DETECT AND PREVENT THE MALICIOUS SOCIAL BOTS BASED ON CLICK STREAM SEQUENCE

MUTALA KESAVA BHARATH KUMAR [#1], L.SOWJANYA [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

In a recent survey ,we found that there is a great increase of malicious social bots which are spread on social media communication and it is very difficult for one to disseminate false information (e.g., fake news), and correct information in this real-world consequences. Hence it became very difficult to detect and removing malicious social bots in online social networks. If we come with the primitive detection methods, they used to analyze and detect the malicious social bots based on the quantitative features of their behavior.. Hence in this proposed application we try to identify the malicious bots which are present in the online social network communication by taking some set of pre-defined malicious bots into four categories like : Brutal,Vulgar,Sex And Detestation.Here in this proposed method we try to find out malicious social bots based on features selection as well as from the conversation which is done between individual users. If the conversation contain any of the words which are matched from the above categories then such conversation is immediately identified as malicious bots and such user is treated as malicious user and those details are recorded by the administrator.

1. INTRODUCTION

In online social networks, social bots are social accounts controlled by automated programs that can perform corresponding operations based on a set of procedures [1]. The increasing use of mobile devices (e.g., Android and iOS devices) also contributed to an increase in the frequency and nature of user interaction via social networks. It is evidenced by the significant volume, velocity and variety of data generated from the large online social network user base. Social bots have been widely deployed to enhance the quality and efficiency of collecting and analyzing data from social network services. For example, the social bot SF QuakeBot [2] is designed to generate earthquake reports in the San Francisco Bay, and it can analyze earthquake related information in social networks in real-time. However, public opinion about social networks and massive user data can also be mined or disseminated for malicious or nefarious purpose [3].

In online social networks, automatic social bots cannot represent the real desires and intentions of normal human beings, so they are usually looked upon malicious ones. For example, some fake social bots accounts created to imitate the profile of a normal user, steal user data and compromise their privacy [4], disseminate malicious or fake information [5], [6], malicious comment, promote or advance certain political or ideology agenda and propaganda [7], and influence the stock market and other societal and economical markets [8]. Such activities can adversely impact the security and stability of social networking platforms. In previous research, various methods were used to protect the security of online social network [9]_[11]. User behavior is the most direct manifestation of user intent, as different users have different habits, preferences, and online behavior (e.g., the way one clicks or types, as well as the speed of typing). In other words, we may be able to mine and analyze information hidden in user&#39;s online behavior to problem and identify different users. However, we also need to be conscious of situational factors that may play a role in changing user&#39;s online behavior. In other words, user behavior is dynamic and its environment is constantly changing _ i.e., external observable environment (e.g., environment and behavior) of application context and the hidden environment in user information [12]. In order to distinguish social bots from normal users accurately, detect malicious social bots, and reduce the harm of malicious social bots, we need to acquire and analyze social situation of user behavior and compare and understand the differences of malicious social bots and normal users in dynamic behavior.

PROJECT SCOPE

The most existing detection methods of malicious social bots analyse the quantitative features of their behavior. These features are easily imitated by social bots; thereby resulting in low accuracy of the analysis. Hence this motivated us to design a novel method in which we can able to find out malicious social bots based on features selection as well as from the conversation which is done between individual users. Specifically, in this paper, we aim to detect malicious social bots on social network platforms in real-time, 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. In this proposed method we try to find out malicious social bots based on features selection as well as from the conversation which is done between individual users. If the conversation contain any of the words which are matched from the above categories then such conversation is immediately identified as malicious bots and such user is treated as malicious user and those details are recorded by the administrator.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

In online social networks, automatic social bots cannot represent the real desires and intentions of normal human beings, so they are usually looked upon malicious ones. For example, some fake social bots accounts created to imitate the profile of a normal user, steal user data and compromise their privacy [4], disseminate malicious or fake information [5], [6], malicious comment, promote or advance certain political or ideology agenda and propaganda [7], and influence the stock market and other societal and economical markets [8]. Such activities can adversely impact the security and stability of social networking platforms. In previous research, various methods were used to protect the security of online social network [9]_[11].

