IMPROVED MODEL FOR DETECTING FAKE PROFILES IN ONLINE SOCIAL NETWORK: A CASE STUDY OF TWITTER

Adebola K. Ojo
Department of Computer Science,
University of Ibadan, Nigeria
adebola_ojo@yahoo.co.uk

ABSTRACT

Online Social Network (OSN) is like a virtual community where people build social networks and relations with one another. The open access to the Internet has increased the growth of OSN which has attracted intruders to exploit the weaknesses of the Internet and OSN to their own gain. The rise in the usage of OSN has posed security threats to OSN users as they share personal and sensitive information online which could be exploited by these intruders by creating profiles to carry out a series of malicious activities on the social network. In fact, it is no gain saying that the intent of creating fake accounts has adverse effect and the Internet has made it quite easy to concede one's identity; and this makes it difficult to detect fake accounts as they try to imitate real accounts. In this study, a model that can accurately identify fake profiles in OSN which uses Natural Language Processing Technique to eliminate or reduce the size of the dataset thereby improving the overall performance of the model was proposed. Principal Component Analysis was used for appropriate feature selection. After extraction, six attributes/features that influenced the classifier were found. Support Vector Machine (SVM), Naïve Bayes and Improved Support Vector Machine (ISVM) were used as Classifiers. ISVM introduced a penalty parameter to the standard SVM objective function to reduce the inequality constraints between the slack variables. This gave a better result of 90% than the SVM and Naïve Bayes which gave 77.4% and 77.3% respectively.

Keywords: *Online Social Network, Natural Language Processing, Principal Component Analysis, Support Vector Machine, Improved Support Vector Machine*

INTRODUCTION

A Social Network is best viewed as a graphical structure with nodes and edges depicting the users and their interaction activities respectively. The nodes and edges in a Social Network graph can be labeled or unlabeled depending upon the structure of the network being used (Pulluri, S.R., Gyani, J., & Gugulothu, N., 2017). OSN is an online platform which people use to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections (Mauro Coletto and Claudio Lucchese, 2017). In a more concise or technical way, OSN is a social structure made of individuals (or organizations) that can be called as "nodes", and the links are the different types of relationships/interdependency, such as friendship, or common interest, established between nodes that are all connected over electronic means, mainly Internet (IGI Global, 2019). People are highly dependent on OSNs which have attracted the interest of cyber criminals for carrying out a number of malicious activities. An entire industry of black-market services has emerged which offers fake account-based services for sale (Gupta, Aditi & Kaushal, Rishabh., 2017). The extensive usage of the OSN has led to the dissemination of massive amount of personal and sensitive information which could be used maliciously by intruders and scammers and put the users at risk. The intent of creating fake accounts has adverse effect and the Internet has made it quite easy to hide one's identity which makes it difficult to detect these accounts without appropriate research. The challenges posed by fake profiles cannot be underestimated as it could lead to emotional and financial risk which could escalate to something more. Significant features that help to detect fake profiles by influencing the classifiers were also detected. It helps OSN providers to curb or minimize the creation of fake profiles which impose threats to the users in OSN. To a large extent, OSN users' data or information is secured from manipulators. Generally, it improves the trust level of users, which in turn makes OSN community more secured for user interaction and better communication. This work aims at dealing with the problem of detecting fake profiles in Online Social Network and to develop a model that can accurately identify fake profiles in Online Social Network with Supervised Machine Learning Techniques using Improved Support Vector Machine. It is geared towards distinctly and accurately detecting fake profiles in OSN using the proposed model (ISVM) by extracting appropriate features that can accurately differentiate fake and real profiles, building a model to identify fake profiles, experimenting the proposed model and comparing it with different models as well as evaluating the performance of the model with the existing ones.

LITERATURE REVIEW

Twitter is currently one of the largest OSN platforms, with 313 million monthly active users (Konstantinos Konstantinidis, Symeon Papadopoulos, Yiannis Kompatsiaris, 2017). Research also records about 4.4 billion Internet users and there are about 3.4 billion active social media accounts (Smith, 2019). It also stated that the average time spent on social media is about 116 minutes a day, which evidently shows that a lot of people live on social media. The term/word fake means a thing that is not genuine, something that is not what it appears to be or an imitation. Identity is an object attached to a human being, separate from him or her (Romanov, A., Semenov, A., Mazhelis, O. and Veijalainen, J., 2017). A fake profile is a form of an identity theft of a user to disguise or imitate a real user for several malicious reasons. Fake Profiles range from spammers/bot accounts to profile cloning or black-market users. Fake accounts are categorized into what Facebook calls as duplicate accounts and false accounts. A duplicate account refers to an account maintained by a user in addition to his/her principal account. False accounts are further broken down into two categories user-misclassified accounts and undesirable accounts. User-misclassified accounts represent the personal profiles created by users for a business, organization, or non-human entity such as a pet. On the other hand, undesirable accounts are the user profiles that are intended to be used for purposes that violate Facebook terms of service, such as spamming (Gupta, Aditi & Kaushal, Rishabh., 2017).Fake identities in social media are often used in APT cases, both to gather intelligence prior the attack, and to establish trust and deliver malware or a link to it. Such fake identities are also used in other types of malicious activities (Romanov, A., Semenov, A., Mazhelis, O., & Veijalainen, J., 2017).

Social Media has impact on politics, commerce, training and development, society, personal relationships and interactions which have both good and adverse effects on OSN users. Because of their scale, complexity, and heterogeneity, many technical and social challenges in online social networks must be addressed. It has been widely recognized that security and privacy are the critical issues in online social networks (Xiang, Yang, Bertino, E, Kutylowski, M., 2017). Figure 1 shows elements of social media while Figure 2 shows social media classification based on information half-life and depth, and associated marketing objectives and purposes.

