THINK INDIA (Quarterly Journal)

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Automatic Detection of Fake Profiles in Online Social Network

Sudipta Acharjee,
sudipta8960acharjee@gmail.com,
Guru Nanak Dev Institute of Technology, Delhi

Abstract

In the present generation, the social life of everyone has become associated with the online social networks (OSN) like Facebook, Twitter etc. 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 the rapid growth in their membership profiles, many problems like fake profiles, online impersonation have also grown. It is almost impossible to examine such huge profiles manually to control these problems. In literature, there are no feasible solution exist to control these problems automatically. In this paper, we propose a framework for automatic detection of fake profiles by the OSNs. This framework will use classification techniques like Support Vector Machine, Nave Bayes Probabilistic and Decision trees approach to best classify the profiles into fake or genuine classes. The simulation results prove the efficiency of the proposed framework.

Keywords: **Online Social Networks, Fake profiles, Online Impersonation, Support Vector Machine, Nave Bayes Probabilistic and Decision tree**

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. Face book was launched in 2004 and presently it is the largest social networking site in the world. These online social networks are growing rapidly and there are more than 160 major social network websites exist in the world. 300 million active accounts in Face book [3, 4, 5]. The social networking sites are making our social lives better but nevertheless there are a lot of issues with using these social networking sites. The issues are privacy, online bullying, potential for misuse, trolling, etc.[13,14,15] These are done mostly by using fake profiles. Intoday's online social networks there have been a lot of problems like fake profiles, online impersonation, etc. Till date, no one has come up with a feasible solution to these problems. In this project we 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 cannot be done manually[6,7,8].This framework will use classification[9,10] techniques like Support Vector Machine, Nave Bayes Probabilistic and Decision trees approach[8] to best 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 profilesthat cannot be examined manually.

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Literature Review

Fake profiles are the profiles which are not genuine [1]. The reason behind to create fake profiles is to defame a person and advertising and campaigning for a person [2]. Social Engineering in terms of security means the art of stealing confidential information from people or gaining access to some computer system mostly not by using technical skills but by manipulating people themselves in divulging information. The hacker does not need to come face to face with the user to do this [11, 12].

Earlier work on threats on OSN

Year with Paper and Conference	Author	Work done
In Proceedings of the 4th Workshop on Social Network Systems, SNS, volume 11, page 8, 2011[1]	T. Stein, E. Chen, and K. Mangla	Facebook immune system.
In Proceedings of the 27th Annual Computer Security Applications Conference, pages 93{102. ACM, 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 WWW, volume 12, 2012[3]	C. Wagner, S. Mitter, C. K•orner, and M. Strohmaier	When social bots attack: Modeling susceptibility of users in online social networks.
In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on, pages 295{300. IEEE, 2011.[4]	G. Kontaxis, I. Polakis, S. Ioannidis, and E.P. Markatos	Detecting social network profile cloning.
Data and Applications Security and Privacy XXIV, pages 335{342, 2010. [5]	A. Wang.	Detecting spam bots in online social networking sites: a machine learning approach.
In Proceedings of the 10th annual conference on Internet measurement, pages 35{47. ACM, 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 26th Annual Computer Security Applications Conference, pages 21{30. ACM, 2010. [7]	Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia	Who is tweeting on twitter: human, bot, or cyborg?
In Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC, pages 255{261. IEEE, 2007. [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

Proposed framework

The proposed framework in the figure 3.1 shows the sequence of processes that need to be followed for

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

continues detection of fake pro les 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 pro le 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.

