ISSN:0975-9646

# Prediction of Fake Profiles on Facebook using Supervised Machine Learning Techniques-A Theoretical Model.

Suheel Yousuf Wani,
*IIIT Banglore*

Mudasir M Kirmani,
*SKUAST-K, J&K*

Syed Imamul Ansarulla,
*MANUU, Hyderabad*

**Abstract-Facebook is a social networking site. This site has changed the way people pursue social life and made it easy to connect with family members, classmates, friends and colleagues. Based on the data available for the first quarter of 2016 facebook has approximately 1.65 billion active users. However, the number of fake profiles has increased manifold and research work of different researchers shows that 20% to 40% of the user profiles available on facebook are fake profiles. but with the fast growth of users, fake profiles/users has also grown. In order to detect and minimize the number of fake profiles on facebook very few techniques do exist. This research work is an effort to explain a theoretical model using which fake profiles can be detected on facebook. The proposed model has used machine learning algorithms like support vector machine(SVM), Decision Tree(DT), artificial neural networks(ANN) and Nave Bayaes (NB) to classify the user profiles into fake and genuine.**

**Keywords: Machine Learning, fake profile detection, ensemble classifier.**

## 1. INTRODUCTION:

### *1.1 Facebook:*

Facebook is an online social networking service where after registering to use the site, users can create user profile, add other users as friends, exchange messages, post status updates, photos, and share videos etc. Facebook site is becoming popular day by day and more and more people are creating user profiles on this site[1][2]. Adding new friends and keeping in contact with them and their updates has become easier with facebook. The social networking sites like facebook are making our social lives better but nevertheless there are a lot of issues which need to be addressed while using facebook. The issues realted to social networking like privacy, online bullying, misuse, and trolling etc. are most of the times used by fake profiles on social networking sites [3]. Fake profiles are the profiles which are not genuine i.e. they are the profiles of persons with false credentials. The fake facebook profiles generally are indulged in malicious and undesirable activities, causing problems to the social network users. People create fake profiles for social engineering, online impersonation to defame a person, advertising and campaigning for an individual or a group of individuals [3]. Facebook has its own security system to protect user credentials from spamming, phishing, etc. and the same is known as Facebook Immune System (FIS) [4][6][7]. The FIS has not been able to detect fake profiles created on facebook by users to a larger extent.

### *1.2 Machine Learning(ML):*

Machine learning is a branch of computer science which deals with the study of algorithms that have ability to learn [8] [9] [10]. Machine learning algorithms are computer programs that try to predict profile type based on the data available with the algorithm related to past experiences. ML algorithms operate by building a model from example inputs in order to make data-driven predictions or decisions expressed as outputs rather than following strictly static program instructions [9]. There are two main common types of ML methods known as

(i) Supervised Learning and
(ii) Unsupervised Learning.

In supervised learning a labeled set of training data is used to estimate or map the input data to the desired output. In contrast, under the unsupervised learning methods no labeled examples are provided and there is no notion of the output during the learning process. In Supervised learning, input data is called training data and has a known label or result such as spam/not-spam at a time. A model is prepared through a training process where it is required to make predictions and is corrected when those predictions are wrong. The training process continues until the model achieves a desired level of accuracy on the training data. The goal of machine learning in fake facebook profile detection is to have trained machine learning algorithm that, given the data of a particular profile like age, gender, numbers of facebook friends etc. This data can facilitate in predicting whether a profile is fake or genuine effectively and will result in ensuring security of data on facebook and other social networking sites. This machine learning model model can make it easier for the facebook to manage the huge number of profiles existing in the database. The machine learning algorithms that have been proposed to be used in this model are Support Vector Machine (SVM), Decision Tree (DT), Artificial Neural Networks (ANN) and Naïve Bayes (NB).

***Support Vector Machines (SVM):***

An SVM classifies data by finding the best hyper-plane that separates all data points of one class from those of the other class. The best hyper-plane for an SVM means the one with the largest margin between the two classes. An SVM classifies data by finding the best hyper-plane that separates all data points of one class from those of the other class. The support vectors are the data points that are closest to the separating hyper-plane. [11]

***Decision Tree:***

Decision tree builds classification or regression models in the form of a tree structure. It breaks down a dataset into smaller and smaller subsets while at the same time an associated decision tree is incrementally developed. The final result is a tree with decision nodes and leaf nodes. A decision node has two or more branches. Leaf node represents a classification or decision and the topmost decision node in a tree which corresponds to the best predictor is known as root node. Decision trees can handle both categorical and numerical data for prediction.