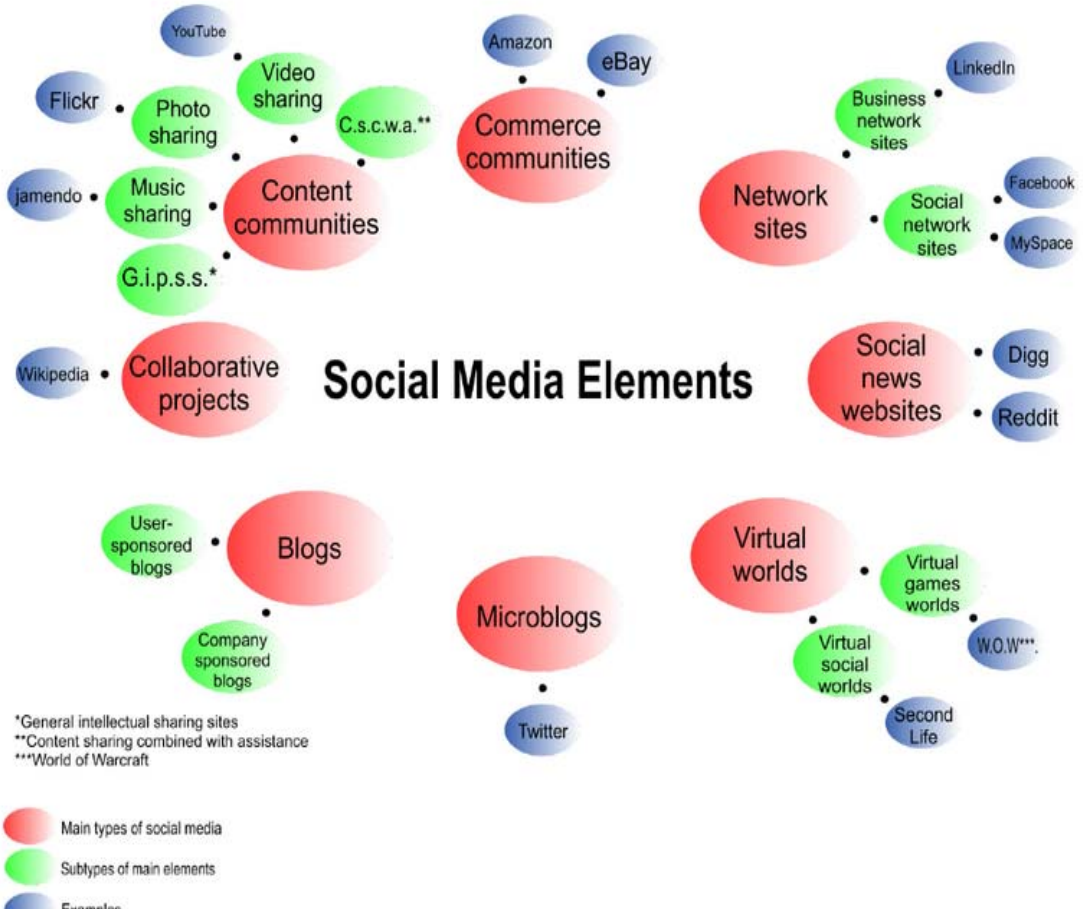

Figure 1: Social Media Elements (Gáti, Mirkó & Csordás, Tamás & Markos-Kujbus, Eva., 2014)

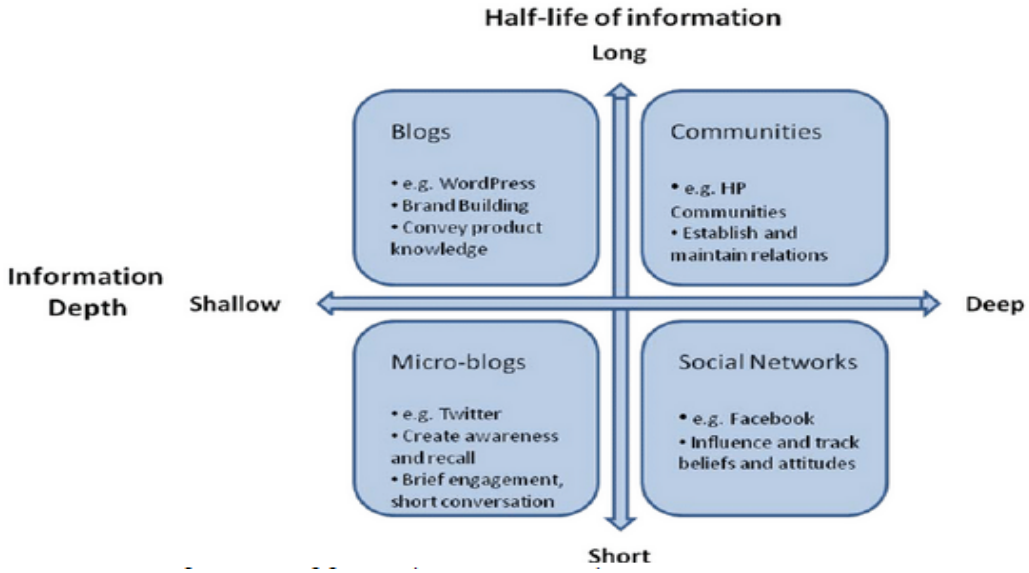

Figure 2:Social Media Classification by half-life and depth, and associated marketing objectives and purposes *(Weinberg, B.D., Pehlivan, E., 2011)*