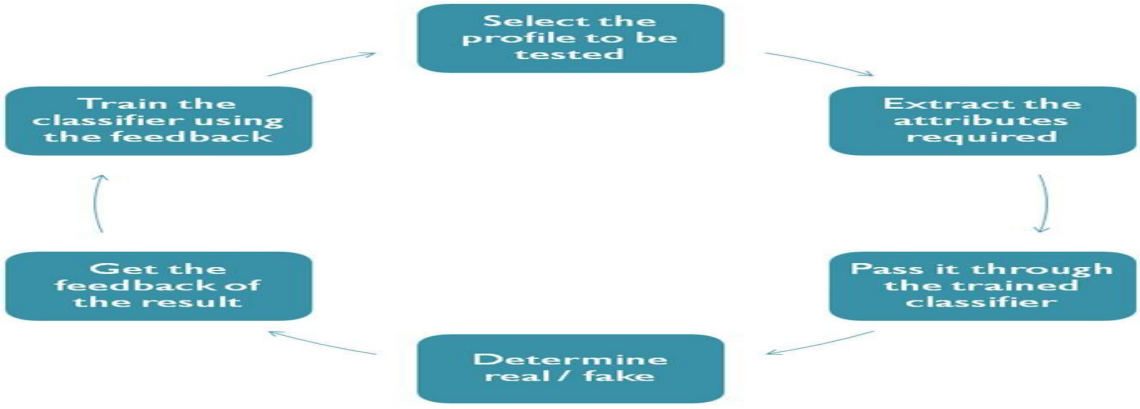


Figure 3.1: Framework for detection of fake profiles and learning

Classification

Classification is the process of learning a target function f that maps each records, x consisting of set of attributes to one of the predefined class labels, y. A classification technique is a approach of building classification models from an input data set. This technique uses a learning algorithm to identify a model that best fits the relationship between the attribute set and class label of the training set. The model generated by the learning algorithm should both t the input data correctly and correctly predict the class labels of the test set with as high accuracy as possible. The key objective of the learning algorithm is to build the model with good

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

generality capability.

The classifiers that we have implemented for classifying the profiles are:

Naive Bayes Classification Decision

Tree classification

Support Vector Machine

All these algorithms are the standard algorithm and is widely used in problems such as detecting spam email messages, categorizing cells as malignant or benign based upon the results of MRI scans, classifying galaxies based upon their shapes etc.

Naive Bayes Classification

In Bayesian classification we have a hypothesis that the given data belongs to a particular class. We then calculate 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. Also, if at some stage additional training data is added then each training example can incrementally increase or decrease the probability that the hypothesis is correct.

Decision Tree

A decision tree is a popular classification method that generates tree structure where each node denotes a test on an attribute value and each branch represents an outcome of the test. The tree leaves represent the classes. The figure 3.3 shows the decision tree evaluated from our training dataset used in the project. It displays the relationships found in the training dataset. This technique is fast unless the training data is verylarge. It does not make any assumptions about the probability distribution of the attributes value. The process of building the tree is called induction.

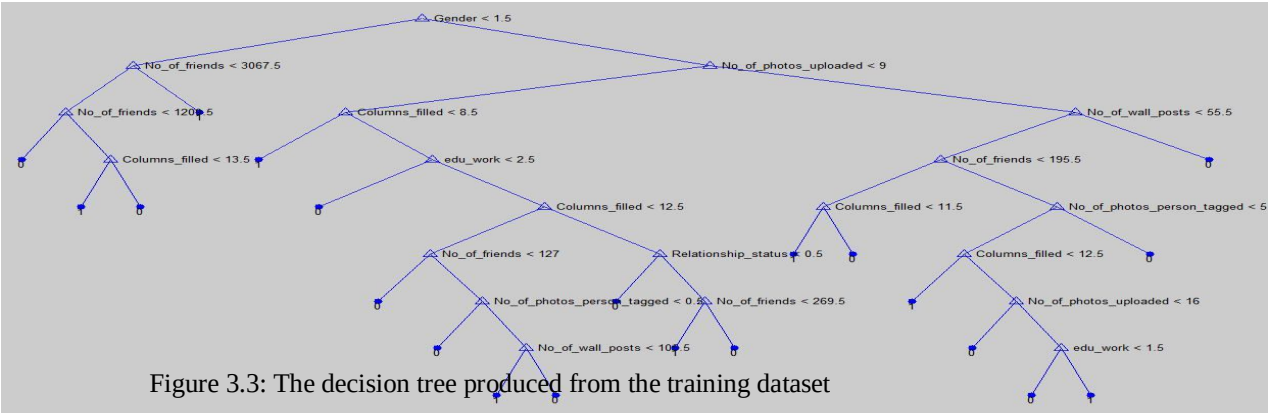


Figure 3.3: The decision tree produced from the training dataset

Building a decision tree

The decision tree algorithm is a top-down greedy algorithm which aims to build a tree that has leaves as homogenous as possible. The major step in the algorithm is to continue dividing leaves that are not