***Artificial Neural Networks (ANN):***

In machine learning and cognitive science, artificial neural networks (ANNs) are a family of models inspired by biological neural networks (the central nervous systems of animals, in particular the brain) which are used to estimate approximate functions that can depend on a large number of inputs and are generally unknown [19]. Artificial neural networks are generally presented as systems of interconnected "neurons" which exchange messages between each other. The connections have numeric weights that can be tuned based on experience, making neural nets adaptive to inputs and capable of learning.

***Naive Bayes Algorithm:***

In Bayesian classification, proposed work has a hypothesis that the given data belongs to a particular class. The model then calculates the probability for the hypothesis of being true. This is among the most practical approaches for certain types of problems. The approach requires only one scan of the whole data. At any stage additional training data is added then each training example can incrementally increase or decrease the probability that the hypothesis is correct.

### *1.3 Ensemble classifier and AdaBoost:*

In machine learning, there is a new concept of combining ML algorithms (classifiers) that are cooperatively trained on data set in a supervised classification problem. And these ensembles of classifiers could achieve more certain, precise and accurate results by giving a new dimention to the research work carried out in an effort to improve the performance of individual classifiers. Boosting is a type of ensemble classifier in machine learning which helps in predicting accurately by combining many relatively weak and inaccurate machine learning algorithms [12] [13]. The AdaBoost algorithm proposed by Freund and Schapire was the first practical boosting algorithm, and remains one of the most widely used and studied, with applications in diverse domain across horizontals and verticals [12].

### *1.4 Feature Selection:*

Three main approaches exist for feature selection namely embedded, filter and wrapper approaches [14]. In case of feature extraction, a new set of features can be created from the initial set that captures all the significant information in a dataset. The creation of new set of features allows for gathering the described benefits of dimensionality reduction. In this research work hybrid of two natural inspired algorithms “Artificial Bee Colony (ABC)” and “Ant Colony Optimization(ACO)” has been used for feature selection [14].

*Artificial Bee Colony (ABC) algorithm:*

Artificial Bee Colony (ABC) is one of the most recently defined algorithms by Dervis Karabogain 2005, motivated by the intelligent behavior of honey bees. It is similar to Particle Swarm Optimization (PSO) and Differential Evolution (DE) algorithms, and uses only common control parameters such as colony size and maximum cycle number. ABC algorithm is an optimization tool which provides population-based search procedure in which individuals called as food-positions are modified by the artificial bees with time and the bee’s aim is to discover the places of food sources with high nectar amount. In ABC algorithm, artificial bees fly around in a multidimensional search space and some (employed and onlooker bees) choose food sources depending on the experience of themselves and their nest mates to adjust their position appropriately. Some scout flies choose the food sources randomly without using experience. If the nectar amount of the new source is higher than that of the previous one in their memory, they memorize the new position and forget the previous one. Thus, ABC system combines local search methods, carried out by employed and onlooker bees, with global search methods, managed by onlookers and scouts, attempting to balance exploration and exploitation process. ABC algorithm is used to select the important features in a data set so that the classifier will be trained very accurately.

*Ant Colony Optimization(ACO) algorithm:*

Ant colony optimization (ACO) is a population-based meta-heuristic that can be used to find approximate solutions to difficult optimization problems. In ACO, a set of software agents called artificial ants search for good solutions to a given optimization problem. To apply ACO, the optimization problem is transformed into the problem of finding the best path on a weighted graph. The artificial ants (hereafter ants) incrementally build solutions by moving on the graph. The solution construction process is stochastic and is biased by a pheromone model, that is, a set of parameters associated with graph components (either nodes or edges) whose values are modified at runtime by the ants. ACO is a natural inspired algorithm which is also used in feature reduction in huge data sets so that the machine learning algorithms will be trained very accurately.