Some algorithms for feature selection include Artificial Bee Colony (ABC), Ant Colony Optimization (ACO) Algorithm, Principal Component Analysis, Linear Discriminant Analysis (LDA), Autoencoders, Independent Component Analysis (ICA) and Probabilistic Principal Component Analysis (PPCA), (Nasreen, 2014) (Wani, S.Y., Ansarullah, S.I., & Kirmani, M., 2016). Furthermore, there are some approaches to detecting fake profiles in OSN; these include Supervised Methods, Unsupervised methods and Semi- Supervised methods (Ravneet Kaur and Sarbjeet Singh, 2016). Some approaches for OSN classifications are Support Vector Machine (SVM) (Mohammadreza Mohammadrezaei, Mohammad Ebrahim Shiri and Amir Masoud Rahmani, 2018), Graph Structure Technique for Classification (Kaur, Ravneet & Singh, Sarbjeet., 2016), (Mohammadreza Mohammadrezaei, Mohammad Ebrahim Shiri and Amir Masoud Rahmani, 2018), Artificial Neural Network (ANN) (Adikari, 2014) (Wani, Suheel Yousuf & Kirmani, Mudasir & Ansarullah, Syed., 2016), Decision Tree (DT) (Suheel Yousuf, WaniMudasir Kirmani and Syed Immamul Ansarullah, 2016) and Naïve Bayes (NB) (Kaur, Ravneet & Singh, Sarbjeet., 2016). (Kumar, A., Sangwan, S. R., & Nayyar, A., 2019)

RELATED WORKS

Some related works to this study are discussed as follows:

- **Identifying Fake Profiles in LinkedIn**: (Adikari, 2014) focused on differentiating legitimate and fake profiles rather than just identifying profile cloning, spam information distribution, and intrusion detection. They used LinkedIn as the basis for their study. The main limitation in this work was the verification of the sources and the published fake profiles. It is identified that when a cloning attack occurs on certain profiles, the system cannot actually identify which is fake.
- **Prediction of Fake Profiles on Facebook using Supervised Machine Learning Techniques-A Theoretical Model**: In (Wani, Suheel Yousuf & Kirmani, Mudasir & Ansarullah, Syed., 2016), a novel approach was proposed for the prediction of fake profiles on Facebook using supervised machine learning algorithms. The proposed model applied sophisticated noise removal and data normalization techniques on datasets before analyzing them. A technique was 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). Four machine learning techniques (SVM, ANN, NB, and DT) were used as the classifiers. It was concluded that a combination of two or more machine learning algorithms can be used for detection of fake as well as genuine profiles on Facebook. The prediction was based on the majority voting of the ensemble classifiers (SVM, ANN, NB, and DT).

- **Towards detecting fake user accounts in Facebook.** (Gupta, Aditi & Kaushal, Rishabh., 2017)**:** This study focused on characterizing and detecting fake accounts on Facebook. The first step in their approach was data collection. Facebook real user and fake user ground truth was captured. Their result indicated that many fake users are classified as real suggesting clearly that fake accounts are mimicking real user behavior to evade detection mechanisms. PCA would have done a great job in shortlisting the important features to be considered that will accurately distinguish real user accounts from fake user accounts.
- **Automatic detection of fake profiles in online social Networks.** (Sumit Milind Kulkarni, Prof. Vidya Dhamdhere, 2018)(Sumit Milind Kulkarni & Prof. Vidya Dhamdhere, 2018): The detection process of this model started with feature selection which selected suitable attributes on which the classification algorithm was implemented. After which the extracted attributes were passed into the trained classifier. The Classifier was said to be trained regularly as the feedbacks of the results were being fed into the classifier as new training data for better accuracy.
- **Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms.** (Mohammadreza Mohammadrezaei, Mohammad Ebrahim Shiri and Amir Masoud Rahmani, 2018): This paper improved the efficiency of detecting fake accounts on social networks by using the definition of similarity measures in order to use the strength of relationship among account's friends, and by using feature extraction methods to prevent the overfitting problem and to create a balance in the dataset by using resampling methods. The method proposed here used similarity matrices between accounts which were calculated according to the graph adjacent matrix. The limitation of this model was that for the proposed model to work, fake accounts must work in the network so that it will be possible to recognize them as legitimate or fake ones, by analyzing their friend's networks.
- **A comprehensive model for detecting fake profiles in online social networks.** (Srinivas Rao Pulluri, Jayadev Gyani, Narsimha Gugulothu, 2017): The main work done here was to identify, and separate the real profiles and false profiles in Facebook. In this work a model was proposed for resolving legal profiles and false profiles in Facebook. The learning algorithm used in this paper was not stated but the evaluation parameters used were True Positive Rate (TPR), False Positive Rate (FPR) and Area under ROC Curve (AUC) to determine legitimate and malicious users.

This study used improved Support Vector Machine and Naive Bayes algorithms for improved efficiency in accurately identifying or differentiating fake profiles in Online Social Network. (Alzubi, J., Nayyar, A., & Kumar, A., 2018)

METHODOLOGY

Various methods have been proposed regarding how to detect fake profiles in OSN. For the purpose of this work, there are five major steps to achieve the main aim to identify fake profile in online social network: Data Collection, NLP Pre-processing technique, Dimensional Reduction technique using PCA for feature extraction, Profile Classification using SVM and NAÏVE BAYES and Evaluation. This proposed methodology is presented in Figure 3.

