International Journal for Modern Trends in Science and Technology, 8(09): 91-94, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809016
Available online at: http://www.ijmtst.com/vol8issue09.html

Spammer Location and Phony Client Id on Informal Communication Framework

G Bharathi[1] | K Lakshmana Reddy[2]

[1]MCA , Department of Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
G Bharathi and K Lakshmana Reddy. Spammer Location and Phony Client Id on Informal Communication Framework. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 91-94. https://doi.org/10.46501/IJMTST0809016

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

Social Media influencing a million of users in the entire world. The social media sites are such as Twitter, Facebook, Instagram, Linked-in and etc…The social media effecting our daily life and at the same time our society.Twitter, for example, has become one of the most extravagantly used platforms of all times and allows an unreasonable amount of spam. Fake users in social media sending fake content and sending it to all over the world.

Spammers effecting the users and also disrupt resource consumption. The possibility of expanding invalid information to users through fake identities has increased those results in the unrolling of harmful content. Now the spammers are taking twitter as a platform to produce fake content. In this paper, we perform a review of techniques used for detecting spammers on Twitter and also the Twitter spam detection approaches is presented that classifies the techniques based on their ability to detect: (i) fake content, (ii) spam based on URL, (iii) spam in trending topics, and (iv) fake users.

.KEYWORDS:Spammer Detection, Fake users, Authentication, Filtering, Classification.

1. INTRODUCTION

It is very easy to obtain any kind of information from any source across the world by using the Internet. The increased demand of social sites permits users to collect abundant amount of information and data about users. Huge volumes of data available on these sites also draw in identifying fake identities of users.

Spammers can be identified based on become an online source for acquiring real-time information about users. Twitter is an Online SocialNetwork (OSN) where users can share anything and everything, such as ideas, images, news, opinions, and even their moods. Several arguments and debates can be held over different topics, such as politics, current issus, and important events. When a Twitter user tweets something, it is instantly conveyed to his/her followers, allowing them to outspread the received information. In this case we have to study and analyze the users behavior in social media platform. People who not aware of Spammers will be easily tricked. Recently, the detection of spam in social networking sites attracted the attention of researchers. Spam detection is a difficult task in maintaining the security of social networking systems.

For classification, we have identified four means of reporting spammers that can be helpful: (i) fake content,(ii) URL based spam detection, (iii) detecting

spam in trending topics, and (iv) fake user identification. Table 1 provides a comparison of existing techniques and helps users to recognize the significance and effectiveness of the proposed methodologies in addition to providing a comparison of their goals and results.. Despite all the existing studies, there is still a gap in the existing literature. Therefore, to bridge the gap, we review state-of-the-art in the spammer detection and fake user identification on Twitter.Tingminprovides an overviewof new methods and techniques for detecting Twitter spam. The above overview represents a comparative study of current approaches. on the other hand, the author conducted research on different behaviors of spammers on the social network Twitter.

Youcanhave multiple discussion so different to pics such as politics, current affairs, and important events. When a user tweets something, it is instantly broadcast to followers, allowing there ceived informationto be disseminated more widely.Withthe development of OSN, there is a growingneedtoresearchandanalyzeuser behavior ononlinesocialplatforms.Manypeoplewhodon't have much information about OSN can be easily duped by scammers. We also need to fight and control people who only use OSN for advertising andspamotherpeople'saccounts.Recently,spam detection on social networking sites has attracted the attention of researchers. Spam detection is a difficult task in maintaining social network security

2. LITERATURE SURVEY

From the survey, we analyzed that malicious activities on social media are being performed in several ways. Moreover, the researchers have attempted to identify spammers or unsolicited bloggers by proposing various solutions. Therefore, to combine all pertinent efforts, we proposed a taxonomy according to the extraction and classification methods. The categorization is based on various classifications such as fake content, URL based, trending topics, and by identifying fake users. The first major categorization in the taxonomy is of techniques proposed for detecting spam, which is injected in the Twitter platform through fake content. Spammers generally combine spam data with a topic or keywords that are malicious or contain the type of words that are likely to be spam. The second categorization considers the techniques for spam detection based on URLs.

Generally, because of the length-limit of tweet description, spammers and it more promising to post URL to spread malicious content than the plain normal text. Therefore, URL based methods are absolutely customized to determine tweets containing excess of URLs specifically on criminal accounts. The third category in the proposed taxonomy contains approaches meant for spam identification from trending topics on Twitter. Hashtag or keywords, which are often seen in tweets at a specific time, appear in the Twitter list of trending topics and are likely to contain spam. Various features for identifying spams in trending topics have been classified with a variety of attributes. The fourth category in the taxonomy is regarding techniques for the identification of fake users to detect spams on Twitter. An assortment of techniques has been introduced for detecting spams of fake users that helps to overcome malicious activities against OSN users.