User behavior is the most direct manifestation of user intent, as different users have different habits, preferences, and online behavior (e.g., the way one clicks or types, as well as the speed of typing). In other words, we may be able to mine and analyze information hidden in user&#39;s online behavior to problem and identify different users. However, we also need to be conscious of situational factors that may play a role in changing user's online behavior. In other words, user behavior is dynamic and its environment is constantly changing _ i.e., external observable environment (e.g., environment and behavior) of application context and the hidden environment in user information [12]. In order to distinguish social bots from normal users accurately, detect malicious social bots, and reduce the harm of malicious social bots, we need to acquire and analyze social situation of user behavior and compare and understand the differences of malicious social bots and normal users in dynamic behavior.

Blei et.al [3]:discussed about "Latent dirichlet allocation," the Journal of machine Learning research,describe latent Dirichlet allocation (LDA), a generative probabilistic model for collections of discrete data such as text corpora. LDA is a three-level hierarchical Bayesian model, in which each item of a collection is modeled as a finite mixture over an underlying set of topics. Each topic is, in turn, modeled as an infinite mixture over an underlying set of topic probabilities. In the context of text modeling, the topic probabilities provide an explicit representation of a document. Present efficient approximate inference techniques based on variational methods and an EM algorithm for empirical Bayes parameter estimation. Report results in document modeling, text classification, and collaborative filtering, comparing to a mixture of unigrams model and the probabilistic LSI model.

Yin et.al [5]: discussed about Social networking sites (SNS) is being rapidly increased in recent years, which provides platform to connect people all over the world and share their interests. However, Social Networking Sites is providing opportunities for cyberbullying activities. Cyberbullying is harassing or insulting a person by sending messages of hurting or threatening nature using electronic communication. Cyberbullying poses significant threat to physical and mental health of the victims.

III. EXISTING SYSTEM

The most existing detection methods of malicious social bots analyze the quantitative features of their behavior. These features are easily imitated by social bots; thereby resulting in low accuracy of the analysis. A novel method of detecting malicious social bots, including both features selection based on the transition probability of clickstream sequences and semi-supervised clustering, is presented.

LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They is as follows:

1. There is no method to identify the malicious bots accurately in the existing system.

2. There is no method to classify based on content as well as feature based

3. All the existing approaches are not accurate and efficient in identifying malicious social bots from OSN user communication.

IV. PROPOSED SYSTEM

In this proposed method we try to find out malicious social bots based on features selection as well as from the conversation which is done between individual users. If the conversation contain any of the words which are matched from the above categories then such conversation is immediately identified as malicious bots and such user is treated as malicious user and those details are recorded by the administrator.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system:

1. By using proposed social bots we can automatically read all the text which is posted by the users and recognize if there are any abused content available on that posted messages.

2. Consider the BoW system, by using this can maintain a bag of words is listed into a database and these bag of words are used for matching the dimensions of corresponding term which is posted on the wall.

3. The advantage of malicious bots is to segregate the messages into categories like malicious messages and normal messages individually.

V. IMPLEMENTATION

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed protocol. The application is divided mainly into following 2modules. They are as follows:

1. OSN Server Module
2. User Module

Now let us discuss about each and every module in detail as follows:

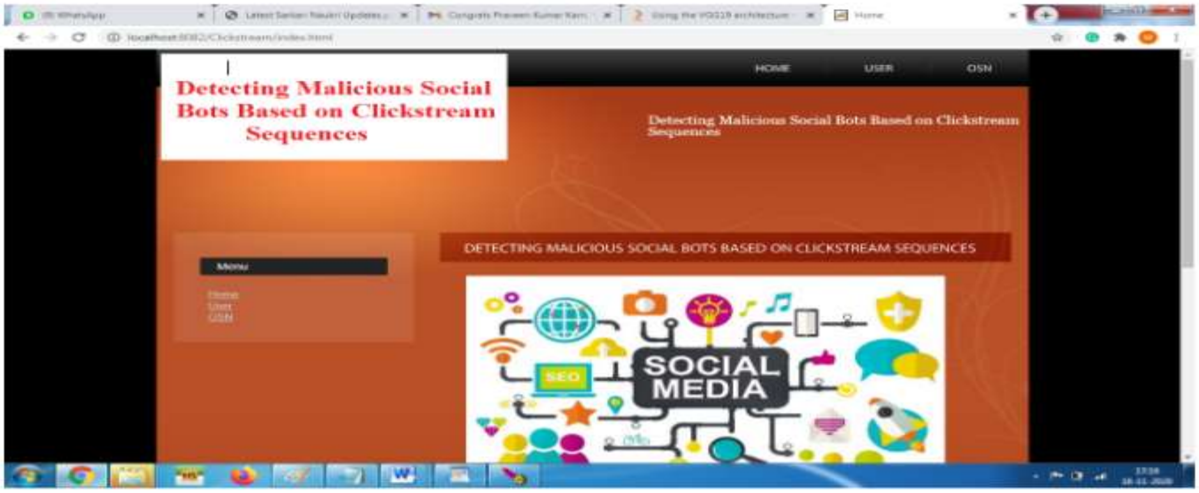
5.1 OSN Server MODULE

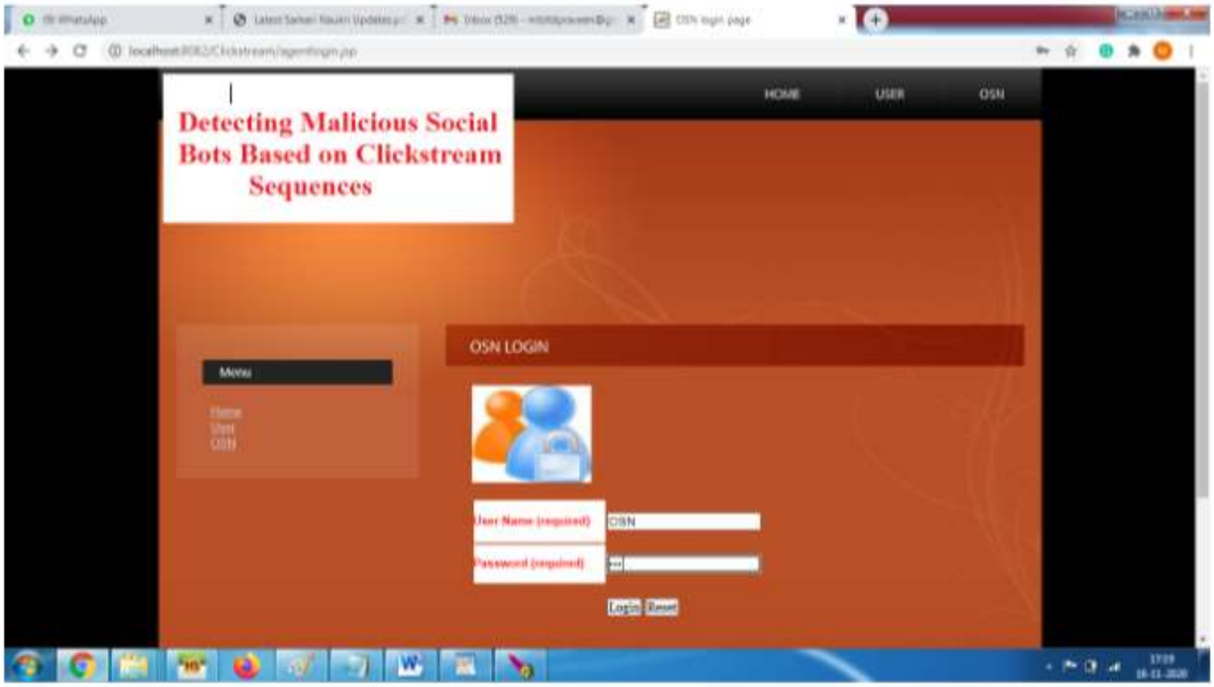
In this module, the OSN Server has to login by using valid user name and password. After login successful he can do some operations such as view all user details and authorize them, list of all friends requests and response ,View all posts like images and messages user, view all Similar group users like doctors, Engineers, Business Man, etc.,. 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.