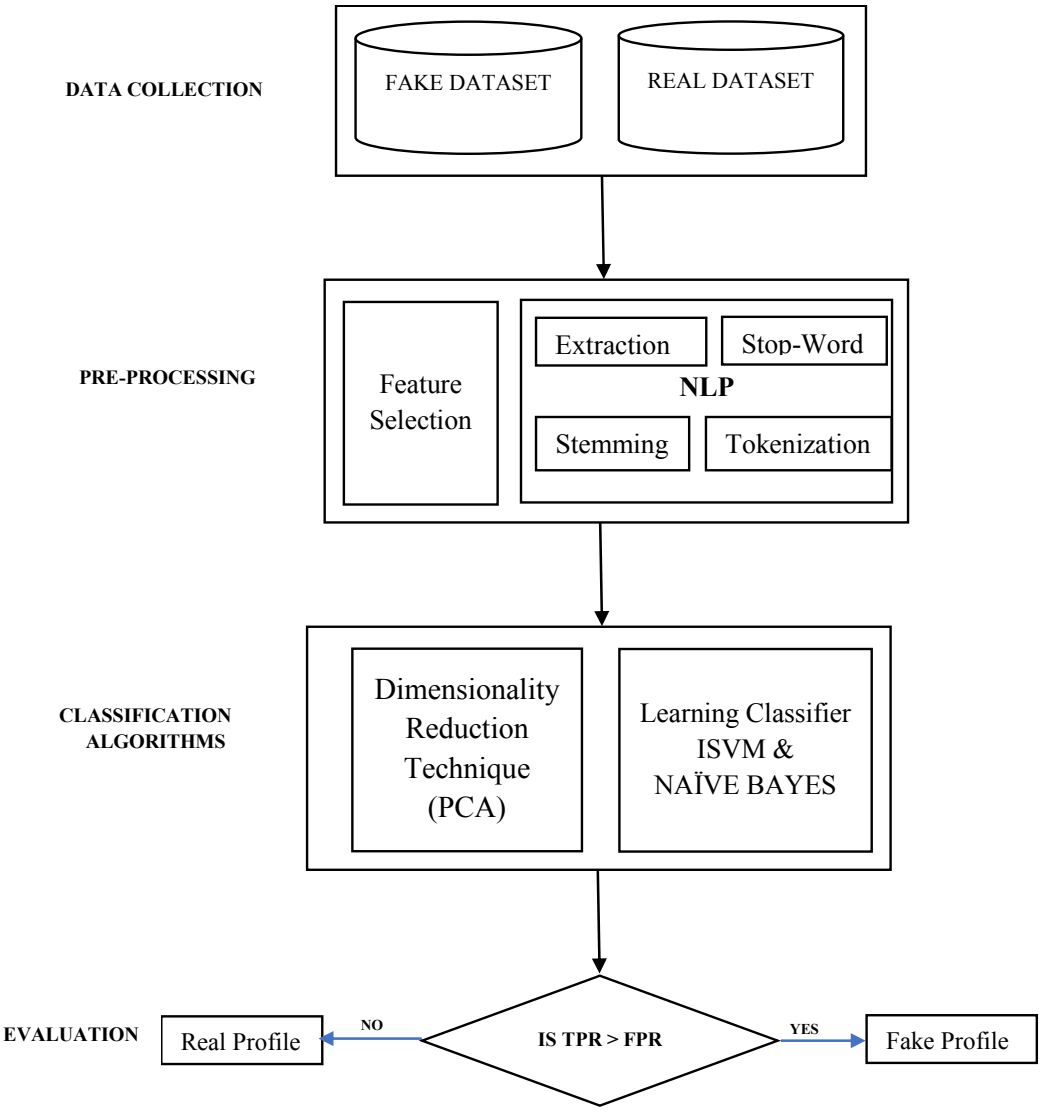

Figure 3: Proposed Methodology

DATA COLLECTION: This is the first step and one of the most important steps. It is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes. In this work, data was collected for both fake and real profiles.

FEATURE EXTRACTION: Prominent features that were perceived to accurately identify or differentiate fake profiles and real profiles were collated to be considered as a measure.

NATURAL LANGUAGE PROCESSING (NLP) PRE-PROCESSING TECHNIQUE: This is an important task and crucial step that can either improve the overall performance if done properly. This is done to reduce the size of the data set which invariably increases efficiency and effectiveness of the system. The four NLP pre-processing techniques which were adopted in this study were Extraction, Stop-Word Elimination, Stemming and Tokenization.

DIMENSIONAL REDUCTION TECHNIQUE USING PCA: As data generation and collection keep increasing, visualizing it and drawing inferences become more and more challenging. It is better to select variables that captures as much information as the original set of variables. A principal component is a normalized linear combination of the original predictors *p*in a data set. For a data set of dimensions (n) × (p). n represents the number of observations, p represents number of predictors and X^1, X^2...,X^p represent a set of predictors. The principal component can be written as

$$Z^1 = \Phi^{11}X^1 + \Phi^{21}X^2 + \Phi^{31}X^3 + ... + \Phi^{p1}X^p \quad (1)$$

Where,

- Z^1 is the first principal component.
- $\Phi^{11}X^1$is the loading vector comprising of loadings (Φ^1, Φ^2 …) of first principal component. The loadings are constrained to a sum of square equals to 1. This is because large magnitude of loadings may lead to large variance. It also defines the direction of the principal component (Z^1), which data varies the most. It results in a line in p dimensional space which is closest to the n observations. Closeness is measured using average squared Euclidean distance.
- $X^1...X^p$ are normalized predictors. Normalized predictors have mean equals to zero and standard deviation equals to one.

Principal Component Analysis (PCA*)* is a method of extracting important variables (in form of components) from a large set of variables available in a data set. It extracts low dimensional set of features from a high dimensional data set with a motive to capture as much information as possible. With fewer variables, visualization also becomes much more meaningful. PCA is more useful when dealing with 3 or higher dimensional data. It is a technique which helps us in extracting a new set of variables which are called Principal Components. A principal component is a normalized linear combination of the original predictors in a data set.

First principal component is a linear combination of original variables which captures the maximum variance in the data set. It determines the direction of highest variability in the data. The larger the variability captured in first component, the larger the information captured by component. No other component can have variability higher than first principal component.