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

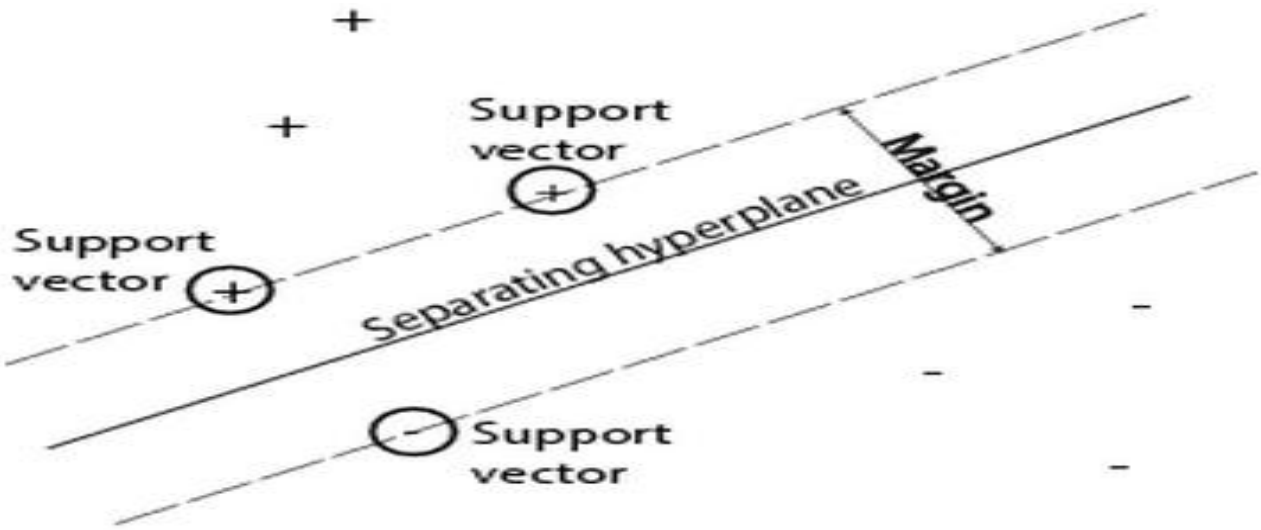
homogeneous into leaves that are as homogeneous as possible until no further division is possible. The algorithm is described below:

1. If some of the attributes are continuous-valued, they should be discredited into categories.
2. If all instances in training dataset are in the same class, then stop.
3. Split the next node by selecting an attribute from the independent attributes that best divides the objects in the node into subsets and create decision tree node.
4. Split the node according to the value of attribute selected in step 3
5. Stop if any of the following conditions meets, otherwise continue step 3:
   (a) If this partition divides the data into subsets that belong to a single class and no more node needs splitting
   (b) If there are no remaining attributes for further division.

Support Vector Machine

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 thoseof the other class. The support vectors are the data points that are closest to the separating hyper plane. The figure 3.4 illustrates linear classification, with + indicating data points of type 1, and indicating data points of type 0.

The datasets that we have used cannot be classified using linear classifier. So, non-linear classifier with Gaussian kernel is used. The implementation of SVM is done on Mat lab.



 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Implementation and Results

Datasets needed

We need dataset with a mixture of real and fake profiles labeled accordingly. The algorithms need to be trained using the training dataset and should be evaluated using the testing dataset. But there are no such datasets available because of privacy issues. As there is no standard dataset present, we need to prepare the dataset by scrapping the profiles from face book. To scrap the data from the profiles, we need to be friends with the profiles which are being scrapped. We may use the profile face book friends to scrap the real profiles.

Scrapping data

Scripts written in python language will be used which logs into face book automatically and scraps required data. Face book Graph API is also used along with python to extract some required data. Anti scrap detection techniques may be implemented to prevent face book immune system from detecting.

Barracuda labs is presently working on face book spam detection making applications for them. They detected and scrapped fake profiles and analyzed the data. We may collect the data from them, altered the profiles in which data is hidden, leaving fake profiles in the dataset.