5.2 USER MODULE

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized user can login by using authorized user name and password. 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. Users can also view all his friends and delete those who don't want, view all group posts like doctor or engineer etc

VI. OUTPUT RESULTS

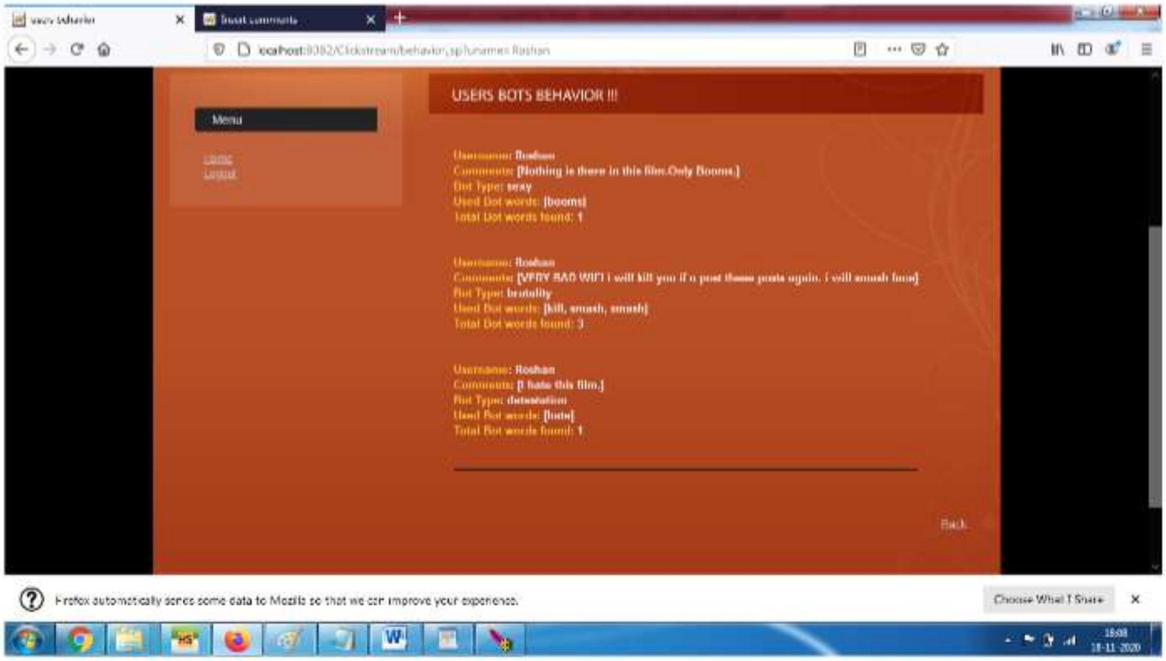

Detecting Malicious Social Bots Based on Clickstream Sequences
HOME
USER
OSN
Detecting Malicious Social Bots Based on Clickstream Sequences
DETECTING MALICIOUS SOCIAL BOTS BASED ON CLICKSTREAM SEQUENCES
Menu
Home
User
OSN
SOCIAL MEDIA
SEO


Detecting Malicious Social Bots Based on Clickstream Sequences
HOME
USER
OSN
OSN LOGIN
Menu
Home
User
OSN
Login
Reset

User Name (required) OSN

Password (required) ***

ADMIN CAN SEE THE USER ROSHAN POST APPEAR ON SOCIAL BOT



users behavior
Insert comments
localhost:8082/Clickstream/behavior.jsp?uname=Roshan
Menu
Home
Logout
Back
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
18:08
18-11-2020