Second principal component(Z^2) is also a linear combination of original predictors which captures the remaining variance in the data set and is uncorrelated with Z^1. In other words, the correlation between first and second component is zero. It can be represented as

$$\mathbf{Z^2 = \Phi^{12}X^1 + \Phi^{22}X^2 + \Phi^{32}X^3 + ... + \Phi^{p2}X^p} \quad (2)$$

Invariably, **second principal component** tries to explain the remaining variance in the dataset and is uncorrelated to the first principal component. **All succeeding principal component** follows a similar concept i.e. they capture the remaining variation without being correlated with the previous component. In general, for $n \times p$ dimensional data, min ($n-1$, p) principal component can be constructed. The directions of these components are identified in an unsupervised way i.e. the response variable(Y) is not used to determine the component direction. Therefore, it is an unsupervised approach. After calculating the principal components on training set, then testing data is predicted on using these components. PCA components on training set is obtained, followed by a bunch of components on testing set. Finally, the model was trained.

PROFILE CLASSIFICATION USING ISVM AND NAÏVE BAYES.

A Support Vector Machine (SVM) is a discriminative classifier formally defined by a separating hyperplane. In other words, given labeled training data (*supervised learning*), the algorithm outputs an optimal hyperplane which categorizes new examples.

A Naïve Bayes classifier is a simple probabilistic classifier based on Bayes' theorem and is particularly suited when the dimensionality of the inputs is high. The goal of the classifier is to determine the probability of features occurring in each class, and to return the most likely class given a set of features x_i through x_n and classes c_i through c_n. So, for each class, the classifier calculates $P(c_i| x_i, \ldots, x_n)$. Bayes Rule states that

$$P(A\backslash B) = \frac{P(B\backslash A)P(A)}{P(B)} \qquad (3)$$

Where

A = Class c_i
B = the set of features x_i through x_n
P(B) serves as normalization and could be ignored. It could be stated that:
$P(c_i| x_i, \ldots, x_n) \alpha\ P(x_i \mid c_i) * P(x_1 \mid c_i) * \ldots * P(x_n \mid c_i)$.

The proposed technique focuses on combining SVM and Naïve Bayes Classifications to get better accuracy of the result. The following section describes the proposed methodology for combining the classifiers.

Improved Support Vector Machine (ISVM): It introduced a penalty parameter to the standard SVM objective function to reduce the inequality constraint between the slack variables. The slack variables help to relax our constraints in cases where we cannot find an appropriate hyperplane that separates the two classes precisely. Thus, the penalty Parameter C, effectively controls how much error one is willing to afford during classification. The larger the C, the lesser the amount of the error it takes and vice-versa.

$$\min \frac{1}{2} \parallel w \parallel^2 \qquad (4)$$

$$\min \frac{1}{2} \parallel X_\phi w \parallel^2 + C(\xi^+ + \xi^-) \qquad (5)$$

Here, equation 4 shows the objective function of the standard SVM while equation 5 shows the objective function of ISVM. Where: w= weight, C= penalty parameter, ξ^+= positive slack variable and ξ^-= negative slack variable

RESULTS AND FINDINGS

The dataset was collected from Kaggle- a kind of data repository center for data mining and twitter. The dataset contains records that spanned through 37 countries, with over one hundred and twenty thousand instances. Figure 4 (***See Appendix A***) shows an overview of the dataset with 34 attributes.

Figure 5 (***See Appendix A***) shows the features or attributes from the whole dataset before feature extraction using PCA. Figure 6 (***See Appendix A***) shows the optimal features that were selected to be able to influence the Classifiers using PCA. A total of six features was chosen, which are: List_count, friends_count, favourite_count, status_count, followers_count and language code. Table 1 shows the justification of the features selected to be able to distinguish fake profiles from real profiles.

Table 1: Description and Justification of the Six Optimal Features Selected

Features	Feature Description	Justification
Followers_Count	The number of followers this account or user has	Fake accounts are expected to have no or low number of followers as compared to their friends_count
Statuses_count	The number of tweets (including retweets) issued by the user to date.	Fake accounts are expected to post and share spam messages.

Language_Code	The BCP 47 code for the user's self-declared user interface language.	Fake accounts tend to different language_codes on their interface.
Friends_Count	The number of users this account is following (also known as followings)	Fake accounts are expected to have a high number of followers in comparison to real users.
Favourite_Count	The number of tweets the user has favourited (liked) in the account's lifetime	Fake accounts are expected to have a high number of favourited (liked) tweets than real users.
Listed_Count	The number of public lists or groups that this user is a member of.	Fake accounts are expected to have a high number of groups compared to the number of followers they have.

