IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Identification of Fake Posts in Instagram using Grade based Approach in Online Social Networks

Sanjeev Dhawan[1], Kulvinder Singh[2], Pooja[3]

[1]CSE Department, University Institute of Engineering & Technology, Kurukshetra University, Kurukshetra, India
[2] CSE Department, University Institute of Engineering & Technology, Kurukshetra University, Kurukshetra, India
[3]CSE Department, University Institute of Engineering & Technology, Kurukshetra University, Kurukshetra, India

*Corresponding Author: tayapooja1@gmail.com, Tel.: 8607475195

Available online at: www.ijcseonline.org

Accepted: 09/Jun/2018, Published: 30/Jun/2018

***Abstract*—** Now a day's use of social networking sites like Instagram, Facebook, Twitter, has increased due to its popularity on network for Communication and maintaining relationship among various users. Each user that uses the social networking sites will make its profiles and upload its private information. These social networks users are not aware of numerous security risks included in these networks like privacy and identity theft. To overcome these kind of threats, an attempt has been made in this paper to identify fake posts in instagram social networks. To identify fake posts, grade-based approach is proposed in which grade of fake profiles are distinguished from genuine profiles. The proposed mechanism is analyzed using Weka tool with performance metrics like Precision, recall, F-measure and ROC curves. The results show that proposed mechanism detects more fake posts.

***Keywords*—** *Fake Posts, Fake Profile, Instagram, Online Social Networks, and Weka.*

I. INTRODUCTION

Social network locales like Facebook, Twitter, and Google+ are encountering mind boggling development in users. There are in excess of a million users starting at now. Other than simply making a profile and connecting with companions, the social networks are presently fabricating stages to run their site[1]. These stages are constructed in light 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 well known methods for correspondence among the web users. Individuals are intensely transferring on online associations. The web is giving diverse 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 much simpler 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 distinctive intends to make

spams misrepresentation and different assaults on the users. Another methods for assault by cybercriminals is the abuse of recordings, pictures and connections appeared by the user[2]. Digital assaults fundamentally happen on social networks. Prominent destinations, for example, Facebook and Twitter as of now have a huge number of dynamic users. The prevalence of social networks makes them leaving settings to for executing malicious exercises. Because of the gigantic ubiquity 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. Cybercriminals make fascinating posts that are really lures 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 occasional occasions, superstar news and even debacles. Aggressors transfer malicious posts in the period of exceptional occasions and fiascos. They will transfer malicious posts which are identified with these occasions and mislead users to click those connections. Users who tap the connections by botch go about as a foe to the assailant on the grounds that the malicious posts would naturally re-posts the malicious substance, for example, connections, pictures or recordings on the user profile. Another prominent form of this assault brings about user profiles to "like" a Facebook page without their insight. Now and again the, spammed posts will lead the users to overview locales which will bring about digital crooks getting benefit. Social network locales give restricted instruments to confine the introduction of user profile information to applications[3]. On account of Facebook, for instance, adopts a win or bust strategy. At the point when users visit an application out of the blue, they should offer authorization to enable that application to get to all required profile information. This single decision is to not utilize or visit the application by any means. Nonetheless, even this does not ensure any honest to goodness safe [4].

This paper is divided into five sections. In section i introduction of social networks are presented after that section ii covers related work of recent research papers with their limitations in section iii proposed mechanism is presented in detail. Section iv presents results and analysis of proposed mechanism at last section v covers conclusion of paper.

