Fake Profile Detection in Instagram Online Social Network

[a]Sanjeev Dhawan [b] Kulvinder Singh [c] Pooja
[a,b] Faculty of Computer Science & Engineering, [c] Post Graduate Student of M.Tech. (Computer Engineering) Department of Computer Science
[a,b,c] University Institute of Engineering & Technology (U.I.E.T)
E-mail: [a]rsdhawan@rediffmail.com [b]kshanda@rediffmail.com [c] tayapooja1@gmail.com

ABSTRACT

Social network provides number of applications such as Myspace, Facbook, Twitter and many more through which users can connect with their friends and share their images and videos with them. Instagram is application of social network which is used to share images and videos with friends also tag a friend on an image and video. It is difficult to recognize which user is normal user or which user is malicious user. In this paper different techniques to recognize fake profile user has been surveyed and provide a mechanism to detect fake profiles in social network. This paper proposed a mechanism to detect normal posts using Random Forest classifier. The proposed mechanism has been analyzed using weka.

Keywords: Social Networks, Fake Profile, Cloning ,Instagram and Facebook.

I. INTRODUCTION

Social networks provides platform where every user has a profile and can stay in touch with friends, share their updates, meet new individuals who have similar interests. These Online Social Networks (OSN) utilizes web2.0 innovation, which enables clients to interface with each other. These social networking locales are developing quickly and changing the way individuals stay in touch with each other. The online groups carry individuals with same interests together which makes clients less demanding to make new friends. There are no possible arrangement exist to control these issues. In this paper, we concocted a system with which programmed discovery of phony profiles is conceivable and is proficient structure utilizes order methods like Support Vector Machine, Nave Bayes and Decision trees to arrange the profiles into phony or certified classes. As, there is a programmed identification strategy, it can be connected effectively by online social networks which has a huge number of profiles whose profiles cannot be analyzed physically. These social networking destinations are developing quickly and changing the way individuals stay in touch with each other. The online groups carry individuals with same interests together which makes clients less demanding to make new friends. In the present age, the social existence of everybody has moved toward becoming related with the online social networks. These locales have rolled out an uncommon improvement in the way we seek after our social life. Including new friends and staying in touch with them and their up-dates has turned out to be less demanding.

A. Instagram

Instagram is an application that provides platform to users for sharing photographs and recordings to online social network.. Like Facebook or Twitter, everybody who makes an Instagram account has a profile and a news encourage. When you post a photograph or video on Instagram, it will be shown on your profile. Different clients who tail you will see your posts in their own nourish. In like manner, you'll see posts from different clients whom you take after . It resembles an improved rendition of Facebook, with an accentuation on versatile utilize and visual sharing. Much the same as other social networks, you can connect with different clients on Instagram by tailing them, being trailed by them, remarking, enjoying, labeling and private informing. You can even spare the photographs you see on Instagram. Instagram is accessible for nothing on iOS and Android gadgets. It can likewise be gotten to on the web from a PC, yet clients can just transfer and offer photographs or recordings from their devices.

B. Issues in OSN

- User's Profile and Personal Information: And in addition user's record, Social Network user's profiles for the most part contain genuine data about users. Delicate data, for example, user's full name, contact data, relationship status, and date of birth, past and current work and training foundation pulls in assailants. In this way, the principle issue of user's profile is the leakage of profile and individual data.
- Leakage of data through poor security settings: Most Social Network users are not cautious about their security settings. Numerous open their profile to the general population so anybody can access and see their data. Likewise, numerous Social Networking destinations default security setting is as yet not sheltered, for example, in Facebook, a friend of a friend who the user does not know can in any case observe his data. In any case, even the most secure protection setting, there are still imperfections that enable aggressors to get to user's data.
- Leakage of data to outsider application: Numerous social networking sites, for example, Facebook give an API (Application Programming Interface) for outsider engineers to make applications that can keep running on its stage. These outsider applications are exceptionally prevalent among Social Network users. When users include and enable outsider applications to get to their data, these applications can get to user's information naturally. It is additionally equipped for posting on user's space or user's friends space, or may get to other user's data without user's information.
- Leakage of data to outsider area: Numerous Social Networking sites utilizes outsider area administration to track social network user's exercises, or permits notice accomplice to access and total Social Network user's information for their business advantage.

