International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Identification of Malicious Posts in Facebook Social Networks

Sanjeev Dhawan[1], Kulvinder Singh[2] and Sanjay Sagwal[3]

[1, 2]Faculty of Computer Science and Engineering, Department of Computer Science and Engineering, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, Haryana, India.

[3]M. Tech. (Computer Engineering), University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, Haryana, India

ABSTRACT

A social network provides interconnectivity between millions of users. In social networks numbers of applications are available like Twitter, Google+ and Facebook through which people can connect with each other. In Facebook, user can add number of users and their friends in friend list. When a user adds more friends and their friends in his friend list then may be some of them could be malicious users and spread malicious spam's or misinformation through posts on user wall. In this paper, an attempt has been made to present comparative analysis of various existing techniques with different parameters to detect malicious posts in online social networks. This paper is divided into four sections. Section I covers introduction of social networks that includes brief discussion on Facebook. In section II literature review on different existing techniques proposed by different researchers to detect and prevent social network from malicious posts posted by malicious users. Section III presents proposed work and at last section IV presents comparison between existing techniques with their pros and cons.

Keywords: Social networks, Facebook, Posts, profile and Malicious users.

I. INTRODUCTION

People can exchange their information in the form of texts, images and videos with each other through social networks. In social networks people are represented as nodes and the connection between them represented as edges to connect them [1]. Number of social networks websites like LinkedIn, Google+, Twitter and Facebook are most used websites by users for communication purpose. Out of these websites, Twitter and Facebook are most used by user's means they are so enthusiastic to use these sites and make more friends and interact with them by sharing or posting various images, texts and videos. So these websites generates large amount of data and it is very easy for attacker to forge personal information by creation of malicious identities and sends malicious posts from these identities [2].

In Facebook social network, some malicious users try to become friend of a normal user and posted malicious posts to spread misinformation and spam. It is very difficult to find which post is genuine or not. For this, researchers proposed number of techniques like web defensio, my page keeper, page rank algorithm and Frappe. These techniques are very efficient to detect and prevent malicious posts in Facebook but each technique has its own pros and cons. In this paper, a detailed study of these techniques has been discussed and also a new mechanism has been proposed based on these techniques to recognize genuine posts and malicious posts [3].

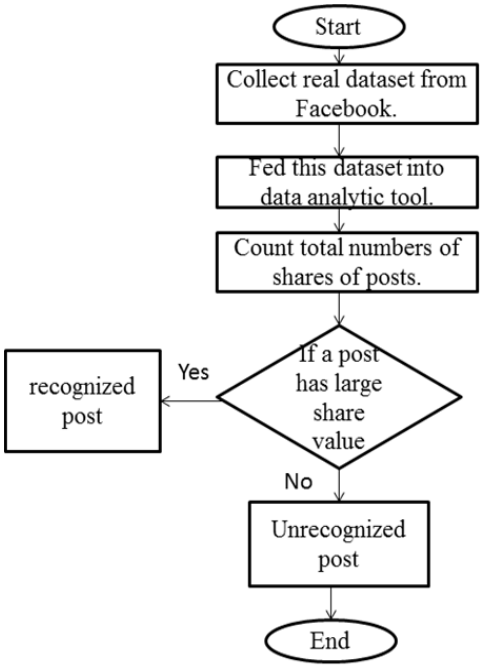
II. RELATED WORK

To steal user's information, attackers are creating so many fake posts and these fake posts seem to be look like real posts. That is the main aspect, many researchers and organizations are designing different techniques to protect the user from the attackers and spammers. Therefore, Puttaswamy [4] explained that the attacks of social intersection were an efficient and less costly to get private information of the user. Rahman et al. [5] developed FRAppE, a suite of efficient classification techniques for identifying

whether an app is malicious or not. Smith et al. [6] defined Life Logging as "the collection of data in order to illustrate a person's life." In other Social Networks, such as, e.g., Twitter or Google+, Graph G can be modeled as a directed graph as the user connections are not necessarily bidirectional. Agichtein et al. [7] described a paradigm shift from Web users as being consumers of content to producers of content. Xiao et al. [8] presented a machine learning pipeline for detecting fake accounts in online social networks. Nandhini and Das [9] presented an assessment of classification different social network and different attacks present on those social networks and methodology has been proposed which help the online users to be safe from numerous fraudulent and malicious activities on the web. In similar way Stringhini et al. [10] created honey profiles on different social networking sites. Honey profile was used to get data about malicious activities. Random Forest Algorithm was applied on collected data and determined the URL ratio of the message. There were many techniques for identification of malicious post and to detect them but in overall could not help to give the refine results and all these techniques are applied on text posts but could not help when there are image post, audio post and video post.

III. PROPOSED WORK

In this paper a novel mechanism is proposed to recognize genuine and malicious posts. The method is based on properties of the connections between Facebook users and their friends and the use of supervised learning techniques. This type of problem is to some degree similar to the problem of predicting links between users in different social networks. The degree of users posts will be decided based on likes, comments, shares and reactions on posts. As number of likes, positive reactions and shares will increases then that post will be recognized as good post similarly if shares will less and likes will less then that post will be treated as not recognized or useless posts.



