OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

AUTOMATIC DETECTION OF FAKE PROFILES IN ONLINE SOCIAL NETWORKS

Sumit Milind Kulkarni[1], Prof. Vidya Dhamdhere[2]
G. H. Raisoni College Of Engineering & Management, Wagholi Pune [1,2]
Sumitkulkarni18@gmail.com[1], vidya.dhamdhere@raisoni.net[2]

ABSTRACT: **In the present age, the social existence of everybody has moved toward becoming related with the online informal communities. These destinations have rolled out a radical improvement in the way we seek after our social life. Reaching them and their updates has turned out to be simpler. Be that as it may, with their fast development, numerous issues like phony profiles, online pantomime have likewise developed. There are no practical arrangement exist to control these issues. In this venture, we concocted a structure with which programmed identification of phony profiles is conceivable and is productive. This system utilizes order methods like Support Vector Machine, Nave Bayes and Decision trees to characterize the profiles into phony or bona fide classes. As, this is a programmed recognition technique, it can be connected effortlessly by online informal organizations which has a huge number of profile whose profiles can't be inspected physically.**

Keywords**:** *Conceptual Similarity, Trademark Infringement, Trademark Retrieval, Trademark Similarity.*

----------∴∴∴----------

I INTRODUCTION

Online informal communities (OSNs) empower and energize outsider (applications) to improve the client encounter on these stages. Such improvements incorporate fascinating or engaging methods for conveying among online companions and different exercises, for example, playing recreations or tuning in to melodies. For instance, Facebook gives designers an API [2] that encourages application reconciliation into the Facebook client encounter. There are 500K applications accessible on Facebook [3], and all things considered, 20M applications are introduced each day [1]. Besides, numerous applications have gained and keep up a truly huge client base. For example, FarmVille and CityVille applications have 26.5M and 42.8M clients to date.

As of late, programmers have begun exploiting the fame of this outsider applications stage and conveying malevolent applications [4]– [6]. Noxious applications would pro be able to vide a lucrative business for programmers, give n the notoriety of OSNs, with Facebook driving the path with 900 M dynamic clients [7].

There are numerous ways that programmers can profit from malicious application:

1) The application can achieve expansive quantities of clients and their companions to spread spam;

2) the application can acquire clients' close to home data, for example, email address, main residence, and sexual orientation; and

3) The application can "replicate" by making different vindictive applications well known.

To exacerbate the situation, the organization of vindictive applications is disentangled by prepared to-utilize toolboxs beginning at $25.[8] As it were, there is intention and opportunity, and thus, there are numerous malevolent applications spreading on Facebook consistently [9].

II LITERATURE SURVEY

1. Prevention of Fake Profile Proliferation in Online Social Networks (2015)

Today, Online Social Networks (OSNs) are the most common platforms on the Internet, on which millions of users register to share personal facts with their friends. Online social network users are unaware of the numerous security risks that exist in these networks, like privacy violation, identity theft and sexual harassment etc. Many users disclose their personal information like phone no., date of birth, address etc. Leakage of personal information is a significant

Concern for social network users. Fake profiles are being created in all the sites and one's information is becoming more and more vulnerable in the past decade. Nowadays the Identity Clone Attack (ICA) is increased in the many social networking websites that causes the frustration between the peoples and social networking websites too. This attack is done by retrieving the information of the individuals profile by anonymous person i.e. individual information is leaked and clone or fake profile is created which shows as real one. Thus this leads to the ambiguity between the owner of the profiles and the person associated to their profile i.e. we cannot have control to create over creation of clone profiles in the OSN and impacts it to the person having his or her own profiles. Hence, a new way of protecting personal information on online social sites is being proposed in this paper.

2. Implications of Various Fake Profile Detection Techniques in Social Networks

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.

3. Automatic detection of fake profiles (2015)

This paper presents the study of various methods for detection of fake profiles. In this paper a study of various papers is done, and in the reviewed paper we explain the algorithm and methods for detecting fake profiles for security purpose. The main part of this paper covers the security assessment of security on social networking sites.

