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

Malicious Posts Detection in Online in Social Networks

Divya
Assistant Professor, RPIIT, Bastarar Kurukshetra, Haryana, India

ABSTRACT

Online Social Networks provides different applications to users through which user can share their emotions in the form of text images and videos to their friends. User can also add new friends in their friend list also create groups of persons having same interest. When a user posts a new post on a group or on a page then it is difficult to justify that whether that post is normal post or malicious post. In this paper an attempt has been made to propose a mechanism to detect malicious posts in social network by analyzing the posts posted by user and number of likes and shares available on a post.

Keywords : Online Social Network , Facebook , posts, URL, Cybercriminals and Shares.

I. INTRODUCTION

Social network sites like Facebook, Twitter, and Google+ are encountering inconceivable development in users. There are more than a million users starting at now. Other than simply making a profile and connecting with companions, the social networks are no building stages to run their website[1]. These stages are fabricated in view of the user profile points of interest. These social applications are soon turning into a case of online correspondence which makes utilization of the user's private data and exercises in social connections for different administrations. The Social networks are famous methods for correspondence among the web users[2].

Individuals are vigorously transferring on online connections. The web is giving distinctive alternatives to make and keep up contacts and relations for the user. With the presentation of social media network these choices have turned out to be considerably less demanding to be utilized. Because of this substantial utilization of social media network a specific gathering of web users called cybercriminal make utilization of this open door for strings. Cybercriminals utilize diverse intends to make spams extortion and different attacks on the users[3].

Another methods for attack by cybercriminals is the abuse of recordings, pictures and connections appeared by the user. Digital attacks basically happen on social networks[4]. Well known sites, for example, Facebook and Twitter right now have a huge number of dynamic users. The popularity of social networks makes them leaving scenes to for executing malicious exercises. Because of the tremendous popularity of social media network these makes it simple for cybercriminal to abuse them. These can be as media, string or malicious post which does not has a place with a user. These post after clicking will take the user to some different pages made by malicious user[5].

Cybercriminals make fascinating posts that are really draws which will be pulled in by a few users. Run of the mill social building designs incorporate the utilization of Interesting posts that ride on regular occasions, superstar news and even calamities. Attackers transfer malicious posts in the period of uncommon occasions and fiascos. They will transfer malicious presents which are connected on these occasions and deceive users to click those connections. Users who tap the connections by botch go about as an enemy to the attacker in light of the fact that the malicious posts would consequently re-posts the malicious substance, for example, connections, pictures or recordings on the user profile. Another famous variant of this attack brings about user profiles to "like" a Facebook page without their insight. Now and again the, spammed posts will lead the users to study sites which will bring about digital lawbreakers getting benefit. Social network sites give restricted components to constrain the presentation of user profile information to applications. On account of Facebook, for instance, adopts a win big or bust strategy. At the point when users visit an application out of the blue, they should offer consent to enable that application to get to all required profile information. This single decision is to not utilize or visit the application by any stretch of the imagination. In any case, even this does not ensure any honest to goodness wellbeing. In this work, build up an arrangement of effective order procedure for distinguishing whether a post produced by an outsider application is malicious or not. Identifying malicious URLs is presently a fundamental errand in network security knowledge. To keep up effectiveness of web security, these malicious URLs must be recognized, distinguished and in addition their relating connections ought to be discovered. Thus users get shielded from it and viability of network security gets expanded [6].

The malicious users can transfer a substance he needs to spread. The substance that contains malicious information is presented on different users divider under an alternate frame. The user mix ups the posts for a genuine substance and snaps the post, which will take him to another page. Consequently the malicious user can profit by this procedure. To get the consideration of the user, the malicious user will incorporate catchphrases or portrayal of pages that will hold any importance with the user. These can be grown-up substance or free downloading sites.

II. RELATED WORK

Golbeck and Rothstein [7] appeared by thinking on FOAF (Friend of a Friend) profiles, that a large number of clients have accounts on various informal organizations, connecting their sub charts in the bound together interpersonal organization. Nonetheless, to distinguish profiles that allude to similar clients yet made with various IFP, different methodologies and techniques must be proposed coming about into a greater crossing point of clients between various interpersonal organization locales. Moreover, Rowe and Ciravegna [8] proposed to disambiguate the personality of a client by utilizing the groups of friends of the clients and some social information labeled with the name of the client. Groups of friends spoke to a gathering of individuals connected to a focal individual by some identifiable normal relation.Dewan and Kumaraguru [9], that is right now sidestepping Facebook's recognition strategies. In the first place contemplated the adequacy of existing systems utilized by Facebook to counter malevolent substance at that point recognized some key qualities of pernicious substance spread on Facebook, which recognize it from real substance. Rahman et al. [10] created FRAppE, a suite of productive grouping procedures for recognizing whether an application is malignant or not. To manufacture FRAppE, they utilized information from MyPage-Keeper, a security application in Facebook. Agichtein et al. [11]described a change in perspective from Web clients as being customers of substance to makers of substance in the mid 2005. Client produced content is one of the key qualities of online networking.