Attributes that we may consider

No. of friends

Education and work Gender

No. of columns filled in about me Relationship

status

No. of photos of the person tagged

No. of wall posts posted by the person

No. of photos uploaded by the person

Some other attributes which can be used in these classification algorithms are :

Ratio of same gender friends and total friends.

Ratio of the no. of friend requests sent and accepted

No. of groups

No. of likes, etc.

Evaluation parameters

$$\text{Efficiency} = \frac{\text{No. of correct predictions}}{\text{Total No. of Predictions}}$$

$$\text{False Positive rate} = \frac{\text{No. of real profiles detected as fake}}{\text{Total No. of fake profiles to be detected}}$$

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

$$\text{False Negative rate} = \frac{\text{No. of fake profiles detected as real}}{\text{Total No. of real profiles}}$$

Results

From the graph we will find that the efficiency of the SVM is highest when the data is well trained and the efficiency of the Nave Bayes is lowest which don't change much when the training dataset increases. As the no. of attributes increases for the training dataset the efficiency of all the algorithms increases. The false positive rate of the SVM is least that means if a profile is detected fake then the chance of being fake is very high in SVM whereas Nave Bayes shows high false positive rate. The false negative rate on the other hand is very low for Naive Bayes and the SVM has average false negative rate is the algorithm is well trained. So, from the results we find that SVM is well suited for classification of the fake profiles in the social networks.

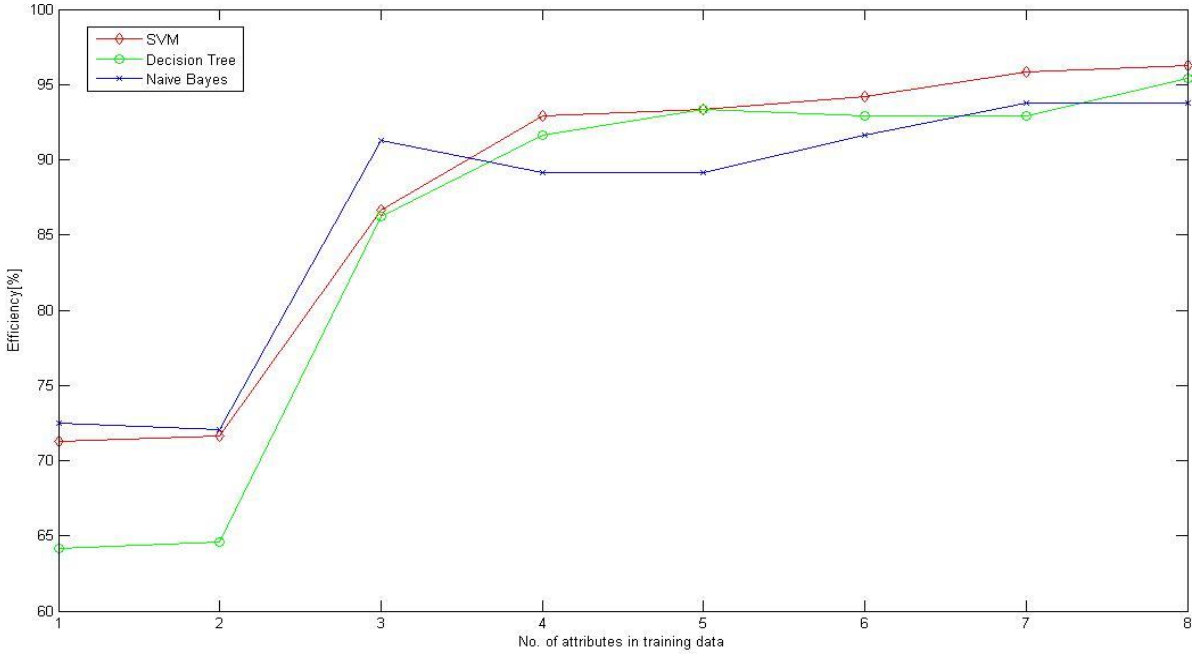
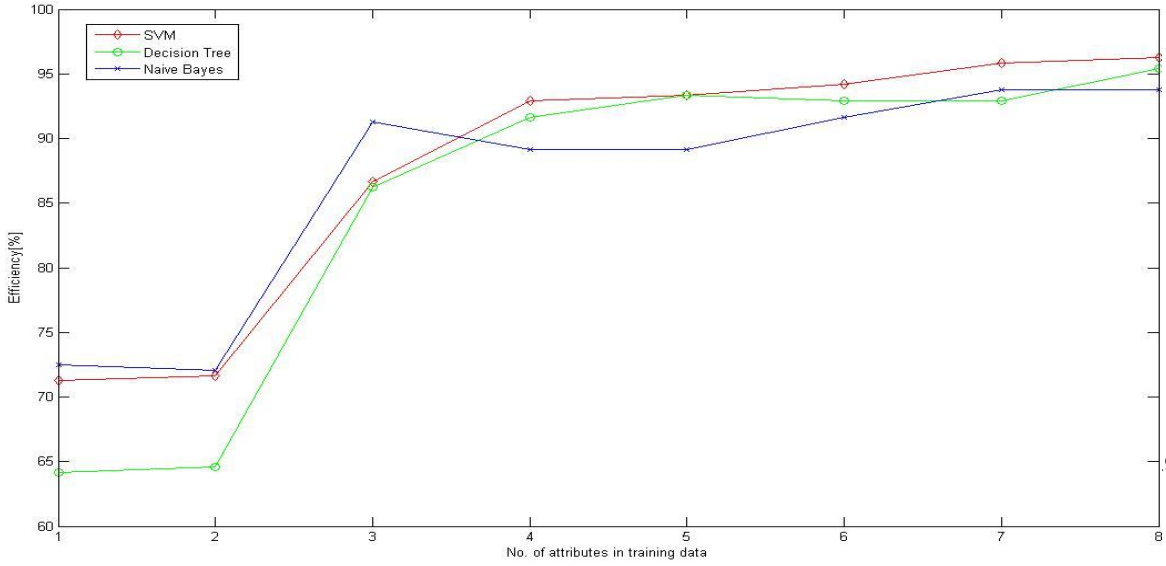