4. An IAC Approach for Detecting Profile Cloning in Online Social Networks(2014)

Nowadays, Online Social Networks (OSNs) are popular websites on the internet, which millions of users register on and share their own personal information with others. Privacy threats and disclosing personal information are the most important concerns of OSNs' users. Recently, a new attack which is named Identity Cloned Attack is detected on OSNs. In this attack the attacker tries to make a fake identity of a real user in order to access to private information of the users' friends which they do not publish on the public profiles. In today OSNs, there are some verification services, but they are not active services and they are useful for users who are familiar with online identity issues.

In this paper, Identity cloned attacks are explained in more details and a new and precise method to detect profile cloning in online social networks is proposed. In this method, first, the social network is shown in a form of graph, then, according to similarities among users, this graph is divided into smaller communities. Afterwards, all of the similar profiles to the real profile are gathered (from the same community), then strength of relationship (among all selected profiles and the real profile) is calculated, and those which have the less strength of relationship will be verified by mutual friend system. In this study, in order to evaluate the effectiveness of proposed method, all steps are applied on a dataset of Facebook, and finally this work is compared with two previous works by applying them on the dataset.

5. Towards Detecting Compromised Accounts on Social Networks

Social Network accounts has become a profitable course of action for cybercriminals. By hijacking control of a popular media or business account, attackers can distribute their malicious messages or disseminate fake information to a large user base. The impacts of these incidents range from a tarnished reputation to multi-billion dollar monetary losses on financial markets. In our previous work, we demonstrated how we can detect large-scale compromises (i.e., so-called campaigns) of regular online social network users.

In this work, we show how we can use similar techniques to identify compromises of individual high-profile accounts. High-profile accounts frequently have one characteristic that makes this detection reliable – they show consistent behavior over time. We show that our system, were it deployed, would have been able to detect and prevent three real-world attacks against popular companies and news agencies. Furthermore, our system, in contrast to popular media, would not have fallen for a staged compromise instigated by a US restaurant chain for publicity reasons.

6. Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model

Social networks such as Facebook, Twitter and Google+ have attracted millions of users in the last years. One of the most widely used social networks, Facebook, recently had an initial public offering (IPO) in May 2012, which was among the biggest in Internet technology. For profit and nonprofit organizations primarily use such platforms for target- oriented advertising and large-scale marketing campaigns. Social networks have attracted worldwide attention because of their potential to address millions of users and possible future customers. The potential of social networks is often misused by malicious users who extract sensitive private information of unaware users. One of

the most common ways of performing a large-scale data harvesting attack is the use of fake profiles, where malicious users present themselves in profiles impersonating fictitious or real persons.

The main goal of this research is to evaluate the implications of fake user profiles on Facebook. To do so, we established a comprehensive data harvesting attack, the social engineering experiment, and analyzed the interactions between fake profiles and regular users to eventually undermine the Facebook business model. Furthermore, privacy considerations are analyzed using focus groups. As a result of our work, we provided a set of countermeasures to increase the awareness of users.

III PROPOSED WORK

The proposed framework in the figure 3.1 shows the sequence of processes that need to be followed for continues detection of fake profiles with active leaning from the feedback of the result given by the classification algorithm. This framework can easily be implemented by the social networking companies.

The detection process starts with the selection of the profile that needs to be tested. After selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented. The attributes extracted is passed to the trained classifier. The classifier gets trained regularly as new training data is feed into the classifier.

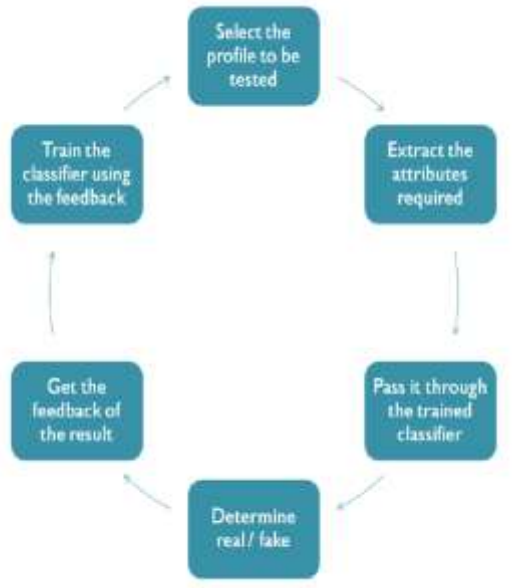

Figure 1 Framework.