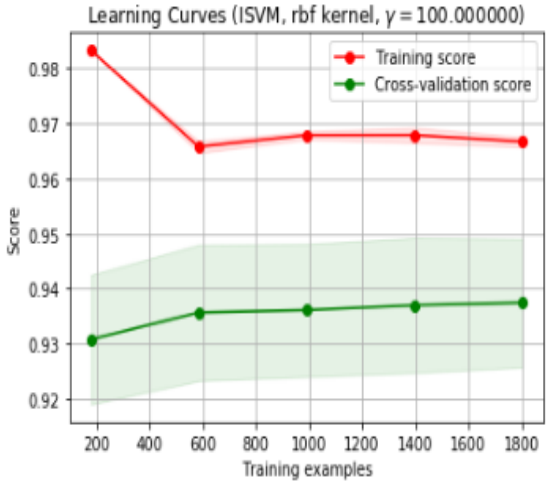

Figure 7: Training Phase of ISVM

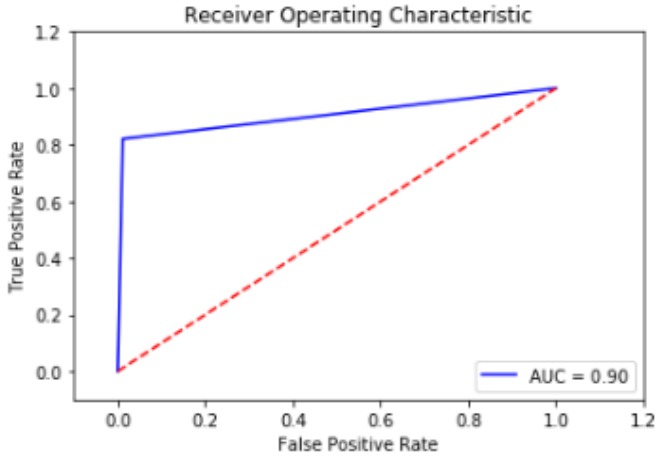

Figure 8: ROC Curve of ISVM

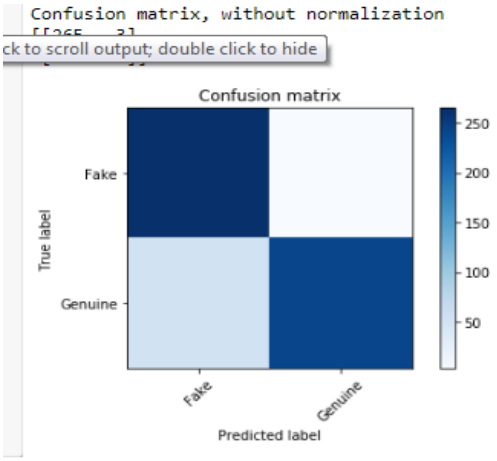

Figure 9: Confusion Matrix of ISVM

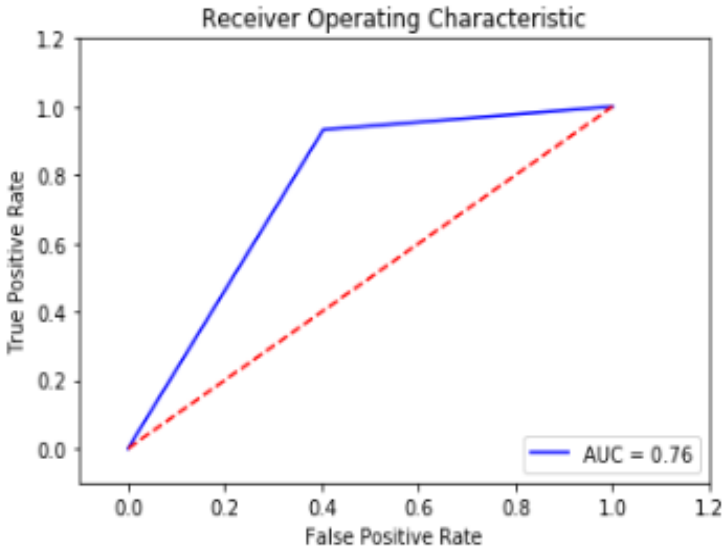

Figure 10: ROC Curve for Naïve Bayes

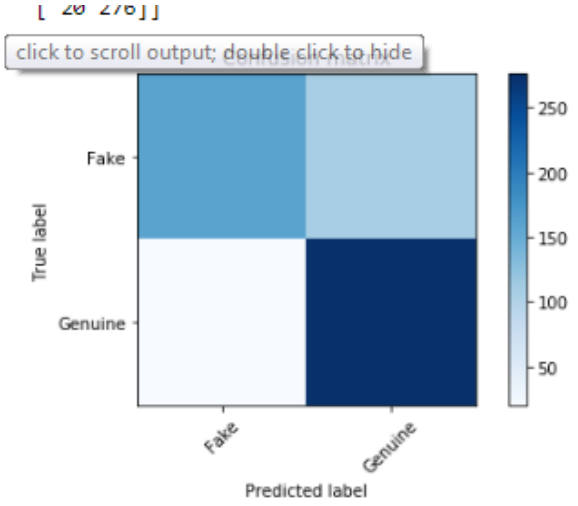

Figure 11: Confusion Matrix for Naïve Bayes

```
[44]: print ('Classification Accuracy on Test dataset: ' ,accuracy_score(y_test, prediction_SVM))

Classification Accuracy on Test dataset:  0.774822695035
```

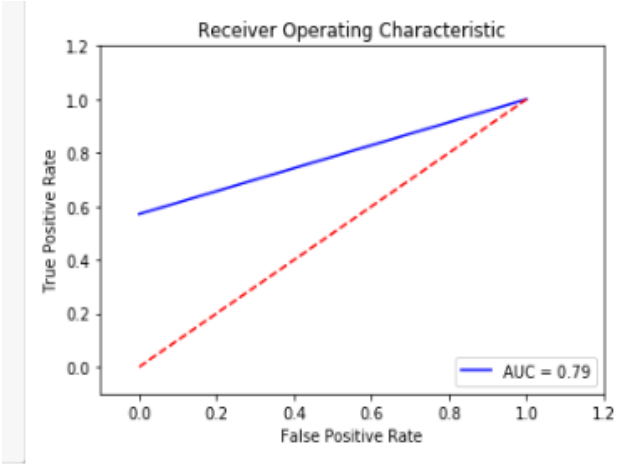

Figure 12: ROC Curve for SVM

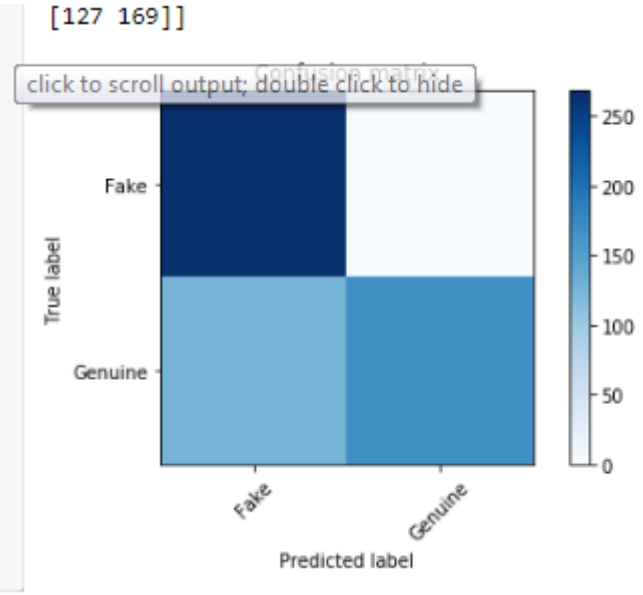

Figure 13: Confusion Matrix for SVM

The model's performance was evaluated based on the classification accuracy and on the following figures of merit:

a) **True Negative (TN):** Case was negative and was predicted negative.
b) **True Positive (TP):** Case was positive and was predicted positive.
c) **False Negative (FN):** Case was positive but was predicted negative.
d) **False Positive (TP):** Case negative but was predicted positive.
e) **Mean Accuracy:** This is the proportion of the number of correct trials to the number of trials of the system or the percentage of correctly classified instances.