Figure 4.1: Efficiency vs. No. of profiles in training dataset



ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Figure 4.2: Efficiency vs. No. of attributes considered in a profile

Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

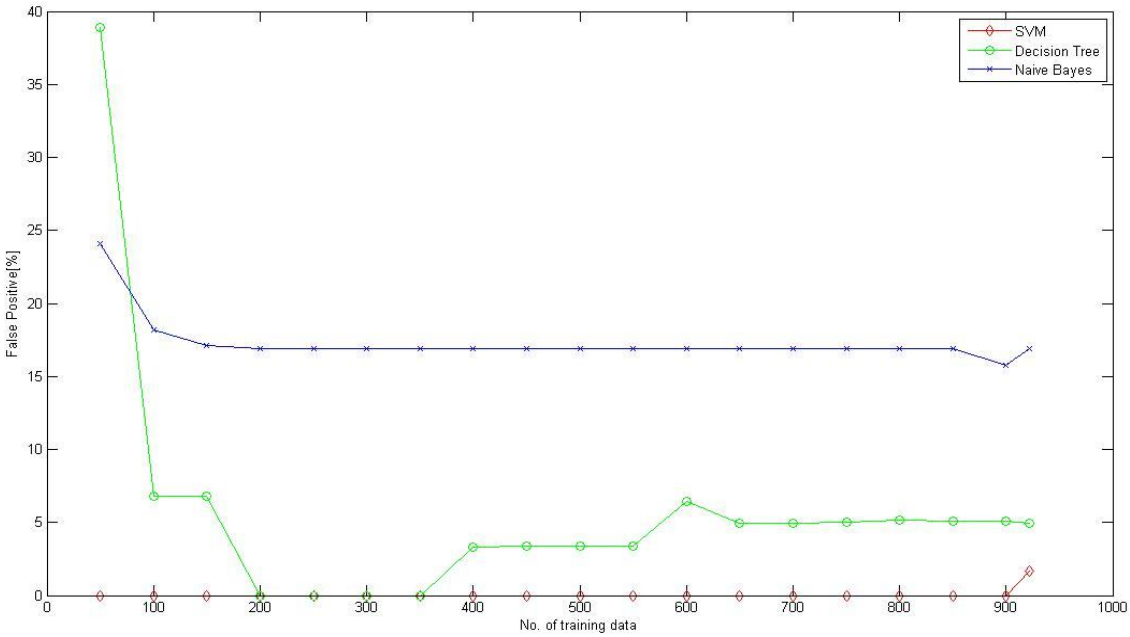


Figure 4.3: False Positive vs. No. of profiles in training dataset

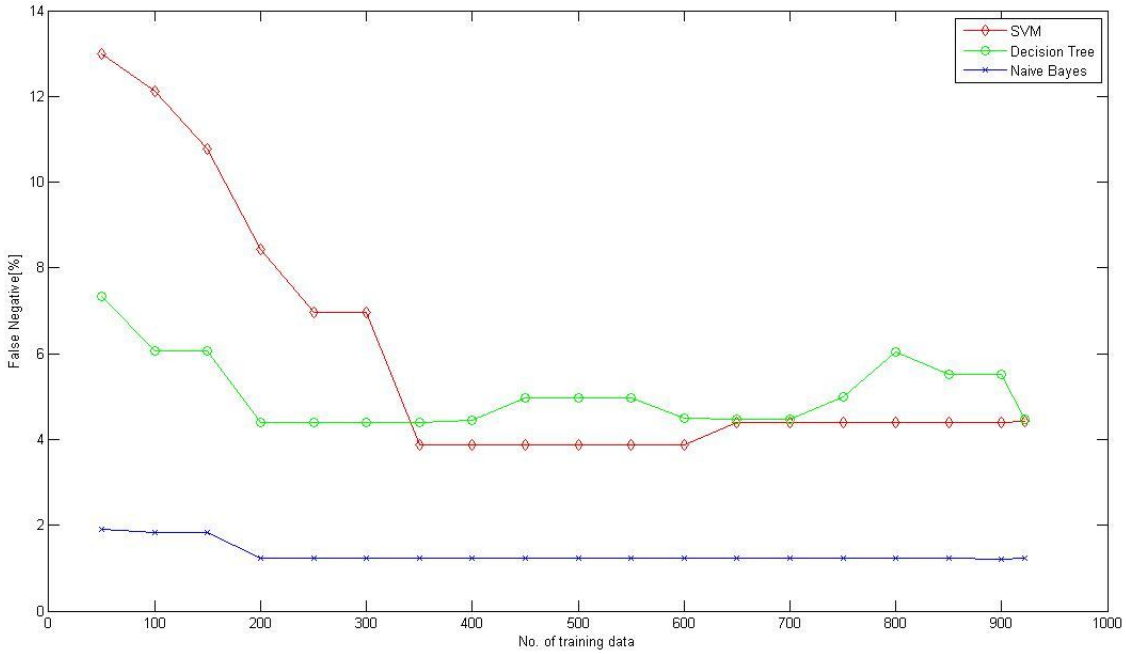


Figure 4.4: False Negative vs. No. of profiles in training dataset

Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

Conclusion and Future Work

We will have given a framework using which we can detect fake profiles in any online social network with a very high efficiency as high as around 95% as targeted. Fake profile detection can be improved by applying NLP techniques to process the posts and the profile

Bibliography

[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 and 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] RajanChattamvelli. 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.

 Copyright ⓒ 2019Authors

ISSN:0971-1260

Vol-22-Issue-4-October-December-2019

[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.

[16] http://ethesis.nitrkl.ac.in/3578/1/thesis.pdf

[17] http://oaijse.com/VolumeArticles/FullTextPDF/188_14.AUTOMATIC_DETECTION_OF_FAKE_PROFILES_IN_ONLINE_SOCIAL_NETWORKS.pdf

[18] https://www.ijcseonline.org/pdf_paper_view.php?paper_id=4717&7-IJCSE-07555.pdf

[19] https://www.ripublication.com/ijaer18/ijaerv13n6_133.pdf

[20] https://pdfs.semanticscholar.org/e5e6/a7e9f8a05cbccb78c5d188de60404b865f9c.pdf

Copyright ⓒ 2019Authors