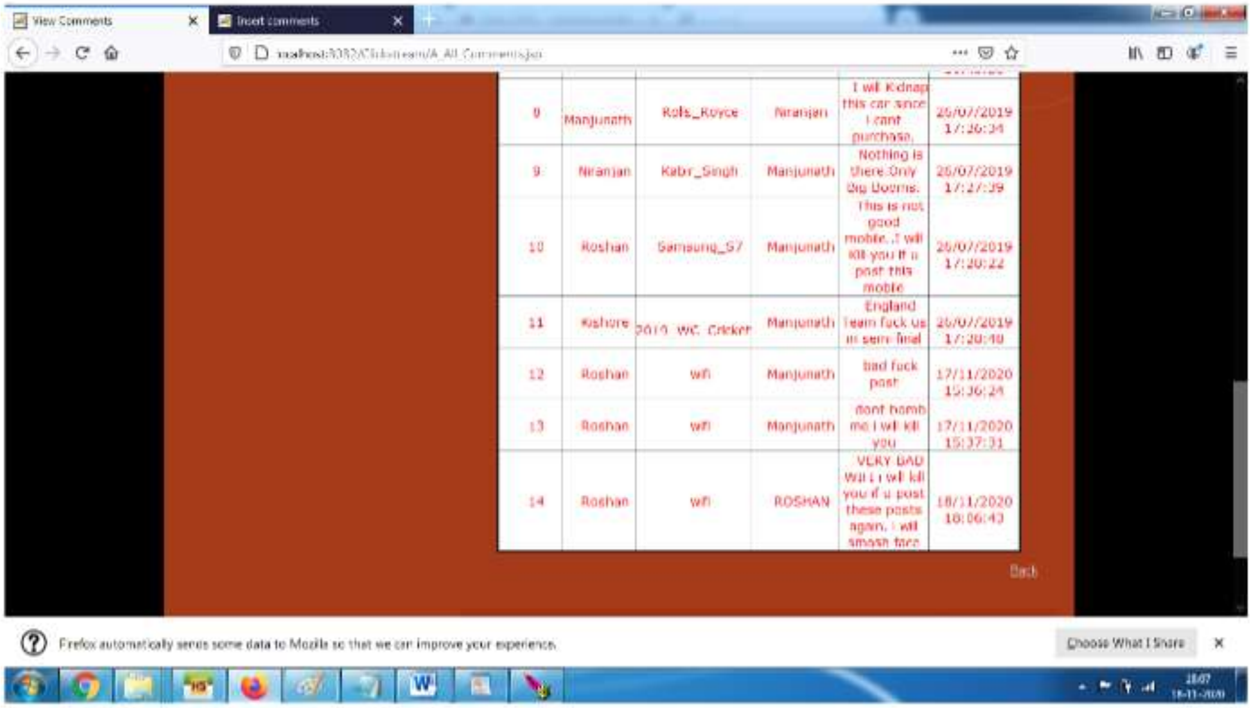
USERS BOTS BEHAVIOR !!!

Username: Roshan
Comments: [Nothing is there in this film.Only Booms.]
Bot Type: sexy
Used Bot words: [booms]
Total Bot words found: 1

Username: Roshan
Comments: [VERY BAD WIFI i will kill you if u post these posts again. i will smash face]
Bot Type: brutality
Used Bot words: [kill, smash, smash]
Total Bot words found: 3

Username: Roshan
Comments: [I hate this film.]
Bot Type: defamation
Used Bot words: [hate]
Total Bot words found: 1

