IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005125

A Hybrid Approach for Detecting Automated Spammers in Twitter Using Machine Learning: A Review

Anjali Machcha[1], Vaishnavi Misal[2], Suksham Pawar[3], Satyavan Pawar[4], Akshay Suryawanshi[5], Prof. Manisha Singh[6]

Student, Department of Computer Engineering, DPCOE - Dhole Patil College of Engineering, Pune, Maharashtra, India[12345]

Assistant Professor, Department of Computer Engineering, DPCOE - Dhole Patil College of Engineering, Pune, Maharashtra, India. [6]

ABSTRACT:Billions of people use social networking sites all over the world. User experiences with social media platforms such as Twitter have significant and often unfavorable consequences for everyday life. Spammers have turned to major social networking sites to disseminate a vast amount of useless and harmful content. Twitter has grown to be one of the most extravagant websites of all time, as well as one of the most influential micro blogging services, and is commonly used to spread an excessive amount of spam. Fake users submit inappropriate tweets to users in order to advertise services or websites, which not only annoy legitimate users but also waste resources. Furthermore, the risk of disseminating incorrect information to users through false identities has increased, leading to malicious material. The detection of spammers, as well as the identification of fake users and fake messages on Twitter, has recently become a hot topic in online social networks study (OSN). The techniques used to identify spammers on Twitter were proposed in this paper. Furthermore, a taxonomy of Twitter spam detection approaches is presented, which divides techniques into categories based on their ability to identify fake content, URL-based spam, and spam on trending topics. In a real-time data set that distinguishes users and spammers, twelve to nineteen different features, including six recently defined functions and two redefined functions, were described to learn two computer supervised learning classifiers.

KEYWORDS: Machine learning, parallel computing, spam detection, scalability, Twitter

I. INTRODUCTION

In recent years, online social networking platforms such as Twitter, Facebook, Instagram, and some online social networking firms have grown in popularity. People in OSN spend a lot of time making friends with people they know or are involved in.After its inception in 2006, Twitter has grown to become one of the most successful micro blogging platforms. For spam growth, about 200 million users generate about 400 million new tweets every day. Twitter spam, also known as unsolicited tweets containing malicious links that send nonstop victims to external sites containing malware, transmitting malicious links, and so on, affects not only more legitimate users, but also the entire network. Consider the case of the Australian Prime Minister, who received a note confirming that his Twitter account had been hacked during his election campaign in 2013.Many of his fans have sent email messages with malicious connections sent directly to their inboxes. For the academic and industrial worlds to uncover secret ideas and forecast patterns on Twitter, the ability to order valuable knowledge is critical. Spam, on the other hand, makes a lot of noise on Twitter. Researchers used machine learning algorithms to transform spam detection into a classification problem in order to detect spam automatically. In the real world, it's more practical to mark a tweet broadcast as spam or non-spam instead of a Twitter consumer.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005125

II. RELATED WORK

1. Alireza Bitarafan, Chitra Dadkhah" SPGD_HIN: Spammer Group Detection based on Heterogeneous Information Network" 2019 5th International Conference on Web Research (ICWR):-

   This article focused on the above, namely the identification of spammer groups. In most previous works, Frequent Item Set Mining (FIM) is used early on to find applicant classes, followed by an unsupervised rating process dependent on certain predefined features.
   This is used on Twitter to boost security and spot spammers using a machine learning algorithm.
   The biggest drawback is that it relies heavily on historical data to build the social graph.

2. FAIZA MASOOD1 , GHANA AMMAD1 , AHMAD ALMOGREN" Spammer Detection and Fake User Identification on Social Networks" IEEE Acess 2019:-

   The author of this paper conducts a study of strategies for identifying spammers on Twitter. Furthermore, a taxonomy of Twitter spam detection approaches is introduced, which categorizes strategies based on their ability to detect: I fake news, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users. The presented strategies are often compared based on different characteristics, such as user characteristics, material characteristics, graph characteristics, structure characteristics, and time characteristics.
   Its key drawback is that it lowers the barriers to account creation, weakens protections, and slows response time.

3. Aditi Gupta1 , Neetika Raina2 , Bharti Jha3 ,Vinay Kumar Jain4" Trending Topics based Spam Detection from the Social Media" ICACCCN 2018:-

   Spammers are users who share unsolicited and meaningless texts to a large number of users with the intent of selling a product or convincing people to click on unsecured links and infecting the user's system in order to make money (click bait). They frequently use trending trends on social media to spam. Spammers often produce spam and false trending, and they sometimes use Trending trends to entice victims to click on them. Most testing has been conducted and continues to be conducted in order to spot spammers in OSNs. This paper examines existing strategies for detecting spammers in social media. Our current research and future plans include an overview of standard classifiers, such as Nave Bayes and Support Vector Machines, and how they are used to identify spam and distinguish a dataset derived from social media into trending and non-trending topics based spam.
   It is used to do statistical analyses on the spam profiles.
   Its biggest drawback is that it consumes a lot of time and resources for the system.