### *1.5 Weka Tool:*

Weka is a collection of machine learning algorithms for data mining tasks. The algorithms can either be applied directly to a dataset or called from Java code. Weka contains tools for data pre-processing, classification, regression, clustering, association rules, and visualization. It is also well-suited for developing new machine learning schemes. In this model weka tool was used for the prediction of fake profile by using its ensemble classifier.

## 2.0 OUR CONTRIBUTION:

In this research work, a novel approach has been presented for the prediction of fake profiles on facebook using supervised machine learning algorithms. The proposed model has applied sophisticated noise removal and data normalization techniques on datasets before analyzing them. A technique has been applied to identify the non-significant attributes in datasets and to do attribute reduction accordingly by applying natural inspired algorithms like Artificial Bee Colony (ABC), Ant Colony Optimization (ACO). The proposed model was trained using supervised machine algorithms individually for both data sets i.e. fake and genuine. Ensemble classifier has been used to make the prediction more accurate as shown in the figure 1.

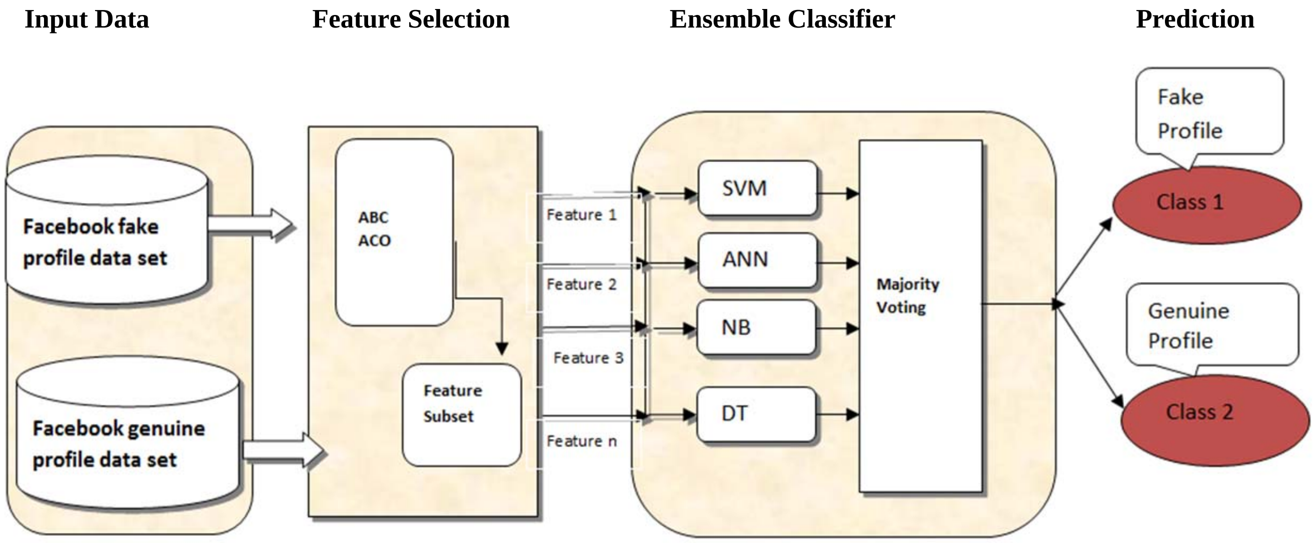

Figure 1.

A common problem with machine learning is over fitting i.e. bias towards the samples in the training set. An algorithm may perform well on the training set and the same may not hold true for other data set. Therefore, cross-fold validation was used, where the data is partitioned into training and testing data in different ways where each partition is called as a fold. The performance of the algorithm is average of all the folds. Which samples are used for training and which for testing can impact the measured performance, so the cross-fold validation is implemented multiple times with different folds. This research work used 5-fold cross validation where the data was split into 5 equal subsets, each of which was held out in turn as the testing data while the algorithm was trained on the remaining 4 subsets. The end results were noted based on the efficiency of the model which was calculated using False Positive and False Negative Analysis. The results calculated justified that the AdaBoost classifier efficiency increases with the increase in number of profiles in training dataset.

