results have shown that our framework can achieve a high identification pace of 96.67% at an exceptionally low bogus positive pace of 0.3%

In a property based encryption, the client is related to help of certain ascribes and their capacities for encryption and unscrambling of the information. The current procedures dependent on quality based encryption have discovered that if client's entrance structure incorporates a lot of characteristic data marked as Don't Care, at that point the encryption matching activity has low count proficiency and ciphertext data repetition. In this paper, we have proposed a progressive multi-authority property put together encryption with respect to prime request gatherings to handle these issues. Our encryption strategy has a polycentric quality approval framework dependent on an AND entryway access structure, with a bound together characteristic list set up by each trait authority all through the framework, to shape a parallel tree, i.e., property access tree. The state estimation of the parent hub can be dictated by the condition of its youngster hub in a trait access tree. The quality based encryption set up thusly is hypothetically demonstrated to successfully diminish the estimation sum for unscrambling and pack the excess data in the ciphertext however much as could be expected. Our encryption method has a hypothetical and useful importance in the arrangement of "huge universe"constructions.

Social bots are viewed as the most widely recognized sort of malwares in social stage. They can deliver counterfeit messages, spread gossipy tidbits, and even control general assessments. As of late, huge social bots are made and broadly spread in social stage, they carry negative impacts to

public and netizen security. Bot recognition expects to recognize bots from human and it gets an ever increasing number of considerations as of late. In this paper, we propose a conduct upgraded profound model (BeDM) [24] for bot location. The proposed model sees client content as fleeting content information rather than plain content to separate inert worldly examples. Also, BeDM wires content data and conduct data utilizing profound learning strategy. To the most awesome aspect our insight, this is the primary preliminary that applies profound neural organization in bot identification. Trials on genuine world dataset gathered from Twitter additionally show the viability of our proposed model.

3 PROBLEM STATEMENT

Morstatter et al. proposed a heuristic-type managed BoostOR[26]model with expanding review rate to identify vindictive bots, which utilizing the extent of tweets sent to the distributed tweets on the Twitter, the mean length of tweets, URL, and sending stretch. Wang et al. built a semi-regulated clickstream comparability chart model for client conduct to distinguish strange records in Renren. As indicated by the social communications between clients of the Twitter client to recognize the dynamic, detached and idle clients, a directed AI strategy was proposed to distinguish social bots based on age, area and other static highlights of dynamic, aloof, and latent clients in the Twitter, just as cooperating individual, connection content, association topic, and some powerful qualities.

3.1 LIMITATION OF SYSTEM

Morstatter et al. proposed a heuristic-type oversaw BoostOR model with growing audit rate to distinguish noxious bots, which using the degree of tweets shipped off the appropriated tweets on the Twitter, the mean length of tweets, URL, and sending stretch. Wang et al. constructed a semi-directed clickstream equivalence diagram model for customer lead to recognize weird records in Renren. As shown by the social correspondences between customers of the Twitter customer to perceive the dynamic, segregated and inactive customers, a coordinated AI technique [25] was proposed to recognize social bots dependent on age, zone and other static features of dynamic, unapproachable, and dormant customers in the Twitter, similarly as participating individual, association content, affiliation theme, and some amazing characteristics.

4. PROPOSED SYSTEM

In this paper, we expect to distinguish malignant social bots on informal community stages continuously, by (1) proposing the change likelihood highlights between client clickstreams

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

dependent on the social circumstance examination; and (2) planning a calculation for recognizing vindictive social bots dependent on spatiotemporal highlights. In request to all the more likely recognize malevolent social bots in online informal communities, we dissect client conduct includes and distinguish change likelihood highlights between client clickstreams Based on the progress likelihood highlights and time span includes, a semi-administered social bots recognition strategy dependent on space-time highlights is proposed.