$$\text{Mean Accuracy} = \frac{\text{True Positive} + \text{True Negative}}{\text{True Positive} + \text{False Positive} + \text{False Negative} + \text{True Negative}}$$

f) **Confusion matrix:** gives a matrix as output and describes the complete performance of the model.
g) **Recall:** This is the proportion of the number of correct trials of the system to the total number of a specific input label.

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}}$$

h) **Precision:** Proportion of the number of correct trials of the system to the total number of a specific output label.

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

i) F1- Score: This is a measure of our test accuracy and is simply referred to harmonic mean such that the best score is 1.0 and the worst score is 0.0

Table 2: Classification accuracy of the three models, SVM, ISVM and NB

	SVM	**Naïve Bayes**	**ISVM**
Accuracy	0.774	0.773	0.900

Table 2 presents the classification accuracy of the three models: SVM, ISVM and NB. It can be seen that ISVM shows the best accuracy with an accuracy of 90% while SVM and NB gave an accuracy of 77.4% and 77.3% respectively.

CONCLUSION AND FUTURE WORK

The security and privacy issue in OSN have posed a lot of threats to users of OSN and OSN providers which have got the attention of OSN Analysts to create a means or model to accurately detect fake profiles in Online Social Network. However, since most fake users try to imitate real users, it has made it difficult to be able to effectively detect fake accounts in OSN, hence this research was tailored to finding a more efficient way of detecting fake accounts in OSN. This study was carried out using datasets got from Twitter as a case study which spanned about 37 countries and contains over one hundred thousand records. The datasets were cleaned and pre-processed first for better efficiency of the classification models. PCA Algorithm was then applied on these well formatted and cleaned data for feature selection. The profiles were passed into the learning models, after which they were classified using the proposed classification algorithms. A classification accuracy of 90% was achieved and the result of the analysis was presented using the confusion matrix and the proposed model showed a significant and better performance as compared to other models used for comparison in this work. In this study, the features that mostly influence the Classification models in detecting fake profiles in OSN were learnt and identified; these are Followers_count, friends_count, statutes_count, language_code, listed_count and favourite_count. It can be concluded that the detection of fake accounts or profiles in OSN using Improved Support Vector Machine and PCA for feature selection yields a better result when detecting fake profiles in OSN. The proposed model performed quite well with an accuracy of 90%. However, the model might not work as efficient as this when deploying to other Online Social Network where profile characteristics do not have any influence to detecting fake profiles. Also, the model cannot detect fake profiles during the process of creation. In the future detecting fake profiles in OSN at creation time can be looked into.

ACKNOWLEDGEMENTS

The author would like to thank Ms Adetoun Opeyemi Adediran of Computer Science Department, University of Ibadan, Nigeria, for so kindly spending her invaluable time and contributions to make this work possible.

References

Adikari, S. (2014). IDENTIFYING FAKE PROFILES IN LINKEDIN. *PACIS 2014 Proceedings.* Retrieved from http://aisel.aisnet.org/pacis2014

Alzubi, J., Nayyar, A., & Kumar, A. (2018, November). Machine learning from theory to algorithms: an overview. *Journal of Physics: Conference Series, 1142*(1), 012012.

Gáti, Mirkó & Csordás, Tamás & Markos-Kujbus, Eva. (2014). The Attributes of Social Media as a Strategic Marketing Communication Tool. *Journalism and Mass Communication, 4*, 48-71.

Gupta, Aditi & Kaushal, Rishabh. (2017). Towards detecting fake user accounts in facebook. *2017 ISEA Asia Security and Privacy (ISEASP)*, (pp. 1-6). doi:10.1109/ISEASP.2017.7976996.

IGI Global. (2019). Retrieved from IGI GLobal Disseminator of Knowledge: https://www.igi-global.com/dictionary/constructing-community-higher-education-regardless/21064

Kaur, Ravneet & Singh, Sarbjeet. (2016). A comparative analysis of structural graph metrics to identify anomalies in online social networks. *Computers & Electrical Engineering*. doi: 57. 10.1016/j.compeleceng

Konstantinos Konstantinidis, Symeon Papadopoulos, Yiannis Kompatsiaris. (2017, February 20). Exploring Twitter communication dynamics with evolving community analysis. *PeerJ Computer Science*. doi:3:e107 https://doi.org/10.7717/peerj-cs.107

Kumar, A., Sangwan, S. R., & Nayyar, A. (2019). Multimedia Social Big Data: Mining. . *Multimedia Big Data Computing for IoT Applications* (pp. 289-321). Singapore: Springer.

Mauro Coletto and Claudio Lucchese. (2017). Social–Spatiotemporal Analysis of Topical and Polarized Communities in Online Social Networks. *Encyclopedia of Social Network Analysis and Mining*, 1-14. doi:https://doi.org/10.1007/978-1-4614-7163-9_110182-1

Mohammadreza Mohammadrezaei, Mohammad Ebrahim Shiri and Amir Masoud Rahmani. (2018). Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms. *Security and Communication Networks*, 1-8. doi:10.1155/2018/5923156.