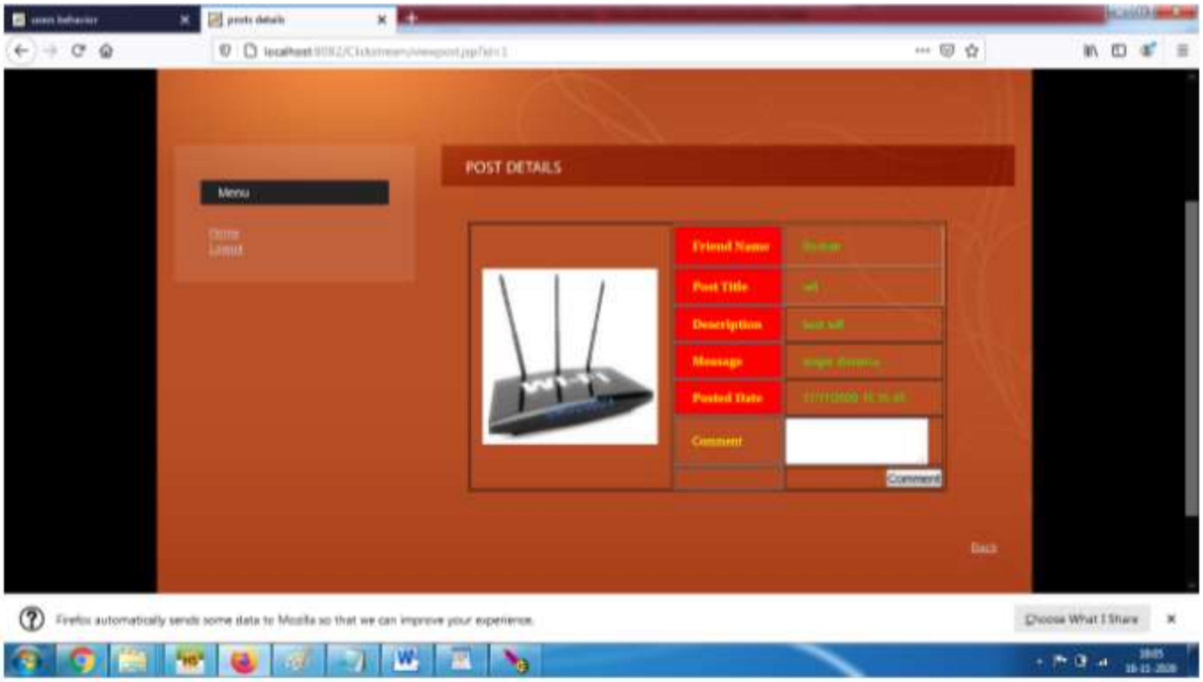
ADMIN CAN VIEW THE USER ROSHAN POSTED MESSAGE



View Comments
Insert comments
localhost:8082/Clickstream/A_All_Comments.jsp
Back
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
18:07
18-11-2020

9	Manjunath	Rols_Royce	Niranjan	I will Kidnap this car since I cant purchase.	26/07/2019 17:26:34
9	Niranjan	Kabir_Singh	Manjunath	Nothing is there.Only Big Booms.	26/07/2019 17:27:39
10	Roshan	Samsung_S7	Manjunath	This is not good mobile. I will kill you if u post this mobile	26/07/2019 17:28:22
11	Kishore	2019_WC_Cricket	Manjunath	England Team fuck us in semi final	26/07/2019 17:28:48
12	Roshan	wifi	Manjunath	bad fuck post	17/11/2020 15:36:24
13	Roshan	wifi	Manjunath	dont bomb me i will kill you	17/11/2020 15:37:31
14	Roshan	wifi	ROSHAN	VERY BAD Wifi i will kill you if u post these posts again. i will smash face	18/11/2020 18:06:43

ADMIN CAN GIVE COMMENTS FOR THE FRIENDS POST



POST DETAILS

Friend Name	[illegible]
Post Title	wifi
Description	best wifi
Message	[illegible]
Posted Date	17/11/2020 18:16:45
Comment	

Firefox automatically sends some data to Mozilla so that we can improve your experience.

VII . CONCLUSION

We proposed a novel method to accurately detect malicious social bots in online social networks. Experiments showed that transition probability between user click streams based on the social situation analytics can be used to detect malicious social bots in online social platforms accurately. In future research, additional behaviors of malicious social bots will be further considered and the proposed detection approach will be extended and optimized to identify specific intentions and purposes of a broader range of malicious social bots. It can be further improve the robustness of the learned representation by considering word order in messages and also using natural language processing techniques in order to predict any MALICOUS words which are not in the dataset and add the same by means of feedback into BoW database.

VIII. 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 withtemplates 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, ``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.