II. RELATED WORK

Dhawan and Ekta [5] dissected different existing procedures that incorporates examination in context of different applications mapping different execution parameters. This incorporates reject to, frappe, my page manager and so forth. Advantages and disadvantages of every strategy have been examined. After that Implication of these methods in context of utilizations and execution parameter have been represented. MoreoverEkta [6] proposed notoriety based system which can recognize authentic posts and the malicious posts in Facebook Social Networks. To gather the dataset for the usage of proposed strategy Netvizz application was utilized. Netvizz application was effortlessly accessible on Facebook and gathers the data of the user's information. To imagine the dataset Gephi apparatus was used.Similarly, Dhawan et al.[7] displayed talked about various existing strategies to recognize malicious posts in Facebook with their upsides and downsides. After that a similar investigation has been done on these systems and examination demonstrates that Web defensiowas a superior strategy in context of my page manager and page rank algorithm.Moreover, Dhawan et al.[8]presented diverse classifiers strategies that are utilized to distinguish the user character whether it was fake or honest to goodness. Distinctive grouping methods are utilized to streamline the exactness, accuracy, time multifaceted nature, and review for a given info. Based on charts got, it can be inferred that the KNN classifier was giving best outcomes when contrasted with other two classifiers. So also, Tiwari [9] surveyed numerous techniques to distinguish the fake profiles and their online social bot. Multi specialist point of view of online social networks has additionally been broke down. It additionally talked about the Machine learning strategies valuable in profile creation and investigation. Fake records have been always advancing throughout the years keeping in mind the end goal to sidestep their identification. Consequently, it is critical to create strategies for identifying fake records, keeping into account their close genuine conduct. In light of this prerequisite, Gupta and Kaushal [10] had made first endeavors to recognize fake records on Facebook in light of the user profile exercises and cooperation with different users on Facebook. These exercises were portrayed through a comprehensive list of capabilities covering the like, remark, share, label propensities and applications utilization of Facebook users.

III. PROPOSED WORK

In this paper a framework to distinguish fake profiles based on grade of profiles in Instagram has been presented. Here Figure 1 shows the working principle of proposed grade based approach.In grade based approach the first step is to collect real data set through Instagram. This dataset is in the format of CSV i.e. comma separated values. After the collection of data set in next step there will be need to extract features of users profile such as post id, user id etcby feature extraction tool. After the extraction of the features grade of each post is calculated. A grade shows the credits of each post posted by different instagram users. This grade is calculated by calculating mean value of likes, comments, shares and reactions. Now compare grade of each post with average grade value. If grade value of post is less thanaverage grade value then post is treated as normal post otherwise it will be treated as malware post generated by some fake profile user. In this manner proposed framework can distinguish fake profile user or normal user in instagram.

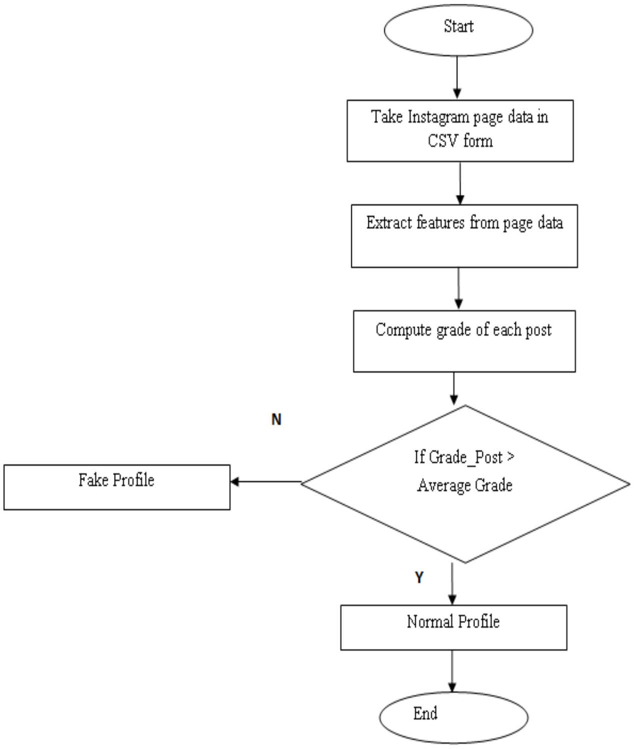

Start
Take Instagram page data in CSV form
Extract features from page data
Compute grade of each post
N
If Grade_Post > Average Grade
Fake Profile
Y
Normal Profile
End

Fig 1 Proposed framework

In the proposed mechanism, random forest classifier is used to classify the fake profiles and normal profiles.

