Implications of Various Fake Profile Detection Techniques in Social Networks

Dr. Sanjeev Dhawan[1], Ekta[2]
[1(]*Assistant professor, UIET, Kurukshetra University, 136119, Kurukshetra, Haryana,India)*
[2(]*Mtech Student, UIET, Kurukshetra University, 136119, Kurukshetra, Haryana,India)*

Abstract: *In the recent years, the fast development and the exponential utilization of social networks has prompted an expansion of social Computing. In social networks users are interconnected by edges or links. Facebook, twitter, linkedin are most popular social networks websites. In this paper focus is made on Facebook for detection of fake profile. Facebook is most used social networking site in which user can share messages, images and videos also users may add number of friends in their personal profiles. But it is difficult to find out whether the new person is genuine or not. May be it could be a malicious user. To detect malicious users or fake profiles different techniques has been proposed. In this paper an attempt has been made to analysis various existing techniques that includes comparison in perspective of various applications mapping various performance parameters.*

Keywords: *Facebook, FRAPPE, My page keeper, malicious, spam.*

I. INTRODUCTION

Social Networks are most popular networks through which information or ideas of human or people are exchanged throughout the world. A social structure is made up of nodes that are generally individuals or organizations. Peoples are communicating in Social Networks and creating relationships with others. In Social Networks Facebook, twitters, my web space and LinkedIn are most used websites. Millions of users, are attracted with these websites and most of them have taken these websites as part of their life. From the last few years, the Social Networking Sites example Facebook, twitter etc. have gained so much popularity as it becomes the daily routine of almost every person to check their profile every day as identified by Michael Fire *et al*. [1]. While it includes a huge number of users and it a center of information, this has become a possible track for attackers to utilize or attack. Various Sites provides different things to thwart these kinds of attacks but it is difficult to stop them because they finding various new techniques every day to performing attack. Due to the friendly nature of Facebook, users are likely disclosing many personal details about themselves and their associates as presented by Abu-Nimeh *et al.* [2]. The details may include date of birth, personal pictures, place of service, email address, high school name, relationship status, and even phone number. If this personal information is accessed by malicious user then it is to them to perform malicious activities on their timeline or even in their personal life [3]. For example, a malicious user can use the personal information accessed on the Facebook site to send modified spam messages to user.

In Facebook there are so many third party applications accessed by the user. When user wants to access any third party application then user must allow the permission to access the some profiles details by the application. When user allows the permission then application can access the user's personal information like name, email id and friends list etc. Sometimes hackers create these applications and convince the user to use these malicious Apps. User accesses malicious Apps and has to share its personal details with App. Hacker takes advantage of user's personal details and posts malicious contents on user's wall.

Figure.1 shows the step by step procedure to posts malicious content on user's wall by hacker using malicious application [4].

1. User requests to access an application to the Facebook server.
2. Facebook server needs to allow the permission for accessing the user's personal details by Apps.
3. User allows the permission to access the information.
4. Facebook server generates the token for the application server to complete its tasks.

5. This token is forwarded to the hacker who created this application to use the user's information for malicious perspective.
6. When hacker gets the access token then he post malicious content on user's wall or perform malicious activity using the personal information of the user.