C. Profile Cloning

One system of taking Social Network user's personality is called profile cloning. The fundamental focuses of profile cloning are users who set their profiles to be open. Open profile enables aggressors to get profile data effectively and consequently can copy or duplicate their profile data to make a false personality. There are two kinds of profile cloning.

- **Existing Profile Cloning**

  In existing profile cloning, aggressors make a profile of effectively existing users by utilizing their name, individual data, and picture to build dependence, and after that sending friend solicitations to friends of that user. This activity is effective since most users acknowledge friend demands from the individual that they definitely know without looking through it precisely. Likewise, it is conceivable that a man may have different records. In the event that casualties acknowledge the friend demands, at that point aggressors will have the capacity to get to their data.

- **Cross-Site Profile Cloning**
  In cross-site profile cloning, aggressors take user's profile from one Social Networking site that users enroll a record, and afterward make another user's profile on another Social Networking site that user has not enlisted on previously. From that point forward, assailants utilize users contact list from the enrolled Social Networking site to send a friend solicitations to every one of those contacts in another Social Networking site. For this situation, it is more persuading than the principal case since there is just a single record for that specific user. At that point, if the contacts acknowledge friend ask for, aggressors can get to their profile.

II. LITERATURE SURVEY

Many Researchers proposed different techniques on different parameters those are also listed in this literature survey Li et al. [5] connected added substance homomorphic encryption in security saving in a situation with numerous middle of the road processing parties. In addition Dong et al. [6] and Narayanan et al. [8] register social vicinity to find potential friends by utilizing both homomorphic cryptography and confusion, which is more effective. Agrawal and Srikant [7] first proposed protection safeguarding information mining, which tries to bother singular records in an amassed database. Notwithstanding, this paper essentially centers around factual data of unordered databases and does not ascend to the level of information coordinating. There are bunches of pertinent work can finish the cloud information coordinating, for example, deterministic encryption and request protecting encryption. In any case, these work additionally require arrangement between users, which can't be connected in our situation since intrigue assault between vindictive users and cloud server may happen. With the communication among users in the current applications got increasingly consideration, a great deal of research on the issue of security information coordinating has been raised as of late. Likewise Rahman et al. [9] created FRAppE, a suite of productive order methods for distinguishing whether an application is vindictive or not. In comparative way Stringhini et al. [10] made nectar profiles on various social networking destinations. Nectar profile was utilized to get information about vindictive exercises.

III. EXISTING TECHNIQUES

My Page Keeper: To recognize malicious posts in facebook. Different crawlers are utilized as a part of this procedure. To channel the profiles of facebook user these crawlers are utilized. It is a productive and exact application which utilizes the URLs and Domains for the distinguishing proof of the socware. This application is intended for socware which originates from user's news bolster or user's divider posts. It doesn't cover different mediums like Facebook applications [11].

