|| Volume 3 || Issue 4 || April 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Automatic Detection of Compromised Accounts and Applications on OS

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

Abstract— **In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake profiles, online impersonation have also grown. There are no feasible solution exist to control these problems. In this project, we came up with a framework with which automatic detection of fake profiles is possible and is efficient. This framework uses classification techniques like Support Vector Machine, Nave Bayes and Decision trees to classify the profiles into fake or genuine classes. As, this is an automatic detection method, it can be applied easily by online social networks which has millions of profile whose profiles cannot be examined manually.**

Keywords: *Item reputation, Reviews, Rating prediction, Recommender system, Sentiment influence, User sentiment.*

I INTRODUCTION

A social networking site is a website where each user has a profile and can keep in contact with friends, share their updates, meet new people who have the same interests. These Online Social Networks (OSN) uses web2.0 technology, which allows users to interact with each other.

These social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with same interests together which makes users easier to make new friends. In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Adding new friends and keeping in contact with them and their updates has become easier. The online social networks have impact on the science, education, grassroots organizing, employment, business, etc. Researchers have been studying these online social networks to see the impact they make on the people. Teachers can reach the students easily through this making a friendly environment for the students to study, teachers now-a-days teachers are getting themselves familiar to these sites bringing online classroom pages, giving homework, making discussions, etc. which improves education a lot. The employers can use these social networking sites to employ the people who are talented and interested in the work, their background check can be done easily using this. Most of the OSN are free but some charge the membership fee and uses this for business purposes and the rest of them raise money by using the advertising. This can be used by the government to get the opinions of the public quickly.

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 parameter.

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

Compromising 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.

1. The detection process starts with the selection of the profile that needs to be tested.
2. After selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented.

3. The attributes extracted is passed to the trained classifier. The classifier gets trained regularly as new training data is feed into the classifier.
4. The classifier determines the whether the profile is fake or real.
5. 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.
6. 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.

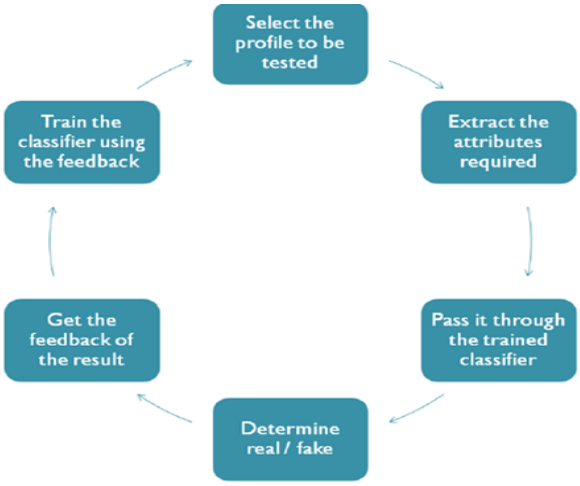

Figure 1: Framework.

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.

IV ADVANTAGES

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

V RESULTS

1. Train data

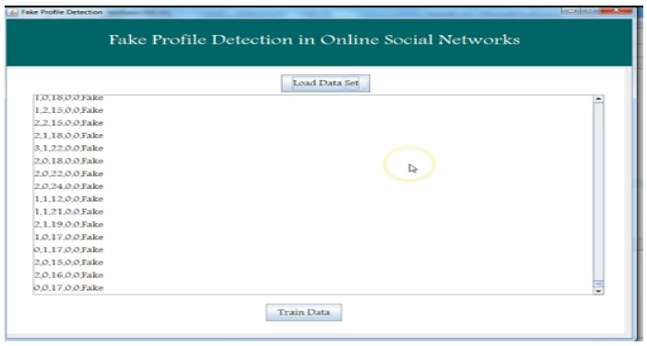

Figure 2: Train data

2. SVM Training

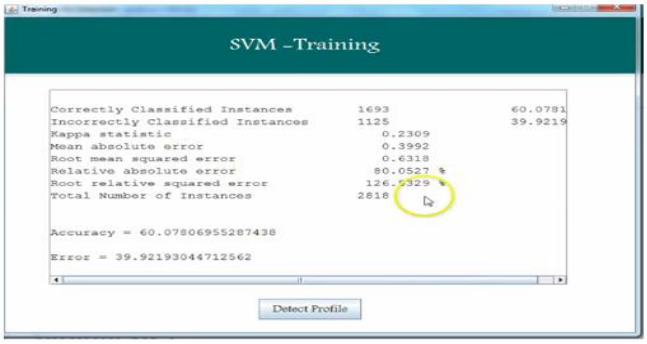

Figure 3: SVM Training

3. Profile Detection

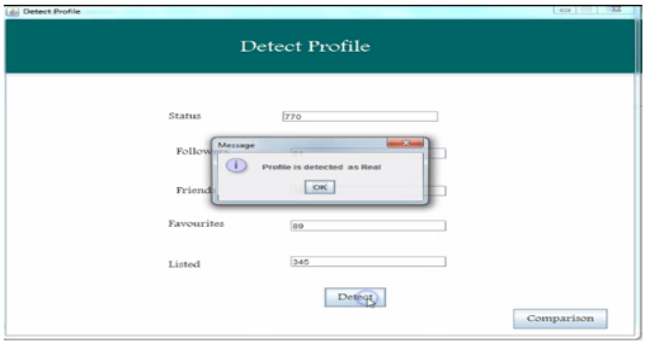

Figure 4: Train data

4. Accuracy

Figure 5: Accuracy

VI CONCLUSION AND FUTURE WORK

Applications exhibit advantageous means for programmers to spread vindictive substance on Facebook. Little is comprehended about the qualities of malevolent applications and how they operate. we demonstrated that pernicious applications vary essentially from favourable applications as for a few highlights . we created and a precise classifier for identifying malignant Facebook applications .We will keep on digging more profound into this environment of pernicious applications on Facebook, and we trust that Facebook will profit by our proposals for diminishing the threat of programmers on their stage.

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.
6. 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.
7. 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.
8. 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.
9. G.K. Gupta. Introduction to Data Mining with Case Studies. Prentice Hall India, 2008.
10. Rajan Chattamvelli. Data Mining Methods. Narosa, 2010.
11. 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
12. 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.
13. How obamas internet campaign changed politics, /bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics.
14. 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.
15. 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, pages 80{89, 2010.