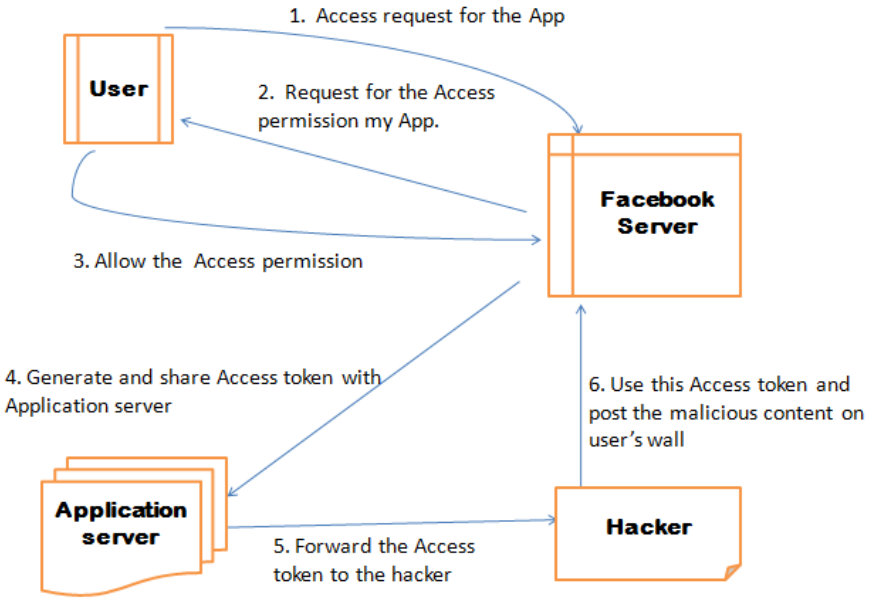

Fig 1: Operation of Facebook Malicious Application [4]

II. RELATED WORK

Social Networks are becoming more popular in these days, more and more people are communicating with friends, colleagues and relatives through Online Social Networks. People are sharing their personal information and important data that is why security and privacy seems to be most important concern in Social Networks for the communication. Attackers and hackers are trying in different ways to steal and get the user's credentials and personal details. To steal user's information attackers are creating so many fake profiles and these fake profiles are seems like real profiles. That is the main aspect many researchers and organizations are designing different techniques to protect the user from the attackers and spammers. Therefore, Puttaswamy [5] explained the attacks of social intersection were an efficient and less costly to get private information of the user. Furthermore, Halim *et al.* [6] described the method to detect people those are involved in malicious activities on Facebook. This technique had two stages: in first stage semantic analysis was performed to classify the malicious posts. In second stage spatiotemporal analysis was done. Then the comparison was done between the original friend graph and the spatiotemporal graph. In another research various Social Network platforms like Facebook which provides different privacy settings to secure user's personal information in network. (Liu *et al.* [7]) Additionally various protection mechanism offers by Facebook protect users from spammers, hackers, or other threats (Mehmood and Desmedt [8]). Moreover Facebook provides immune system (Stein *et al.* [9]). Social Network provides better security to protect its user by using authentication route to make sure that already registered user is a genuine person (Kuzma [10]).

Debarr and Wechsler [11] classified different spammers by using graph centrality. Moreover, Yang *et al.* [12] detected fake profiles which was based on some features. First was time stamp of link creation and second was frequency of friend request. In similar way reflective policy assessment tool represented by Anwar and Fong [13] which observed profile from various viewpoints. In another way Rahman *et al.* [14] proposed an application named my page keeper. There were number of attacker whose aim was to add some malicious data on user's timeline. To detect this type of attacks my page keeper application was used. Similar to this technique now this time Rehman *et al.* [4] presented Frappe which was used to detect malicious application on Facebook like what does your name

mean? Etc. Based on this technique Fire *et al.* [15] detected fake profiles in Social Networks on the basis of profile anomalies. To identify spam profiles Ahmed *et al.* [16] proposed a technique on the basis of social interaction in Facebook. Interaction was determined by using the page-likes, active friends and the URLs shared between the different profiles. Then clustering technique was applied and obtained this proposed technique was efficient to detect the spam profiles. In similar way Stringhini *et al.* [17] 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 messages.

As part of this study, different techniques were proposed by various researchers to detect the fake profiles and malicious content. Each technique had its advantages and disadvantages those are discussed further in Section III that is classification of various techniques.

III. CLASSIFICATION OF VARIOUS TECHNIQUES

There are number of techniques are available to prevent users from malicious activities in Social Networks. Some techniques are used to detect fake profiles; some are used to prevent users from malicious apps. In this section comparison is made among a number of techniques for fake profile detection. Table 1 explains various techniques to detect fake profiles in social networks. In this table brief description of techniques and there pros and cons are discussed. Figure 2 describes various technique for detecting fake profiles, malicious application, spam etc.

