Identifying Deceptive Profiles using MachineLearning

Dr. S. Sravan Kumar,
Associate Professor
M. Vishwanath
Asst Professor **Dept of EEE**
Sree Dattha Institute of Engineering and science

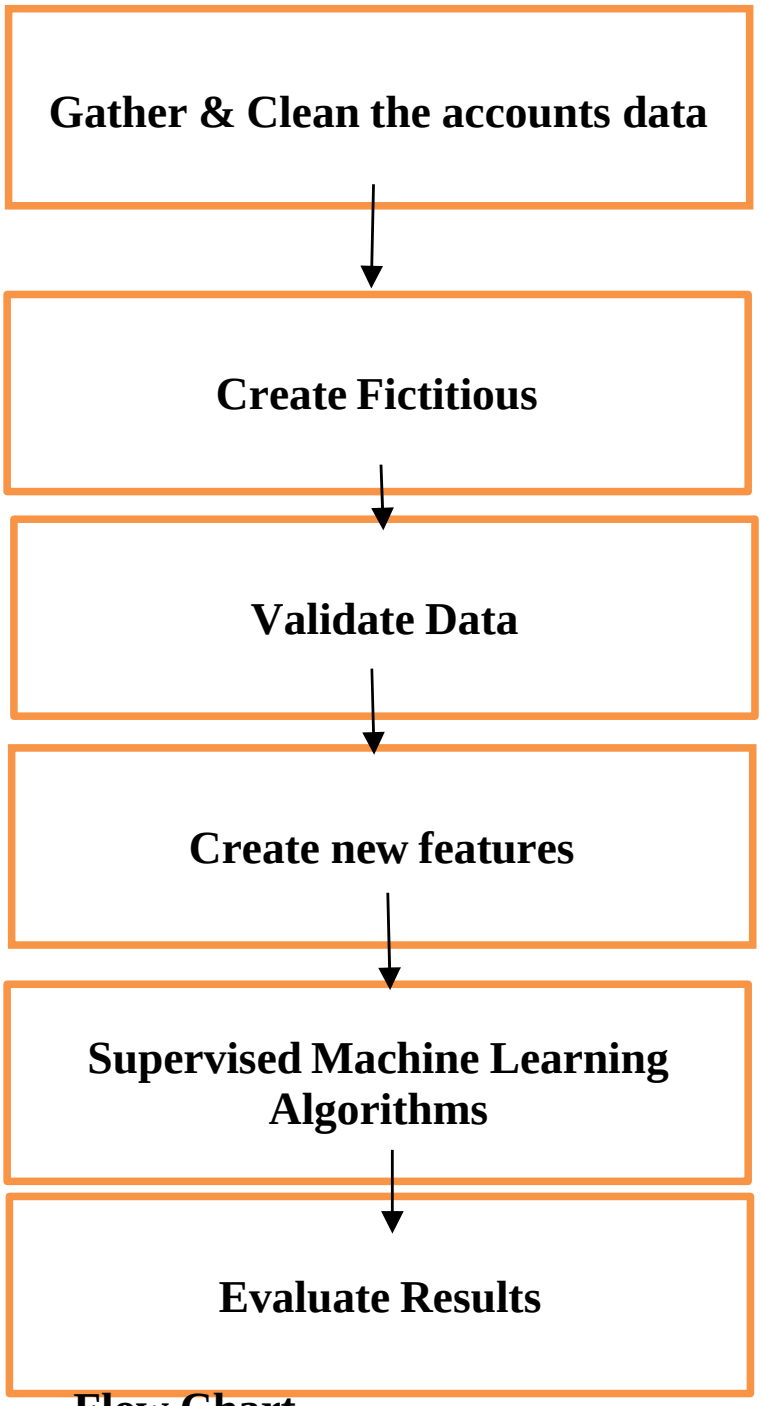
Abstract: Identity deception on big data platforms (like social media) is an increasing problem, due to the continued growth and exponential evolvement of these platforms. Social media is one of the preferred means of communication and has become a target for spammers and scammers alike, Cyber threats like spamming, which involves the sendingof unsolicited emails, are common in email applications. These same threats - and more - now emerge on social media. 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 andtheir updates has become easier. But with their rapid growth, many problems like deceptive profiles, online impersonation have also grown. There are no feasible solutions exist to control these problems. In this paper, I came up with a framework with which the automatic identification of deceptive profiles is possible and is efficient. This framework uses classification techniques like Random Forest Classifier, Support Vector Machine (SVM) & Neural Networks to classify the profiles into deceptive or genuine classes. As this is an automatic detection method, it can be applied easily by online social networksthat have millions of profiles whose profiles cannot be examined manually.

II. INTRODUCTION

Social media is growing incredibly fast these days. This is very important for marketing companies and celebrities who try to promote themselves by growing their base of followers and fans. The social networks are making our social lives better but there are a lot of issues which need to be addressed. The issues related to social networking likeprivacy, online bullying, misuse, and trolling etc. are most of the times used by fakeprofiles on social networking sites. However, fake profiles, created seemingly on behalf of organizations or people, can damage their reputations and decrease their numbers of likes and followers. On the other hand fake profile creation is considered to cause more harmthan any other formof cybercrime. This crime has to be detected even before the user is notified about the fake profile creation. In this very context figures this article, which is part of a series of research conducted by our team within the user profiling subject and profiles classification in social networks. Facebook is one of most famous online social networks. With Facebook, users can create user profile, add other users as friends, exchange messages, post status updates, photos, and share videos etc. Facebook website is becoming popular day by day and more and more people are creating user profiles on this site. Fake profiles are the profiles which are notgenuine i.e. they are the profiles of persons with false credentials.