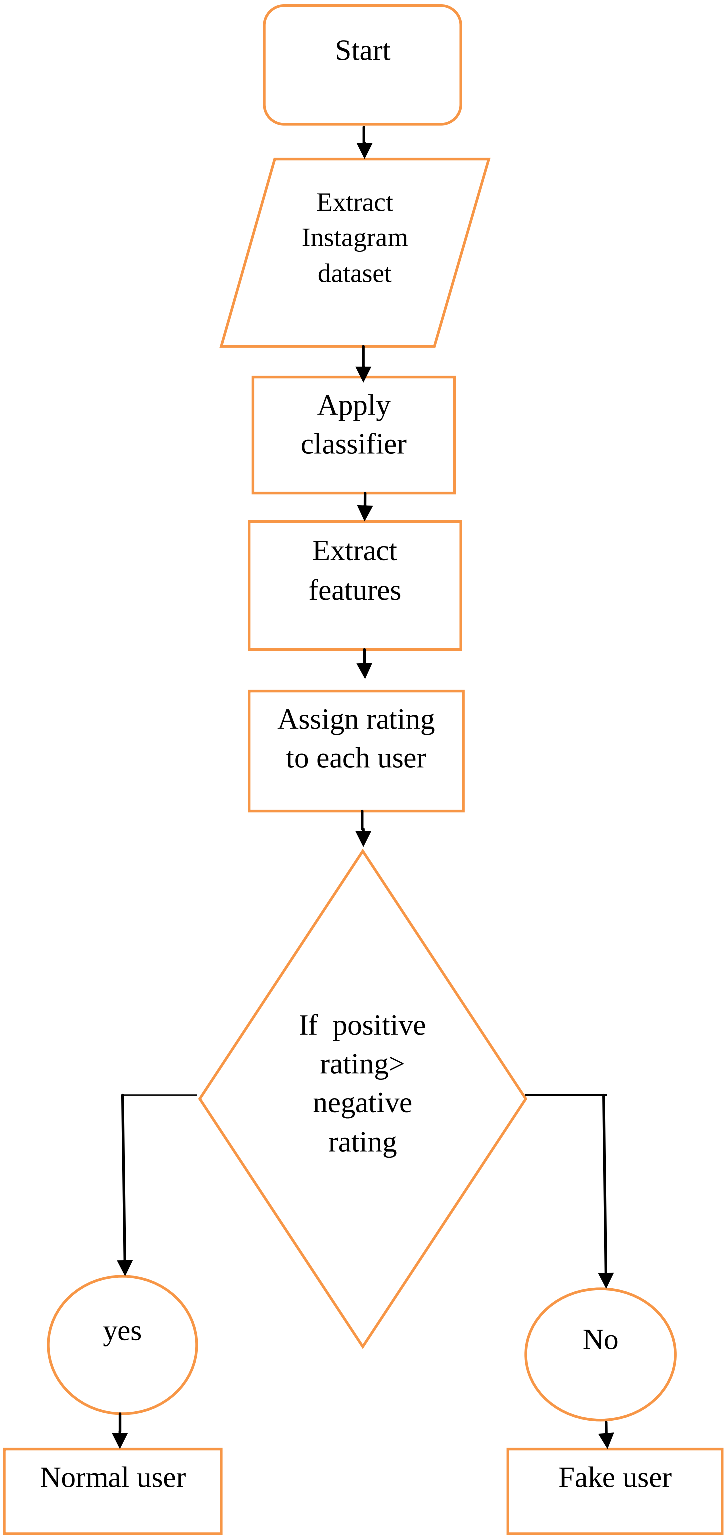
Web Defensio: To monitor user’s profile a third party application is used in this technique. It can detect if a post is legitimate or spam.. this technique helps to find the links those are used in the spam or malicious posts in the user’s profile. Its only focuses on the user profile posts to detect the malicious or spam [12].

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 [13].

FRAppE: In FRAppE malicious applications are recognized in light of some edge esteem like prevalence scores of application. It can distinguish the malicious application with exactness utilizing the no false positive and high obvious positive rate. It doesn't cover the more profound data about the biological community of malicious applications on Facebook [14].

IV. PROPOSED WORK

To identify and arrange malicious users and ordinary users here we exhibit few stages that depict how to recognize malicious users by means of flowchart. Figure 1 demonstrate the working guideline of proposed work. In initial step genuine informational index will be gathered through Instagram. After the accumulation of informational collection in subsequent stage there will be have to separate highlights of users profile by include extraction device. After the extraction of the highlights distinctive parameters will utilized like positive rating and negative rating for deciding the ordinary user and the phony users. On the off chance that positive rate is higher than negative rating then that will be recorded as a typical user else that will be dealt with as a unauthorized user.


Start
Extract Instagram dataset
Apply classifier
Extract features
Assign rating to each user
If positive rating> negative rating
yes
No
Normal user
Fake user

V. RESULTS AND ANALYSIS

Weka: It is open source software for analyzing real dataset by providing different classifiers such as random forest, naïve bayes, one R classifier etc. It is a java based tool.
Random Forest classifier: Random forest classifier collects all the dataset values and divides it into number of sub trees which are called as decision trees. After that values are assigned to these decision trees which are then classified into classes.
Metrics used:
A). Confusion matrix: A confusion matrix is a matrix that gives output into four columns having values: TP (true positive), FP (false positive), TN (true negative), and FN (false negative).
B). Recall: Recall is the TP rate. Recall matrix is used to find true positive values out of all actual positive values.

Recall = TP / actual positives

C). Precision (Positive predictive value): Precision matrix is used to find true positive values out of all predictive values.

Precision = TP / predicted Positive

D). F-measure: F-measure is the sum of precison values and recall values.