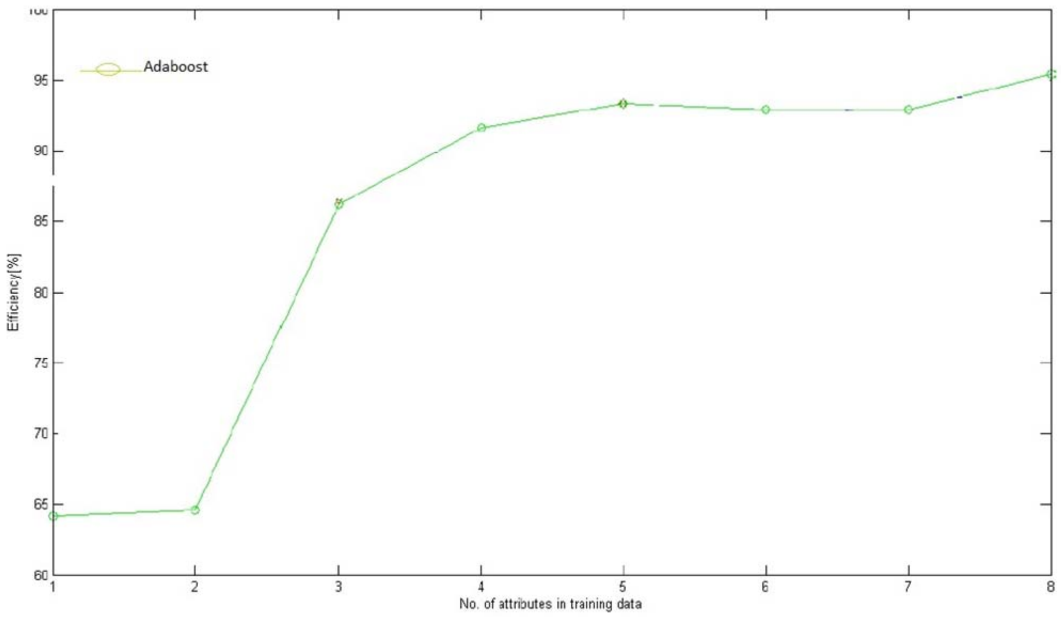

Figure 2: Efficiency vs No. of profiles in training dataset

## 3.0 CONCLUSION:

In this research work a theoretical machine learning model has been proposed for prediction of fake profiles on facebook. The evaluation of the theoretical model using ensemble classifiers showed good performance using Weka tool for detection of fake profiles on facebook. Based on the analysis in this research work it was concluded as there is no such model being used for detection of fake as well genuine facebook profiles. Therefore, a combination of two or more machine learning algorithms can be used for detection of fake as well as genuine profiles on facebook.

## REFERENCES:

[1] Facebook-Newsroom. http://www.facebook.com.

[2] Nielsen. The social media report. http://blog.nielsen.com/nielsenwire/social

[3] 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.

[4] D. DeBarr and H. Wechsler. Using social network analysis for spam detection. Advances in Social Computing, pages 62–69, 2010.

[5] Facebook. Report abuse or policy violations.

[6] M. Conti, R. Poovendran, and M. Secchiero. Fakebook: Detecting fake profiles in on-line social networks. In Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012), ASONAM ’12, pages 1071–1078, Washington, DC, USA, 2012. IEEE Computer Society.

[7] 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.

[8] 2011 IEEE International Conference on, pages 295{300. IEEE, 2011. [10] Bishop CM. Pattern recognition and machine learning. New York: Springer; 2006.

[9] Mitchell TM. The discipline of machine learning: Carnegie Mellon University. Carnegie Mellon University, School of Computer Science, Machine Learning Department; 2006.

[10] Witten IH, Frank E. Data mining: practical machine learning tools and techniques. Morgan Kaufmann; 2005.

[11] Platt JC, Cristianini N, Shawe-Taylor J. Large margin DAGs for multiclass classification; 1999 547–53.

[12] P.L., Traskin, M.: AdaBoost is consistent. Journal of Machine Learning Research 8, 2347–2368 (2007)

[13] Bickel, P.J., Ritov, Y., Zakai, A.: Some theory for generalized boosting algorithms. Journal of Machine Learning Research 7, 705–732 (2006)

[14] Y. He & S.C. Hui, “Exploring ant-based algorithms for gene expression data analysis,” *Artif.Intell.Med.* vol. 47, pp. 105–19, 2009.