Comparative Analysis

In this, the table 1 represents comparison between various techniques with different performance parameters. These are the following techniques likes My page keeper, page rank algorithm and web defensio and comparison is done on the basis of following parameter like Detection, Prevention, Security, Overhead.

Table1 : comparison between various techniques with different performance parameters

Techniques	Detection	Prevention	Security	Overhead
My page Keeper	Yes	No	Medium	High
Page Rank Algorithm	Yes	Yes	Medium	Low
Web Defensio	Yes	No	High	Medium

Here comparison of these existing techniques is done on the basis of advantages and disadvantages starting with the discussion.

Table 2. Comparison of various existing techniques with advantages and disadvantages

Techniques	Description	Advantage	Disadvantage
My Page Keeper	To detect malicious users in facebook. Various crawlers are used in this technique. To filter the profiles of facebook user these crawlers are used.	It is an efficient and accurate application which uses the URLs and Domains for the identification of the socware.	This application is only designed for socware which comes from user's news feed or user's wall posts. It does not cover other mediums like Facebook applications.
Web Defensio	To monitor user's profile a third party application is used in this technique.	It can detect if a post is legitimate or spam..this technique helps to find the links those are used in the spam or malicious posts in the user's profile.	Its only focuses on the user profile posts to detect the malicious or spam.
Page Rank Algorithm	Based on trend values, ranking of twitter pages are decided in this technique. Malicious pages are detected based on this ranking.	Depending upon the active period and the tweets, classification of trending topics is done.	It requires separate analysis of user's tweet and the followers.

IV. CONCLUSION

Online social networks provide malicious entities a lucrative environment to spread scams, and other types of malicious content during real world events. Security in social networks is very important because users can share their personal details and their emotions on social sites. So a malicious user may spread malicious contents on facebook through posts. To overcome this kind of problem number of techniques have been proposed by number of researchers. In this paper, different existing techniques to detect malicious posts in Facebook have been discussed with their pros and cons. After that a comparative analysis has been done on these techniques and analysis shows that Web defensio is a better technique in perspective of my page keeper and page rank algorithm. In future try to propose a new mechanism to recognize malicious posts in Facebook social networks.

V. REFERENCES

[1]. Pran Dev, Jyoti, Dr. Kulvinder Singh and Dr. Sanjeev Dhawan, "A Naive Algorithmic Approach for Detection of Users' with Unusual Behavior in online Social Networks" International Journal of Software and Web Sciences (IJSWS), ISSN: 2279-0071pp: 37-41,2015.

[2]. Ekta and Sanjeev Dhawan, "Classification of Data Mining and Analysis for Predicting Diabetes Subtypes using WEKA", Vivechana: National Conference on Advances in Computer Science and Engineering (ACSE-2016), pp. 1-5.

[3]. Ekta, Sanjeev Dhawan and Kulvinder Singh, "Feature Extraction and Content Investigation of

Facebook User's using Netvizz and Gephi", Advances in Computer Science and Information Technology (ACSIT), ACSIT 2016, pp. 262-265.
[4]. Sanjeev Dhawan and Ekta, "Implications of Various Fake Profile Detection Techniques in Social Networks", IOSR Journal of Computer Engineering (IOSR-JCE), AETM'16, 2016, pp. 49-55.
[5]. Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos, "Detecting Malicious Facebook Applications", IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE 2015, pp. 1-15
[6]. Smith A, O'Hara K and Lewis P, "Visualizing the past: Annotating a life with linked open data", in: Web Science Conference '11, 2011.
[7]. Agichtein E, Castillo C, Donato D, Gionis A and Mishne G, "Finding high-quality content in social media", Proceedings of the international conference on Web search Fake Identities in Social Media", Journal of Service Science Research (2012), pp.175-212.
[8]. Cao Xiao, David Mandell Freeman and Theodore Hwa, "Detecting Clusters of Fake Accounts in Online Social Networks", 2015 ACM. ISBN 978-1-4503-3826-4 pp: 1-11.
[9]. M. Nandhini and Bikram Bikash Das, "An Assessment And Methodology For Fraud Detection In Online Social Network", Second International Conference on Science Technology Engineering and Management (ICONSTEM) 2016, pp: 104-108.
[10]. G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference. ACM Request Permissions, 2012, pp. 1-9.
[11]. Haewoon Kwak, Changhyun Lee, Hosung Park, and Sue Moon, "What is Twitter, a Social Network or a News Media?", International World Wide Web Conference Committee (IW3C2),ACM 2010, pp. 1-10.
[12]. Anwar M, Fong PW, "A visualization tool for evaluating access control policies in Facebook-style social network systems", In: Proceedings of the 27th annual ACM symposium on applied computing, ACM 2012, pp. 1443-1450.
[13]. S. Abu-Nimeh, T. M. Chen, and O. Alzubi, "Malicious and Spam Posts in Online Social Networks," Computer, vol. 44, no. 9, IEEE 2011, pp. 23-28.