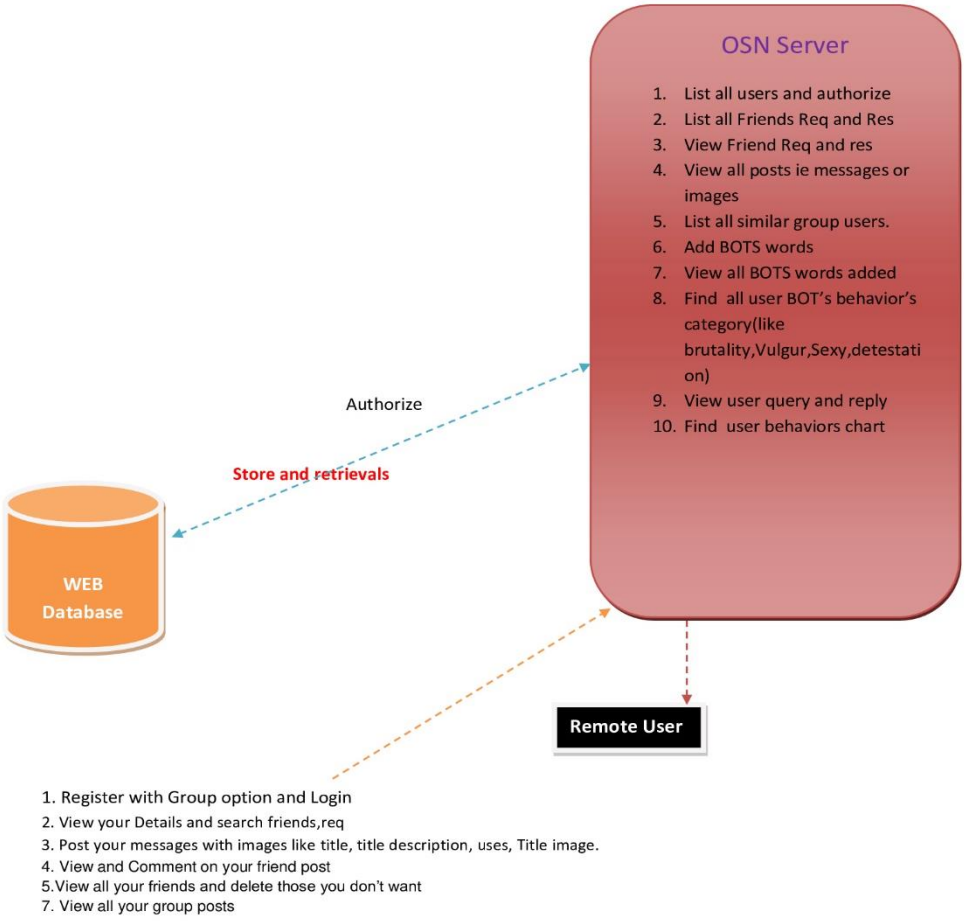
4.1 ADVANTAGES OF PROPOSED SYSTEM

We at that point break down and order circumstance mindful client practices in interpersonal organizations utilizing our proposed semisupervised grouping discovery strategy. This permits us to immediately distinguish noxious social bots utilizing just few labeled clients. To recognize possible noxious social bots in online interpersonal organizations progressively, we investigate the social circumstance conduct of clients in online informal communities. We likewise assess client conduct includes and select the change likelihood of client conduct based on broad conduct qualities. We at that point examine and group circumstance mindful client practices in informal organizations utilizing our proposed semisupervised bunching recognition strategy. This permits us to instantly identify malignant social bots utilizing just few labeled clients.

Q
Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

6.1 Data cleaning:

Information that are clicked less should be cleanedto eliminate wrong information, get precise change probabilitybetween clickstreams, and evade the blunder oftransition likelihood brought about by less information.

6.2 Data processing:

Some information are chosen haphazardly fromthe ordinary client set and social bots set to the label.Normal client account is named as 1, and the social botsaccount is named. Seed clients are characterized asthe classification of groups.