The classifier determines the whether the profile is fake or real. The classifier may not be 100% accurate in classifying the profile so; the feedback of the result is given back to the classifier. For example, if the profile is identified as fake, social networking site can send notification to the profile to submit identification. If the valid identification is given, feedback is sent to the classifier that the profile was not fake. This process repeats and as the time proceeds, the no. of training data increases and the classifier becomes more and more accurate in predicting the fake profiles.

In the Proposed System First user send message than it goes to the message filter and it checks. After check post it stored to the database. It calculates the post means how many upload picture, audio, video etc. All this data like and comment and stored to the database. For e.g. Person A using the Facebook account A person has 40 friends and A person upload one image it gets 250 likes or comment than our system check and shows the result his/her account is fake.

User gets the many message for example it gets app notification. In the notification it provides the link for application download, User download the app but sometimes virus in the application so our system first check the link is malicious or not.

1) If in the link virus is not than it shows the user message virus free link you can securely download the app

2) If in the link virus presence than it shows the user message not download the application.

Advantages

1. It focuses on quantifying, profiling & understanding malicious apps.
2. User information's are secured and safe.
3. Avoiding use of different client IDs in app installation.
4. FRAppE can detect malicious apps with 99% accuracy.

CONCLUSION AND FUTURE WORK

We have given a framework using which we can detect fake profiles in any online social network with a very high efficiency as high as around 95%. Fake profile detection can be improved by applying NLP techniques to process the posts and the profile.

REFERENCES

1]T. Stein, E. Chen, and K. Mangla. Facebook immune system. In Proceedings of the 4th Workshop on Social Network Systems, SNS, volume 11, page 8, 2011.

2]Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 93{102. ACM, 2011.

3]C. Wagner, S. Mitter, C. K□orner, and M. Strohmaier. When social bots attack: Modeling susceptibility of users in online social networks. In Proceedings of the WWW, volume 12, 2012.

4]G. Kontaxis, I. Polakis, S. Ioannidis, and E.P. Markatos. Detecting social network profile cloning. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on, pages 295{300. IEEE, 2011.

5]A. Wang. Detecting spam bots in online social networking sites: a machine learning approach. Data and Applications Security and Privacy XXIV, pages 335{342, 2010}.

5] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B.Y. Zhao. Detecting and characterizing social spam campaigns. In Proceedings of the 10th annual conference on Internet measurement, pages 35{47. ACM, 2010.

6] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia. Who is tweeting on twitter: human, bot, or cyborg? In Proceedings of the 26th Annual Computer Security Applications Conference, pages 21{30. ACM, 2010.

7] S. Krasser, Y. Tang, J. Gould, D. Alperovitch, and P. Judge. Identifying image spam based on header and _le properties using c4. 5 decision trees and support vector machine learning. In Information Assurance nd Security Workshop, 2007. IAW'07. IEEE SMC, pages 255{261.IEEE, 2007.

8] G.K. Gupta. Introduction to Data Mining with Case Studies. Prentice Hall India, 2008.

9] Rajan Chattamvelli. Data Mining Methods. Narosa, 2010.

10] Spies create fake facebook account in nato chief's name to steal personal details, http://in.news.yahoo.com/spies-create-fake-facebook-account-nato-chiefs-name-114824955.html

11] Man arrested for uploading obscene images of woman colleague, http://www.ndtv.com/article/andhra-pradesh/man-arrested-for-uploading-obscene-images-of-woman-colleague-173266.

12] How obamas internet campaign changed politics, /bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics.

13] S. Nagaraja, A. Houmansadr, P. Piyawongwisal, V. Singh, P. Agarwal, and N. Borisov. Stegobot:A covert social network botnet. In Information Hiding, pages 299{313. Springer, 2011.

14] M. Huber, M. Mulazzani, and E. Weippl. Who on earth is mr. cypher: Automated friend injection attacks on social networking sites. Security and Privacy{Silver Linings in the Cloud.