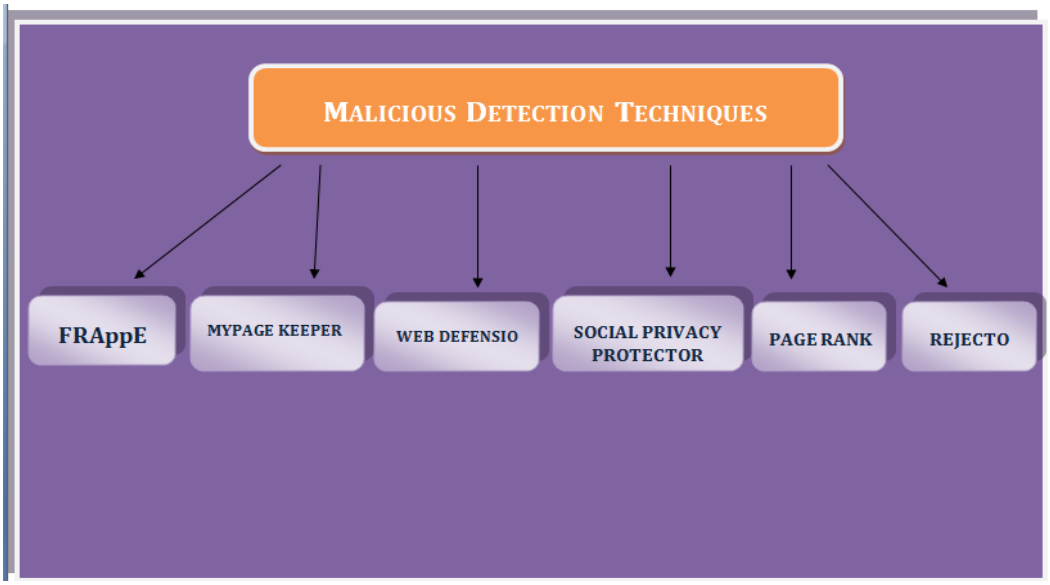

Fig 2: Different Malicious Detection Techniques

Table 1: Various Malicious Detection Techniques

Techniques	Description	Advantage	Disadvantage
My Page Keeper[13]	In my page keeper technique various crawlers are used to detect malicious users in Facebook. These crawlers are used to filter the profile of Facebook user.	It is 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.
FRAppE[4]	In FRAppE malicious applications are detected based on some threshold value like popularity scores of application.	It can detect the malicious application with accuracy using the no false positive and high true positive rate.	It does not cover the deeper information about the ecosystem of malicious apps on Facebook.

Web Defensio[2]	In this technique a third party application is used to monitor user's profile.	It can detect a post that is legitimate or spam. It can also find the links those are used in the spam or malicious posts in the user's profile.	It only focuses on the posts in the profile of the user to detect the malicious or spam.
Page Rank Algorithm[18]	In this technique ranking of twitter pages are decided based on their trend values. Then based on the ranking malicious pages are detected.	Classification of trending topics is done depending upon the active period and the tweets.	It requires separate analysis of user's tweet and the followers.
Rejecto[3]	This is an effective system to detect the fake accounts those can be spammers or can act as spammers. It monitors the friend requests sent by the user and detect the fake account requests and then prevent user from these requests in future.	It can detect the fake accounts that can be friend spammers by monitoring the friend requests sent by users. It can prevent form these fake accounts.	This system detects the fake accounts by using sent out friend requests only.
Social Privacy Protector[1]	It is used to identify the fake accounts and also used to improve the security and the privacy of the user. It has three layers first is focused on the detection of possible threat and restrict that friend to share the information. Second layer conveys the privacy settings on the basis of the usage. Third layer gives a alert message for the installed applications those want to access the private information of the user.	It is focused on the privacy. It also restricts the possible threat to share the private information with other user that is restricted.	It is compatible only with Mozilla firefox. It does not interact with other browsers. It does not work with the large data.