Q
Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

Q
Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

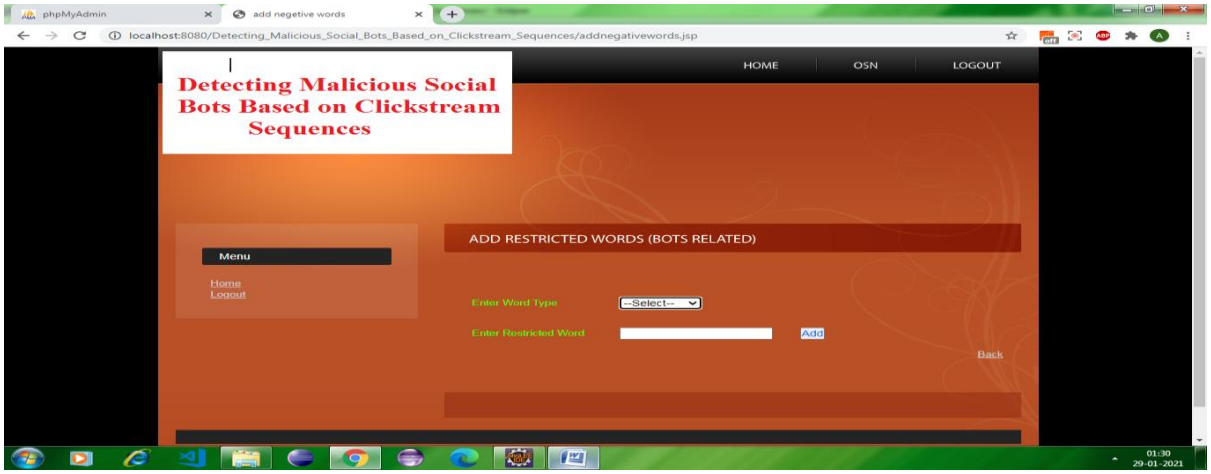
6.3 Feature selection:

In the spatial measurement: concurring tothe fundamental elements of the CyVOD stage, we selectthe change likelihood highlights identified with the playbackfunction: P(play;play), P(play;like), P(play;feedback),P(play;comment), P(play;share) and P(play;more); in the timedimension: we can get the between appearance times (IATs).Because if all progress likelihood lattices of userbehavior are built, amazingly gigantic information sizeand meager network can build the trouble of datadetection.

6.4 Semi-supervised clustering method:

To begin with, the initialcenters of two bunches are controlled by named seedusers. At that point, unlabeled information are utilized to repeat andoptimize the grouping results constantly.Obtain the ordinary client set and social bots set: the normaluser set and social bots set can be at last obtainedby identifying.

7. EXPECTED RESULTS



Q
Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

7. CONCLUSION

In this paper, we have considered the issue of robotization by bots and cyborgs on Twitter. As a mainstream web application, Twitter has become an exceptional stage for data imparting to an enormous client base. In any case, its ubiquity and extremely open nature have made Twitter an

exceptionally enticing objective for abuse via computerized programs, i.e., bots. The issue of bots on Twitter is additionally muddled by the key job that robotization plays in regular Twitter use. To more readily comprehend the job of mechanization on Twitter, we have estimated and described the practices of people, bots, and cyborgs on Twitter. By creeping Twitter, we have gathered one month of information with more than 500,000 Twitter clients with in excess of 40 million tweets. In light of the information, we have distinguished highlights that can separate people, bots, and cyborgs on Twitter. Utilizing entropy measures, we have established that people have complex timing conduct, i.e., high entropy, while bots and cyborgs are frequently parted with by their standard or intermittent timing, i.e., low entropy. In analyzing the content of tweets, we have seen that a high extent of bot tweets contain spam content. Ultimately, we have found that certain account properties, similar to outer URL proportion and tweeting gadget cosmetics, are useful on distinguishing mechanization.

In view of our estimations and portrayal, we have planned a robotized order framework that comprises of four fundamental parts: the entropy segment, the spam location part, the record properties segment, and the chief. The entropy part checks for intermittent or customary tweet timing designs; the spam location part checks for spam content; and the record properties segment checks for unusual estimations of Twitter-account-related properties. The choice producer sums up the recognized highlights and chooses regardless of whether the client is a human, bot, or cyborg.