3. PROBLEM STATEMEN

Shen et al. examined problems in detecting spammers on Twitter. The proposed method combines the functionality of disengagement from text content and information from social networks. The authors used matrix factorization to determine underlining matrices or tweets, and developed social regularization using interaction coefficients to teach underlining matrix factorization. Subsequently, the author combined their knowledge with social regularization and factorization matrix processes and conducted experiments on his real Twitter dataset. H. UDI Twitter Records, by.

Wosha et al.described a hidden Markov model for filtering spam in relation to recent time. This method supports accessible and retrievable information in the Tweet object to detect spam Tweets and previously featured Tweets on the same topic

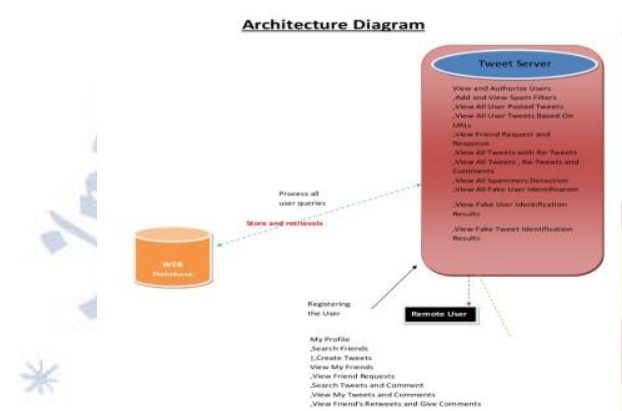
Chong et al. The Twitter follow spam analyzed was followed by spammers and followed by authorized users instead of spreading provocative public messages. Classification techniques used to detect follow spammers have been proposed. The focus of social relationships is cascaded and expressed through two mechanisms. H. Filtering Social Status and Commercial Importance.

Profile filtering. Each uses a two-hop sub-network centered on each other. Assembly techniques and cascade filtering have also been proposed to combine

properties of both trade importance profile and social status. In order to verify whether a user is fake or not, each user's two-hop social network focuses on collecting social information from social networks

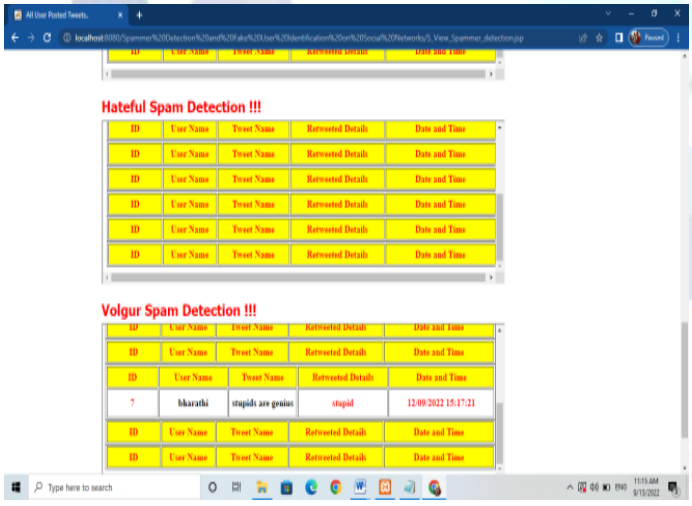
The proposed framework focuses on random forests and non-uniform features ampling techniques. Random Forecast classification and regression learning algorithm that works by assembling multiple decision trees during preparation and choosing the one with the highest number ofvotesin eachindividualtree. Thisscheme integrates bootstrap aggregation techniques with unplanned feature selection.

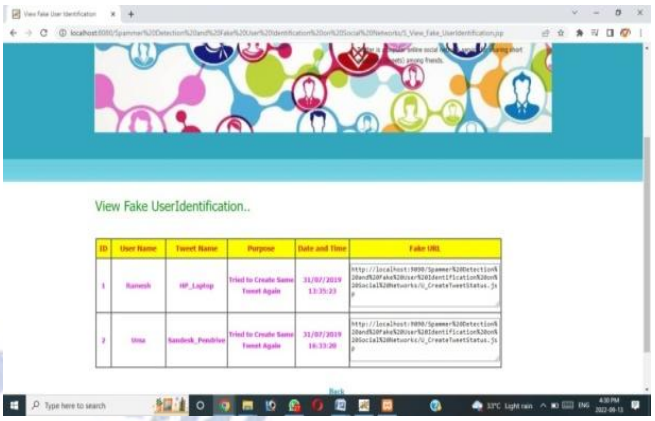
ARCHITECHTURE:



4.