IV. PROPOSED WORK

To detect and classify malicious users and normal users here we present few steps that describe how to distinguish malicious users via flowchart. Figure 3 show the working principle of proposed work. In first step real data set will be collected which is in .csv file format through Facebook. After the collection of data set in next step there will be need to extract features of users profile by feature extraction tool. After the extraction of the features different parameters will used like True positive rate (TPR) and false positive rate (FPR) for determining the legitimate user and the malicious users. If True positive rate is higher than False positive rate then that will be listed as a legitimate user else that will be treated as a malicious user.

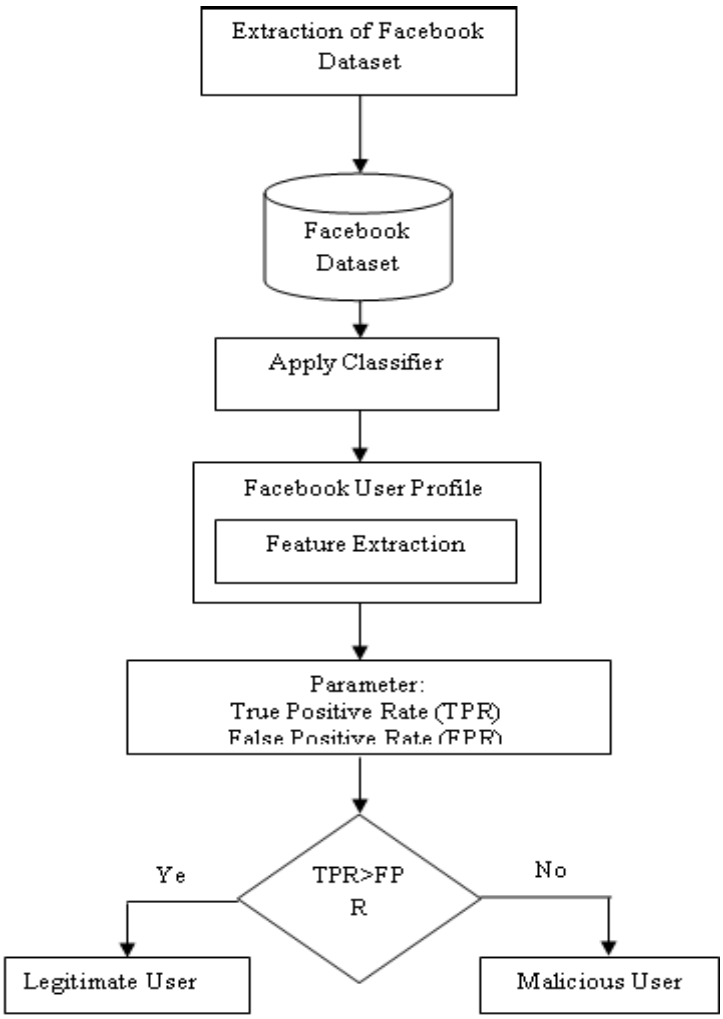

Fig 3: Working principle of Proposed Work

Table II comparative analysis of different techniques with various social network applications

Techniques	**Facebook**	**LinkedIn**	**Google+**	**Myspace**	**Friendster**	**Hi5**	**Twitter**
Mypage Keeper	✓	X	X	X	X	X	X
Rejecto	✓	✓	✓	✓	✓	X	X
FRAppE	✓	X	X	X	X	X	X
Web Defensio	✓	X	X	✓	X	✓	✓
Page Rank Algorithm	X	X	X	X	X	X	✓
Social Privacy Protector	✓	X	X	X	X	X	X

V. COMPARATIVE ANALYSIS

Applications: Above table II shows comparative analysis has been done on various techniques. This analysis is done by using results provided by research paper of these techniques.