The adequacy of the grouping framework is assessed through the test informational index. Also, we have applied the framework to characterize the whole informational index of more than 500,000 clients gathered, and estimated the current creation of Twitter client populace dependent on the characterization results.

8. FUTURE SCOPE

The project on detecting malicious social bots based on click stream sequences holds immense future potential. Its application spans across various domains including cybersecurity, social media analytics, and online platform integrity. By leveraging machine learning and behavioral analysis techniques, the project can evolve to detect increasingly sophisticated bot behaviors, enhancing online security measures. Furthermore, as social media continues to evolve, this technology could become integral in preserving the authenticity of interactions and content dissemination. Future

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

advancements may include real-time detection capabilities, integration with platform APIs for proactive bot mitigation, and collaboration with cybersecurity firms for broader industry impact.

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 53, Issue 5, May : 2024

9. REFERENCES

[1] F. Morstatter, L. Wu, T. H. Nazer, K. M. Carley, and H. Liu, ``A newapproach to bot detection: Striking the balance between precision andrecall," 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 abnormalbehavior 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, ``Detectingsocial-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, andB. 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," Common. 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 compressedciphertext length scheme using multi-authority CP-ABE for hierarchicalattributes," 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 insocial 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 engineeringparadigm," Computer, vol. 49, no. 1, pp. 24_33, Jan. 2016.

[13] Z. Zhang, R. Sun, X. Wang, and C. Zhao, ``A situational analytic methodfor user behavior pattern in multimedia social networks," IEEE Trans. BigData, 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 maliciousbot in online social networks based on wavelets," ACM Trans. MultimediaComput., 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.

[16] 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.

[17] Y. Liu, C.Wang, M. Zhang, and S. Ma, ``User behavior modeling for betterWeb search ranking," Front. Comput. Sci., vol. 11, no. 6, pp. 923_936,Dec. 2017.

[18] M. Al-Qurishi, M. S. Hossain, M. Alrubaian, S. M. M. Rahman, andA. Alamri, ``Leveraging analysis of user behavior to identify maliciousactivities in large-scale social networks," IEEE Trans. Ind. Informat.,vol. 14, no. 2, pp. 799_813, Feb. 2018.

[19] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, ``Botnet: Classi_-cation, attacks, detection, tracing, and preventive measures," EURASIPJ. Wireless Commun. Netw., vol. 2009, Dec. 2009, Art. no. 692654. doi:10.1155/2009/692654.

[20] Z. Chu, S. Gianvecchio, H.Wang, and S. Jajodia, ``Detecting automation oftwitter accounts: Are you a human, bot, or cyborg?" IEEE Trans. Depend.Sec. Comput., vol. 9, no. 6, pp. 811_824, Nov. 2012.

[21] E. Van Der Walt and J. Eloff, ``Using machine learning to detectfake identities: Bots vs humans," IEEE Access, vol. 6, pp. 6540_6549,Jan. 2018.

[22] C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer,``BotOrNot: A system to evaluate social bots," in Proc. 25th Int. Conf.Companion World Wide Web, Montreal, Canada, 2016, pp. 273_274.

[23] M. Fazil and M. Abulaish, ``Identifying active, reactive, and inactive targetsof socialbots in Twitter," in Proc. Int. Conf. Web Intell., Leipzig, Germany,2017, pp. 573_580.

[24] A. F. Costa, Y. Yamaguchi, A. J. M. Traina, C. Traina, Jr., and C. Faloutsos,``Modeling temporal activity to detect anomalous behavior in socialmedia," ACM Trans. Knowl. Discovery Data, vol. 11, no. 4, Aug. 2017,Art. no. 49.

[25] S. Basu, A. Banerjee, and R. Mooney, ``Semi-supervised clustering byseeding," in Proc. 19th Int. Conf. Mach. Learn., Sydney, NSW, Australia,2002, pp. 19_26.

[26] Z. Zhang, R. Sun, C. Zhao, J. Wang, C. K. Chang, and B. B. Gupta,``CyVOD:Anovel trinity multimedia social network scheme," MultimediaTools Appl., vol. 76, no. 18, pp. 18513_18529, Sep. 2017.