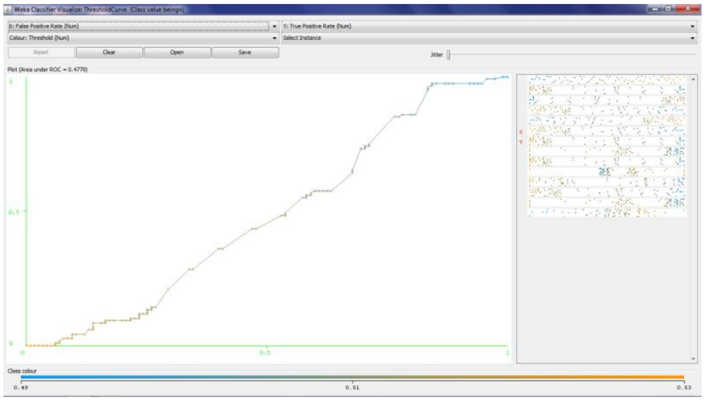
F-measure = Precision + Recall

TABLE 1: Detailed Accuracy by Class

TP Rate	FP Rate	Precision	Recall	F-Measure	Class
0.975	0.878	0.537	0.975	0.692	Normal
0.122	0.025	0.824	0.122	0.212	Malicious

TABLE 2: Confusion Matrix

A	B	Class
117	3	Normal
101	14	Malicious



Weka Classifier Visualize: ThresholdCurve. (Class value beingn)

X: False Positive Rate (Num)

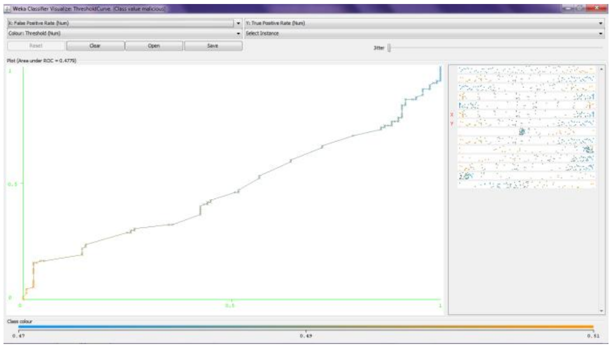
Y: True Positive Rate (Num)

Colour: Threshold (Num)

Select Instance

Plot (Area under ROC = 0.4779)

Figure.1 ROC Analysis of Random Forest Classifier Describing Normal posts


Weka Classifier Visualize: ThresholdCurve. (Class value malicious)

X: False Positive Rate (Num)
Y: True Positive Rate (Num)
Colour: Threshold (Num)
Select Instance

Plot (Area under ROC = 0.4779)

Figure.2 ROC Analysis of Random Forest Classifier Describing Malicious posts

Figure 1 and Figure 2 shows ROC (Receiver Operating Characteristic) curves of Random Forest classifier in point of view of malicious and normal curves. These curves created by plotting the false positive rate (FPR) along x-axis against the true positive rate (TPR) along y-axis at various thresholds cut points.

VI. CONCLUSION

Social networks provide new application called Instagram which is used to share images and videos. It helps user to add new videos and images and tag some of their friends. In this paper an attempt has been made to discuss different fake profile detection techniques such as Frappe, Page Rank Algorithm and Web Defensio in social networks. After that we provide a mechanism to recognize fake profiles in instagram social network. In proposed mechanism a rating is calculated of each profile of instagram and the profile getting positive rating is said o be normal otherwise it is fake profile. the proposed mechanism is analyzed using performance metrics like confusion metrics, F-Measure, Precison and R-call. The results show that proposed mechanism detects high normal posts by taking less execution time. In future try to propose mechanism which gives more better results and give correct classification of dataset.

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] M. Li, N. Cao, S. Yu, and W. Lou, “FindU: Privacy-preserving personal profile matching in mobile social networks,” in Proc. IEEE INFOCOM, Shanghai, China, 2011, pp. 2435–2443.

[6] W. Dong, V. Dave, L. Qiu, and Y. Zhang, “Secure friend discovery in mobile social networks,” in Proc. IEEE INFOCOM, Shanghai, China, 2011, pp. 1647–1655.

[7] R. Agrawal and R. Srikant, “Privacy-preserving data mining,” in ACM Sigmod Rec., vol. 29, no. 2, pp. 439–450, 2000.

[8] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, “Location privacy via private proximity testing,” in Proc. NDSS, San Diego, CA, USA, 2011.

[9] 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

[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] 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.

[12] 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.

[13] 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.

[14] 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.