Random Forest classifier is a gathering learning technique utilized for relapse, characterization and different errands. First calculation for arbitrary timberland was made by Tin Kam Ho. Later on it was altered by different specialists. The preparation calculation for irregular backwoods utilizes the procedure of bootstrap totaling or packing to tree students. This bootstrapping methodology prompts better ex/ecution models as the change estimation of the model is diminished without bargaining the predisposition. This is done to maintain a strategic distance from connection of trees in straightforward bootstrap test which is on account of once in a while a component can be a solid indicator of the objective variable[11].

IV. RESULTS

In this paper Python language is used to implement proposed mechanism and to analyze the performance of proposed mechanism,Weka tool is used[12]. The performance metrics used for analysis are as follows:

- True Positives (TP): Terms that were correctly identified as entities.
- False Positives (FP): Terms that were identified as entities but should not have been.
- True Negative (TN): Terms that were not identified as entities and should not have been.
- False Negative (FN): Terms that were not identified as entities but should have been.

Precision: As precision is a measure of exactness that reflects False Positives, given by above equation, if the number of false positives becomes zero; precision becomes 1 which means exactness of the proposed algorithm is perfect. Also, large number of false positive that surpasses true positives indicates value approaching 0; poor precision.

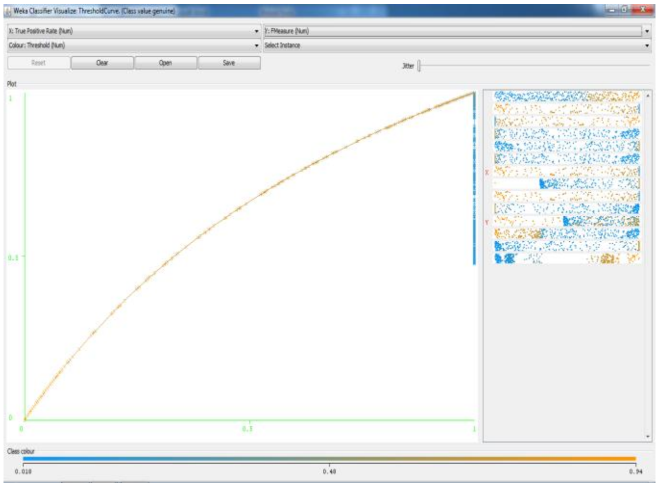
Recall: Recall is a measure of completeness, as given by above formula, indicates a perfect recall value if number of false negatives becomes zero. As the number of false negatives increase, recall approaches zero.

Confusion Matrix:It is defined as a table M that is used to describe the performance of a classification model on a set of data values for which true values are known.

Table 1 Confusion Matrix

TP	FP
FN	TN

ROC Curve: It is a graph that summarizes the performance of a classifier over all possible thresholds. It is plotted by taking False Positive Rate along x-axis and True Positive Rate along Y-axis [50].


Weka Classifier Visualize: ThresholdCurve. (Class value genuine)

X: True Positive Rate (Num)

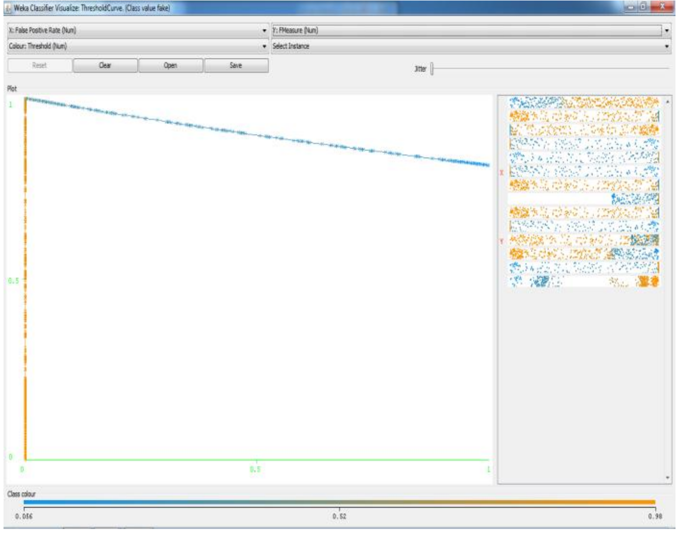
Y: FMeasure (Num)

Colour: Threshold (Num)

Select Instance

Fig 2 ROC curve with genuine profiles

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


Weka Classifier Visualize: ThresholdCurve. (Class value fake)

X: False Positive Rate (Num)

Y: FMeasure (Num)

Colour: Threshold (Num)

Select Instance

Fig 3 ROC curve of fake profiles

Figure 3 shows ROC (Receiver Operating Characteristic) curves of Random Forest classifier in perspective of True positive rate and false positive rate. These curves created by plotting the true positive rate (FPR) along x-axis against the false positive rate (TPR) along y-axis at various thresholds cut points.