RESULTS:





5. CONCLUSION

In this white paper, we examined techniques used to detect spammers on Twitter. We also presented a taxonomy of Twitter spam detection approaches, categorizing them into fake content detection, URL-based spam detection, trending topic spam detection, and fake user detection techniques. We also compared the presented techniques based on several characteristics such as: B. User Characteristics, Content Characteristics, Diagram Characteristics, Structure Characteristics, and Time Characteristics. In addition, these techniques were also compared with respect to the stated goals and the datasets used. It is hoped that the overview presented will help researchers find information about his Twitter spam detection technology on the cutting edge in a consolidated format. Despite the development of efficient and effective approaches to spam detection and identification of spoofed users on Twitter , there are still some unresolved areas that require significant attention from researchers. Thereis The problem is Briery is: Identification of fake news in social networks is a problem that needs to be studied at the individual and collective level because of the serious consequences of such news . Another related topic worth investigating is identifying the sources of rumors on social media. Some studies based on statistical methods have already been carried out to uncover the sources of rumors, but more sophisticated approaches, for example those based on the social networks, can be applied.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology, Vol. 27, pp. 206 – 211, 2007.

[2] Xiao Huijuan, QiuShuisheng, Deng Chengliang He Yong-Zhong, Cai Ying, "A Composite Image Encryption Scheme Using AES and Chaotic Series", The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007), pp. 277 – 279, 2007.

[3] Guanrong Chen, Yaobin Mao b, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, Vol. 21, 749 – 761, 2007.

[4] Ashtiyani, M. Birgani, P.M. Hosseini, H.M., "Chaos-Based Medical Image Encryption Using Symmetric Cryptography", Information and Communication Technologies: From Theory to Applications, ICTTA-08. 3rd International Conference on, pp. 1 – 5, Apr 2008.

[5] Zhenzhen Lv1, Lei Zhang2, and JianshengGuo, "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System", Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT '09) Huangshan, P. R. China, 26-28, pp. 191-194, Dec. 2009.

[6] Bibhudendra Acharya, GirijaSankarRath, Sarat Kumar Patra, Saroj Kumar Panigrahy, Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, 2007, pp. 14-21.

[7] AbdulkarimAmerShtewi, BahaaEldin M. Hasan, Abd El Fatah, A. Hegazy, "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems", IJCSNS International Journal of Computer Science and Network Security, Vol. 10 No. 2, pp. 226 – 232, Feb 2010.

[8] R. Lukac and K. Plataniotis. Bit-Level Based Secret Sharing for Image Encryption. Pattern Recognition, 38(5):767–772, May 2005.

[9] Rodrigues, J.M. Puech, W. Bors, A.G. "Selective Encryption of Human Skin in JPEG Images",IEEE International Conference on Image Processing, 2006.

[10] Puech, W.; Rodrigues, J.M.; Bors, A.G.,"Analysis and Cryptanalysis of a Selective Encryption Method for JPEG Images", Eighth International Workshop on Image Analysis for Multimedia Interactive Services, 2007. WIAMIS07, June 2007.

[11] V.U.K. Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix", International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, October 2012, pp.1-6.

[12] Alasdair Mcandrew, —Digital Image processing with MatLab, Cengage learning 2004.

[13] Rafael C. Gonzalez & Richard E. Woods,— Digital Image processing, 2ndEdition Pearson Education 2004

Authors Biography

G.BHARATHI Currently pursuing MCA in SVKP & DR. K.S.RAJU Arts & Science college affiliated to Adikavi Nannaya University, Rajamahendravaram. His research interests include Data Structures, Web Technologies, Operating System, Data Science and Artificial Inteligence.

K LAKSHAMANA REDDY isWorking as Associate Professor in SVKP &Dr K S Raju Arts & Science College(A), Penugonda , West Godavari District, A.P. He received Master's Degree in Computer Applications from Andhra University'C' level from DOEACC, New Delhi and M.Tech from Acharya Nagarjuna University, A.P. He attended and presented papers in conferences and seminars. He has done online certifications in several courses from NPTEL. His areas of interests include Computer Networks, Network Security and Cryptography, Formal Languages and Automata Theory and Object Oriented programming languages.