III. PROBLEM STATEMENT AND PROPOSED WORK

Online social networks are widely use these days for the purpose of communication. Users can share more type of information among friends. But there exist some social network users who misuse the features of these social networks and promote the spreading of malicious content. They do this by uploading the malicious post in other user page. These contents spread at a fast rate. There is no proper mechanism to detect these malicious posts immediately and remove it effectively.

There exists a wide range of malicious content on OSNs today. These include phishing, advertising campaigns, content originating from compromised profiles, artificial reputation gained through fake likes, etc. The main focus on analysis on identifying text posts, malicious URL and creating automated means to detect such posts in real time, without looking at the landing pages of the URLs.

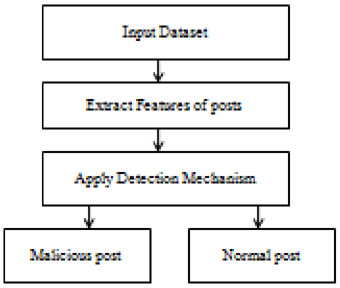

Figure 1. Proposed Mechanism

A. Data Collection and Text Corpus

Text corpus is an immense and organized arrangement of writings posted in the social media, and diverse strategies can be utilized in this progression. In this stage utilize dataset of Facebook. It's exceptionally rich of information users' content posts. furthermore, URLs.

B. Corpus Processing

This stage comprises to evacuate stop words and stemming. In figuring, stop words will be words which are sifted through preceding, or in the wake of, preparing of characteristic dialect information (content). To streamline the investigation need to dispose of stop words3 that contains no helpful data, as stop word expel stemming can improve the preparing and lessen mistakes.

C. Classification Process Using Similarity

The framework takes malicious post and remarks and that are identified by administrator utilizing catchphrases which are there in the administrator area. The possibility of this approach is to break down sentences posted by users in social media. Framework deteriorates each post in wording and looks at them consequently to suspicious terms. The administrator will scan for the malicious substance on user post and erase that post from the user page and after that send an alarm to the specific user. The administrator can likewise distinguish the undesirable remarks which show up in the user divider posted by user companions. In light of the demand by the user the administrator will evacuate the asked for post in the event that it is wellspring malicious. On the off chance that a sentence contains two terms (suspicious words) which presents likeness with the terms of database and characterize as suspicious post.

IV. CONCLUSION

In Online Social Network as number of users increases the chances of malicious posts also increases. A post is malicious when it contains vulgar content. It is difficult to find which post is malicious or posted by which user. To overcome this kind of problem in this paper provides a mechanism to detect malicious posts in online social network. In future try to improve the system in term of execution time, developing automated classification and using other knowledge resources in order to improve the precision rates, the semantic of exchanged information will be used to identify more significant suspicious profiles.

V. REFERENCES

[1]. G.Stringhini, C. Kruegel and G. Vigna, Detecting Spammers on Social Networks, in proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), 2010, pp.1-9.

[2]. De Wang, “Analysis and Detection of Low Quality Information in Social Networks”, ICDE Workshops 2014, IEEE 2014, pp.350-354.

[3]. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, “Detecting and characterizing social spam campaigns”, In IMC, 2010, pp.1-6.

[4]. 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.

[5]. 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.

[6]. Divya, Dr. Kulvinder Singh and Dr. Sanjeev Dhawan, “Threshold Based Mechanism to Detect Malicious URL’s in Social Networks”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727pp:18-21.

[7]. J. Golbeck and M. Rothstein, “Linking social networks on the web with FOAF: a semantic web case study,” in Proceedings of the 23rd national conference on Artificial intelligence - Volume 2. Chicago, Illinois: AAAI Press, 2008, pp. 1138-1143.

[8]. M.Rowe and F.Ciravegna, “Disambiguating identity through social circles and social data,” in Collective Intelligence Workshop ESWC 2008, Tenerife, Spain, IEEE 2008, pp. 1-4

[9]. Prateek Dewan, Ponnurangam Kumaraguru,” Towards Automatic Real Time Identification of Malicious Posts on Facebook”, 2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST), IEEE 2015, pp.85-92

[10]. 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

[11]. 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.