Table 1 Confusion Matrix

A	B	A= Genuine profiles
337	2	B=Fake profiles
1	741	

Table 1 shows confusion matrix in which variable a show recommended product while variable B shows not recommended products. In this table total numbers of recommended products and not recommended products are represented. In proposed work 337posts are normal and 741posts are fake.

V. CONCLUSION

Instagram is a new application of social network where users can share their images and videos as a post on their profile and tag their friends in posts that they shared. A fake profile user can tag different person in fake or wrong posts that will not suitable according to user profiles so it is very difficult to find these fake posts from instagram. In this paper an attempt has been made to identify fake posts in instagramsocial networks. The advances in digital and multimedia technology are significantly impacting human behaviors and social interactions. The main idea of proposedmechanism is to develop an grade based system for detecting suspicious profiles in the social media, through which uncover suspicious behavior can be uncovered.In future formulate a hybrid approach for detecting fake profiles by combining present approach with graph-based techniques. This paper would like to provide a web service to instagram users as an online application or a mobile application to facilitate determination of a given profile as fake or real.

REFERENCES

[1]. ShikhaAgrawal, JitendraAgrawal, " Survey on Anomaly Detection using Data Mining Techniques": 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems, Procedia Computer Science 60, page no. 708 – 713,Year of publication 2015.

[2]. Nandhini, M. and Das, B.B., "An assessment and methodology for fraud detection in online social network", IEEE Second International Conference on In Science Technology Engineering and Management (ICONSTEM), pp. 104-108,2016.

[3]. Yadav, Neha M., and P. N. Chatur. "Compromised Account Detection and Prevention by Profiling Social Behavior and FASS Key Concept." In Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT),International Conference on, pp. 164-168. IEEE, 2017.

[4]. Van Der Walt, Estée, and Jan Eloff. "Using Machine Learning to Detect Fake Identities: Bots vs Humans." IEEE Access 6 (2018): 6540-6549.

[5]. Egele, Manuel, GianlucaStringhini, Christopher Kruegel, and Giovanni Vigna. "Towards detecting compromised accounts on social networks." IEEE Transactions on Dependable and Secure Computing 14, no. 4 (2017): 447-460.

[6]. Dr. SanjeevDhawanandEkta, "Implications of Various Fake Profile Detection Techniques in Social Networks", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, pp:49-55,2016.

[7]. Ekta, " Reputation Based Technique to Distinguish Posts in Facebook Social Network ", 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), pp:307-312,2016.

[8]. SanjeevDhawan, KulvinderSinghand Sanjay Sagwal, "Identification of Malicious Posts in Facebook Social Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, ISSN: 2456-3307, Vol.2, Issue 5, pp: 43-46, 2017.

[9]. SanjeevDhawan, Kulvinder Singh and Satinder, "Uncovering of Fake Users in Twitter Using Classifiers", International Journal of Emerging Technologies in Computational and Applied Sciences,ISSSN:2279-0055pp:75-80, 2016.

[10]. Dr Vijay Tiwari, " Analysis and Detection of Fake Profile Over Social Network ", International Conference on Computing, Communication and Automation, pp: 175-179, 2017.

[11]. https://towardsdatascience.com/the-random-forest-algorithm-d457d499ffcd?gi=1ae814c17d8d accessed on 22-05-2018.

[12]. https://machinelearningmastery.com/what-is-the-weka-machine-learning-workbench/ accessed on 22-05-2018.

Authors Profile

Pooja has completed Bachelor of Technology from Kurukshetra Institute of Technology & Management in 2015. She is currently pursuing Master's Of Technology in Computer Science and engineering from University Institute of Engineering Technology, Kurukshetra, Haryana.