4. M. Tsikerdekis, "Identity deception prevention using common contribution network data," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 188–199, 2017:-

   The activities of spammers on Twitter were studied by evaluating tweets sent by suspended users in retrospect. An emerging spam-as-a-service industry comprised of both legitimate and shady partner schemes, ad-based shortens, and Twitter account sellers.
   Its key benefits are that it is suitable for unbalanced classes, that it is simple to compute, and that it is suitable for gradual learning.
   The only drawback is that the Independence assumption for computing P^c is often violated.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005125

III. RESULTS OF THE BASE PAPER

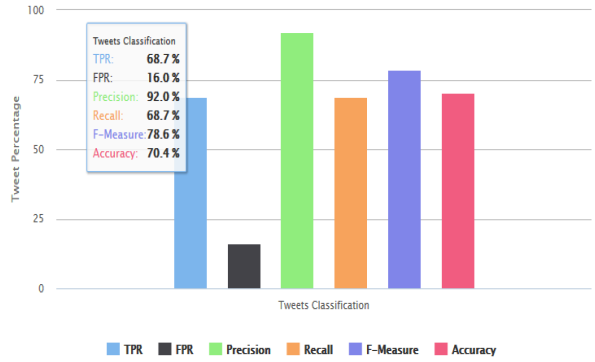

Fig. System Architecture

Parameters	Percentage
TPR	68.7
FPR	58.7
Precision	92.6
Recall	68.1
F-Measure	78.8
Accuracy	70.4

Advantages:

- This system categories the Spammers and Non-spammers.
- To work on a performance evaluation such as Precision, Recall, F-measure.
- This system categorize the tag based tweets and link based tweets.
- To try to improve detection accuracy using machine learning algorithms.

Disadvantages:

- Need Strong internet connection
- Not Worked on Shared link

IV. CONCLUSION

In this project, the system discovered that classifiers' ability to detect Twitter spam decreased in a near-real-world scenario due to imbalanced data. Feature discretization was also defined as an effective pre-process for machine learning-based spam detection by the system. Second, after a certain amount of testing samples, increasing training data would not have any further advantages for detecting Twitter spam. To increase the spam detection rate even further, the system should try to add more discriminative functionality or a better model.

REFERENCES

[1] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, “Aiding the detection of fake accounts in large scale social online services,” in Proc. Symp. Netw. Syst. Des. Implement. (NSDI), 2012, pp. 197–210.
[2] G. Stringhini, C. Kruegel, and G. Vigna, “Detecting spammers on social networks,” in Proc. 26th Annu. Comput. Sec. Appl. Conf., 2010, pp. 1–9.
[3] J. Song, S. Lee, and J. Kim, “Spam filtering in Twitter using sender receiver relationship,” in Proc. 14th Int. Conf. Recent Adv. Intrusion Detection, 2011, pp. 301–317.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005125

[4] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: social honeypots + machine learning," in Proc. 33rd Int. ACM SIGIR Conf. Res.Develop. Inf. Retrieval, 2010, pp. 435–442.
[5] Nathan Aston, Jacob Liddle and Wei Hu*, "Twitter Sentiment in Data Streams with Perceptron," in Journal of Computer and Communications, 2014, Vol-2 No-11.
[6] K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended accounts in retrospect: An analysis of Twitter spam," in Proc. ACM SIGCOMM Conf. Internet Meas., 2011, pp. 243–258.
[7] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time URL spam filtering service," in Proc. IEEE Symp. Sec. Privacy, 2011, pp. 447–462.
[8] X. Jin, C. X. Lin, J. Luo, and J. Han, "Socialspamguard: A data mining based spam detection system for social media networks," PVLDB, vol. 4, no. 12, pp. 1458–1461, 2011.
[9] S. Ghosh et al., "Understanding and combating link farming in the Twitter social network," in Proc. 21st Int. Conf. World Wide Web, 2012, pp. 61–70.
[10] H. Costa, F. Benevenuto, and L. H. C. Merschmann, "Detecting tip spam in location-based social networks," in Proc. 28th Annu. ACM Symp. Appl. Comput., 2013, pp. 724–729.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details