Table III mapping of various techniques to performance parameter

Parameters	**Techniques**					
	My page Keeper	**Reject to**	**FRAppE**	**Social privacy protector**	**Page Rank Algorithm**	**Web Defensio**
Security	Medium	High	Medium	High	Medium	High
Efficiency	High	Medium	High	Medium	Medium	Medium
Overhead	High	Medium	Medium	High	Low	Medium
True positive Rate	-------	--------	High	-------	--------	--------
False Positive Rate	--------	--------	Low	-------	--------	---------
Privacy	Medium	High	Medium	High	Low	Low

Table III provides mapping of various techniques with different performance parameters like security, efficiency, overhead, true positive rate false positive rate, privacy etc.

VI. CONCLUSION AND FUTURE WORK

This paper presents classification of various techniques to detect malicious users and to prevent users from fake profiles. This includes reject to, frappe, my page keeper etc. Pros and cons of each technique have been discussed. After that Implication of these techniques in perspective of applications and performance parameter have been represented. Results show that reject to and social privacy protector techniques are most efficient out of other techniques to prevent networks from malicious users. In future effort will be made a new enhanced algorithm will be proposed based on these techniques to prevent fake profile detection on social networks.

REFERENCES

[1] Michael Fire, Dima Kagan, Aviad Elyashar and Yuval Elovici," Friend or foe? Fake profile identification in online social networks", Soc. Netw. Anal. Min. (2014), Springer-Verlag Wien 2014, pp. 1-23.

[2] 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.

[3] Qiang Cao, Michael Sirivianos, Xiaowei Yang and Kamesh Munagala" Combating Friend Spam Using Social Rejections", IEEE 35th International Conference on Distributed Computing Systems, IEEE 2015, pp.235-244.

[4] Rahman MS, Huang TK, Madhyastha HV, Faloutsos M,"Frappe: detecting malicious Facebook applications", in: Proceedings of the 8th international conference on emerging networking experiments and technologies, ACM 2012, pp. 313–324.

[5] Puttaswamy KPN, Sala A, and Zhao BY," Starclique: Guaranteeing user privacy in social networks against intersection attacks", in: Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, CoNEXT '09. ACM 2009, New York, NY, USA, pp.157-168.

[6] Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz,"Malicious users' circle detection in social network based on spatiotemporal co-occurrence," in Computer Networks and Information Technology (ICCNIT), 2011 International Conference on, July, pp. 35–390.

[7] Liu Y, Gummadi K, Krishnamurthy B, Mislove A," Analyzing Facebook privacy settings: User expectations vs. reality", in: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, ACM, pp. 61–70.

[8] Mahmood S, Desmedt Y," Poster: preliminary analysis of google?'s privacy. In: Proceedings of the 18th ACM conference on computer and communications security", ACM 2011, pp.809–812.

[9] Stein T, Chen E, Mangla K," Facebook immune system. In: Proceedings of the 4th workshop on social network systems", ACM 2011, pp.1-8.
[10] Kuzma J," Account creation security of social network sites", Inter J Appl Sci Technol 1(3):2011, pp. 8–13.
[11] Debar D, Wechsler H," Using social network analysis for spam detection", In: Proceedings of the third international conference on social computing, behavioral modeling, and prediction (SBP'10). Springer-Verlag, Berlin, Heidelberg 2010, pp. 62–69.
[12] Cukierski WJ, Hamner B, Yang B,"Graph-based features for supervised link prediction. In: IEEE International Joint Conference on Neural Networks (IJCNN)", IEEE 2011, pp. 1237–1244.
[13] 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.
[14] Rahman M, Huang T, Madhyastha H, Faloutsos M," Efficient and scalable socware detection in online social networks", In: Proceedings of the 21st USENIX conference on security Symposium 2012, USENIX association, pp. 32–32.
[15] Fire M, Katz G, Elovici Y," Strangers intrusion detection detecting spammers and fake profiles in social networks based on topology anomalies", ASE Hum J 1(1):2012, pp.26–39.
[16] F. Ahmed and M. Abulaish, "An MCL-Based Approach for Spam Profile Detection in Online Social Networks," IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications 2012, pp. 1–7.
[17] 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.
[18] 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.