Nasreen, S. (2014). A Survey Of Feature Selection And Feature Extraction Techniques . *In Machine Learning,SAI.*

Pulluri, S.R., Gyani, J., & Gugulothu, N. (2017). A Comprehensive Model for Detecting Fake Profiles in Online Social Networks. *International Journal of Advance Research in Science and Engineering, 6*(6), 385-394.

Ravneet Kaur and Sarbjeet Singh. (2016, July). A survey of data mining and social network analysis based anomaly detection techniques. *Egyptian Informatics Journal, 17*(2), 199-216.

Romanov, A., Semenov, A., Mazhelis, O. and Veijalainen, J. (2017). Detection of Fake Profiles in Social Media - Literature Review. *Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017)* (pp. 363-369). SCITEPRESS – Science and Technology Publications, Lda. doi:DOI: 10.5220/0006362103630369

Romanov, A., Semenov, A., Mazhelis, O., & Veijalainen, J. (2017). Detection of Fake Profiles in Social Media. . *In Proceedings of the 13th International Conference on Web Information Systems and Technologies* (pp. 363-369). SCITEPRESS – Science and Technology Publications. doi:10.5220/0006362103630369

Smith, K. (2019, June 13). *126 Amazing Social Media Statistics and Facts.* Retrieved from Brandwatch: https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/

Srinivas Rao Pulluri, Jayadev Gyani, Narsimha Gugulothu. (2017). A Comprehensive Model for Detecting Fake Profiles in Online Social Networks. *International Journal of Advance Research in Science and Engineering, 6*(6), 385-394.

Suheel Yousuf, WaniMudasir Kirmani and Syed Immamul Ansarullah. (2016). Prediction of Fake Profiles on Facebook using Supervised Machine Learning Techniques-A Theoretical Model. *International Journal of Computer Science and Information Technologies, 7*(4), 1735-1738.

Sumit Milind Kulkarni, Prof. Vidya Dhamdhere. (2018). AUTOMATIC DETECTION OF FAKE PROFILES IN ONLINE SOCIAL NETWORKS. *Open Access International Journal of Science and Engineering, 3*(1), 70-73.

Wani, S.Y., Ansarullah, S.I., & Kirmani, M. (2016). Prediction of Fake Profiles on Facebook using Supervised Machine Learning Techniques-A Theoretical Model. *International Journal of Computer Science and Information Technologies (IJCSIT), 7*(4), 1735-1738.

Wani, Suheel Yousuf & Kirmani, Mudasir & Ansarullah, Syed. (2016). Prediction of Fake Profiles on Facebook using Supervised Machine Learning Techniques-A Theoretical Model. *International Journal of Computer Science and Information Technologies, 7*(4), 1735-1738.

Weinberg, B.D., Pehlivan, E. (2011). Social Spending: Managing the Social Media Mix. *Business Horizons,, 54*(1), 275-282.

Xiang, Yang, Bertino, E, Kutylowski, M. (2017). Security and privacy in social networks. *Concurrency and Computation: Practice & Experience, 29*(7). doi:10.1002/cpe.4093

Appendix A

Out[8]:

	id	name	screen_name	statuses_count	followers_count	friends_count	favourites_count	listed_count	created_at	url	...
0	3610511	Davide Dellacasa	braddd	20370	5470	2385	145	52	Fri Apr 06 10:58:22 +0000 2007	http://braddd.tumblr.com	...
1	5656162	Simone Economo	eKoeS	3131	506	381	9	40	Mon Apr 30 15:08:42 +0000 2007	http://www.lineheight.net/	...
2	5682702	tacone	tacone_	4024	264	87	323	16	Tue May 01 11:53:40 +0000 2007	http://t.co/LKrI1dZE	...
3	6067292	alessaura	alesstar	40586	640	622	1118	32	Tue May 15 16:55:16 +0000 2007	http://alesstar.wordpress.com/	...
4	6015122	Angelo	PerDiletto	2016	62	64	13	0	Sun May 13 19:52:00 +0000 2007	http://www.flickr.com/per_diletto	...

5 rows × 34 columns

Figure 4 Overview of the Dataset

```
In [9]: x.columns

Out[9]: Index(['id', 'name', 'screen_name', 'statuses_count', 'followers_count',
               'friends_count', 'favourites_count', 'listed_count', 'created_at',
               'url', 'lang', 'time_zone', 'location', 'default_profile',
               'default_profile_image', 'geo_enabled', 'profile_image_url',
               'profile_banner_url', 'profile_use_background_image',
               'profile_background_image_url_https', 'profile_text_color',
               'profile_image_url_https', 'profile_sidebar_border_color',
               'profile_background_tile', 'profile_sidebar_fill_color',
               'profile_background_image_url', 'profile_background_color',
               'profile_link_color', 'utc_offset', 'protected', 'verified',
               'description', 'updated', 'dataset'],
              dtype='object')
```

Figure 5 Columns/ features before PCA

```
In [10]: print ("extracting featues.....\n")
         x=extract_features(x)
         print( x.columns)
         print (x.describe())

extracting featues.....

Index(['statuses_count', 'followers_count', 'friends_count',
       'favourites_count', 'listed_count', 'lang_code'],
      dtype='object')
       statuses_count  followers_count  friends_count  favourites_count  \
count     2818.000000      2818.000000    2818.000000       2818.000000
mean      1672.198368       371.105039     395.363023        234.541164
std       4884.669157      8022.631339     465.694322       1445.847248
min          0.000000         0.000000       0.000000          0.000000
25%         35.000000        17.000000     168.000000          0.000000
50%         77.000000        26.000000     306.000000          0.000000
75%       1087.750000       111.000000     519.000000         37.000000
max      79876.000000    408372.000000   12773.000000      44349.000000
```

Figure 6 Columns/ Features after PCA