

CSE3021- Social and Information Networks

J Component – Review 1 -Project Report

FAKE PROFILE DETECTION SYSTEM

By

Reg. No: 20BCE1560

Reg. No: 20BCE1650

Name: *Kunal Gupta*

Name: *Amritansh Anand*

B.Tech CSE-CORE

Submitted to

Dr.A.Bhuvaneswari,

Assistant Professor Senior,
SCOPE, VIT, Chennai

School of Computer Science and Engineering



VIT[®]

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

August 2022



VIT[®]

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computing Science and Engineering

VIT Chennai

Vandalur - Kelambakkam Road, Chennai - 600 127

FALL SEM 22-23

Worklet details

<i>Programme</i>	B.Tech with CSE-CORE	
<i>Course Name / Code</i>	Social and Information Networks – CSE3201	
<i>Slot</i>	B1+TB1	
<i>Faculty Name</i>	Dr.A.Bhuvaneswari	
<i>Component</i>	J – Component	
<i>J Component Title</i>	Fake Profile Detection System	
<i>Team Members Name Reg. No</i>	Kunal Gupta	20BCE1560
	Amritansh Anand	20BCE1650

Team Members(s) Contributions:

<i>Worklet Tasks</i>	<i>Contributor's Names</i>
Dataset Implementation	Amritansh Anand & Kunal Gupta
Preprocessing	Amritansh Anand & Kunal Gupta
Model building	Amritansh Anand & Kunal Gupta
Visualization	Amritansh Anand & Kunal Gupta
Technical Report writing	Amritansh Anand & Kunal Gupta
Presentation preparation	Amritansh Anand & Kunal Gupta

ABSTRACT

In the present generation, the social life of everyone has become associated with 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 solutions exist to control these problems. In this report, we came up with a framework with which the automatic identification of fake profiles is possible and is efficient. This framework uses classification techniques like Random Forest Classifier 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 that have millions of profiles whose profiles cannot be examined manually. Also, we will be comparing the result with the another method of implementation that is already existing, i.e., SVM (Support Vector Machine).

1.Introduction

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) use web2.0 technology, which allows users to interact with each other. Social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with the same interests together which makes users easier to make new friends.

In today's online social networks there have been a lot of problems like fake profiles, online impersonation, etc. To date, no one has come up with a feasible solution to these problems. In this project, I intend to give a framework with which the automatic detection of fake profiles can be done so that the social life of people become secured and by using this automatic detection technique we can make it easier for the sites to manage the huge number of profiles, which can't be done manually.

2.Literature Survey

Sl. no	Title	Author / Journal name / Year	Technique	Result (Accuracy)
1	Identifying Fake Profiles in LinkedIn	Shalinda Adikari & Kaushik Dutta arXiv preprint arXiv: 2006.01381 (2020)	Number of languages spoken, education, skills, recommendations, interests, awards, etc. are used as features to train neural networks, SVMs, and principal component analysis.	84% TP, 2.44% FN

2	Source Based Fake News Classification using Machine Learning	Avinash Bharadwaj, Brinda Ashar IJIRSET, 2020	I. Text classification via Bayesian classifier (Orthogonal Sparse Bigram); 2. Regularity of tweets; 3. Frequency and types of URLs; the use of APIs.	100%
3	Identifying Fake Profile in Online Social Network: An Overview and Survey.	Shruti Joshi International Conference on Machine Learning, Image Processing, Network Security and Data Sciences. Springer, Singapore, 2020.	In a general approach for the identification of fake accounts in large scale online social networks following steps are used: <ul style="list-style-type: none"> • Data collection. • Feature selection. • Feature extraction. • Data classification/techniques used. 	79%
4.	The social honeypot project: protecting online communities from spammers	Kyumin Lee & Steve Webb Proceedings of the 19th International Conference on World Wide Web, WWW 2010, Raleigh, North Carolina, USA, 2010	Over 60 classifiers available in Weka are tried. Features include: i) demographics, ii) content and iii) frequency of content generation, iv) number and type of connections. The Decorate meta-classifier provided the best results.	99,21% (MySpace). 88.98% (Twitter)
5.	Detecting spammers on social networks	Gianluca Stringhini Twenty-Sixth Annual	Random forest was constructed based on the following features: ratio of accepted friend requests, URL. ratio, message similarity, regularity in	2% FP. 1% FN (Facebook): 2.5% FP. 3.0%

		Computer Security Applications Conference, ACSAC 2010, Austin, Texas, USA, 2010	the choice of friends, messages sent, and number of friends.	EN (Twitter)
6.	Twitter spam detection: Survey of new approaches and comparative study	Yang Xiang & Tingmin Wu November 2017	Graph based features (local clustering coefficient, betweenness centrality, and bi-directional links ratio), neighbor-based features (e.g. average neighbors' followers), automation-based features (API ratio, API URL ratio and API Tweet similarity), and timing-based features were used to construct different classifiers.	86% TP. 0,5% EP
7.	Aiding the Detection of Fake Accounts in Large Scale Social Online Services	Xiaowei Yang USENIX conference, 2012	Invitation frequency, rate of accepted outgoing and incoming requests, and clustering coefficient were used as features for an SVM classifier.	99%
8.	Towards Detecting Fake User Accounts in Facebook	Aditi Gupta & Rishabh Kaushal 2017 ISEA Asia Security and Privacy (ISEASP) January 2017	Machine learning classification techniques on a basic dataset comprising of our own node and our friends in our social neighborhood and also a set of manually identified spam accounts.	accuracy of 79%. (79%)
9.	Facebook immune system	Stein, Tao, Erdong Chen, and Karan	To protect the graph the Immune System runs classifiers to block and respond and anomaly detection	82%

		<p>Mangla</p> <p>Proceedings of the 4th workshop on social network systems, 2011</p>	<p>to detect new and mutated attacks. Developing, deploying, and operating these classifiers has a number of challenges. Attacks mutate across different channels within a large user-interface surface area. The system must defend against these attacks while meeting severe scalability and latency requirements. This section discusses several of the important system requirements.</p>	
10.	<p>Detecting fake accounts on social media.</p>	<p>2018 IEEE International Conference on Big Data (Big Data). IEEE, 2018</p>	<p>In this paper, a new algorithm, SVM-NN, is proposed to provide efficient detection for fake Twitter accounts and bots, feature selection and dimension reduction techniques were applied. Machine learning classification algorithms were used to decide the target accounts identity real or fake, those algorithms were support vector machine (SVM), neural Network (NN), and our newly developed algorithm, SVM-NN.</p>	<p>98%</p>

3.Dataset and Tool to be used

We needed a dataset of fake and genuine profiles. Various attributes included in the dataset are a number of friends, followers, status count. Dataset is divided into training and testing data. Classification algorithms are trained using a training dataset and the testing dataset is used to determine the efficiency of the algorithm. From the dataset used, 80% of both profiles (genuine and fake) are

used to prepare a training dataset and 20% of both profiles are used to prepare a testing dataset.

LINK TO DATASET:

<https://www.kaggle.com/datasets/joewilson02/social-media-fake-account>

4. Algorithms / Techniques description

The classifier that we have implemented for classifying the profiles is Random Forest.

Random forest is a supervised learning algorithm that is used for both classifications as well as regression. But however, it is mainly used for classification problems. As we know that a forest is made up of trees and more trees mean more robust forests. Similarly, the random forest algorithm creates decision trees on data samples and then gets the prediction from each of them and finally selects the best solution by means of voting. It is an ensemble method that is better than a single decision tree because it reduces the over-fitting by averaging the result.

We can understand the working of the Random Forest algorithm with the help of following steps:

Step 1 – First, start with the selection of random samples from a given dataset.

Step 2 – Next, this algorithm will construct a decision tree for every sample.

Then it will get the prediction result from every decision tree.

Step 3 – In this step, voting will be performed for every predicted result.

Step 4 – At last, select the most voted prediction result as the final prediction result.

5. Github Repository Link

https://github.com/amritansha28/amritanshkunal_fakeprofiledetection

REFERENCES

- [1] Mohanty, Sachi, et al. Recommender System with Machine Learning and Artificial Intelligence. Wiley-Scrivener, 2020.
- [2] Balaanand, Muthu, et al. "An enhanced graph-based semi-supervised learning algorithm to detect fake users on Twitter." The Journal of Supercomputing 75.9 (2019): 6085-6105.
- [3] Boshmaf, Yazan, et al. "Integro: Leveraging Victim Prediction for Robust Fake Account Detection in OSNs." NDSS. Vol. 15. 2015.
- [4] Erşahin, Buket, et al. "Twitter fake account detection." 2017 International Conference on Computer Science and Engineering (UBMK). IEEE, 2017.
- [5] Mateen, Malik, et al. "A hybrid approach for spam detection for Twitter." 2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST). IEEE, 2017.
- [6] Gupta, Arushi, and Rishabh Kaushal. "Improving spam detection in online social networks." 2015 International conference on cognitive computing and information processing (CCIP). IEEE, 2015.
- [7] Nazir, Atif, Saqib Raza, Chen-Nee Chuah, Burkhard Schipper, and C. A. Davis. "Ghostbusting Facebook: Detecting and Characterizing Phantom Profiles in Online Social Gaming Applications." In WOSN. 2010.
- [9] Chu, Zi, Steven Gianvecchio, Haining Wang, and Sushil Jajodia. "Who is tweeting on Twitter: human, bot, or cyborg?." In Proceedings of the 26th annual computer security applications conference, pp. 21- 30. ACM, 2010.
- [10] Stringhini, Gianluca, Gang Wang, Manuel Egele, Christopher Kruegel, Giovanni Vigna, Haitao Zheng, and Ben Y. Zhao. "Follow the green: growth and dynamics in twitter follower markets." In Proceedings of the 2013 conference on Internet measurement conference, pp. 163-176. ACM, 2013.