II **METHODOLOGY**

The proposed system is equipped with various Machine Learning tasks and the architecture followed is as shown below. The proposed system collects the dataset which are pre-processed by providing a framework of algorithms using which we can detect fake profiles in Facebook by comparing the accuracy of three machine learning algorithms and the algorithm with very high efficiency is found for the given dataset.



Flow Chart

The different ways in which an algorithm can model a problem is based on its interaction with the experience or environment for the model preparation process that helps in choosing the most appropriate algorithm for the given input data in order to get the best result.

Support Vector Machine (SVM): Support-vector machines (SVMs, also support-vector networks) are the supervised learning models with associated learning algorithms that analyse data used for classification and regression analysis. For the given labelled training data (supervised learning), the algorithm outputs an optimal hyper plane which categorizes new examples.

Neural Networks: A neural network is a network or circuit of neurons, or in a modern sense, an artificial neural network, composed of artificial neurons or nodes. A neural network(NN), in the case of artificial neurons is an interconnected group of natural or artificial neurons that uses a mathematical model for information processing based on connectionist approach.

Random Forest: Random Forest algorithm is a supervised classification algorithm. As the name suggest, this algorithm creates the forest with a number of trees. In general, the more trees in the forest the more robust the forest looks like. In the same way in the random forest classifier, the higher the number of trees in the forest gives the high accuracy results.

EXPLANATION OF ATTRIBUTES:

Attribute importance is a supervised function that identifies and ranks the attributes that aremost important in predicting a target attribute. Raw machine learning data contains a mixture of attributes, some of which are relevant to making predictions.

Attribute Name	Description
ID	The unique ID given to the accountholder.
NAME	The name given to the account holder.
SCREEN-NAME	The pseudo name given to the accountholder.
CREATED-AT	The data when the account is created.
FRIENDS-COUNT	The number of friends for the account.
STATUSES-COUNT	The number of statuses posted from theaccount.
FOLLOWERS-COUNT	The numbers of followers for theaccount.
LISTED-COUNT	The number of groups the accountbelongs to.
URL	The URL of the account.
TIME-ZONE	The time-zone of the account holder.
UTC-OFFSET	The UTC-OFFSET, given time-zone
LOCATION	The location of the account holder.
GEO-ENABLED	This field must be true for the currentuser to attach geographic data when using POST statuses/update.
VERFIED	When true, indicates that the user has averified account.

Explanation of Attributes

VI. RESULTS

Algorithm	Normalised True Positives	Normalised True Negatives	Normalised False Positives	Normalised False Negatives	AUC	Accuracy(%)
Random Forest Algorithm	0.8935	0.9921	0.0078	0.106	0.94	93.79
Support Vector Machine Algorithm	0.8516	0.9763	0.0236	0.1483	0.91	90.78
Neural Networks	0.9850	0.9932	0.0149	0.0067	0.99	98.93

Comparison of Random Forest, Support Vector Machine, Neural Network Algorithms:

CONCLUSION

The model presented in this project demonstrates that Support Vector Machine (SVM) is an elegant and robust method for binary classification in a large dataset. Regardless of the non-linearity of the decision boundary, SVM is able to classify between fake and genuine profiles with a reasonable degree of accuracy (>90%). This method can be extended on any platform that needs binary classification to be deployed on public profiles for various purposes. This project uses only publicly available information which makes it convenient for organizations that want to avoid any breach of privacy, but organizations can also use private data available to them to further extend the capabilities of the proposed model.

IV. REFERENCES

[1] Nitika Kadam, Harish Patidar : **"Social Media Fake Profile Detection Technique Based on Attribute Estimation and Content Analysis Method"**, International Journal of Recent Technology and Engineering(IJRTE) ISSN: 2277- 3878, Volume-8 Issue-6, March 2020

[2] Er.Parveen Kumar, Er.Pooja Sharma : **"Artificial Neural Networks – A Study"**, International Journal of Emerging Engineering Research and Technology Volume 2, Issue 2, May 2014, PP 143-148

[3] Michael Fireetal. (2012). **"Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies."** Human Journal 1(1): 26-39.Günther, F. and S. Fritsch (2010).

[4] Dr. S. Kannan, Vairaprakash Gurusamy, **"Preprocessing Techniques for Text Mining",** 05 March 2015.

[5] Shalinda Adikari and Kaushik Dutta, **Identifying Fake Profiles in LinkedIn, PACIS 2014 Proceedings,** AISeL

[6] Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz,**"Malicious users'circle**

detection in social network based on spatiotemporal co-occurrence," inComputer Networks and Information Technology (ICCNIT),2011 International Conference on, July, pp. 35–390.

[7] Liu Y, Gummadi K, Krishnamurthy B, Mislove A," **Analyzing Facebook privacy settings: User expectations vs. reality",** in: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference,ACM,pp.61–70.

[8] Mahmood S, Desmedt Y," **Poster: preliminary analysis of google?'s privacy. In: Proceedings of the 18th ACM conference on computer and communications security",** ACM 2011, pp.809–812.

[9] Stein T, Chen E, Mangla K,**" Facebook immune system. In: Proceedings of the 4th workshop on social network systems",** ACM 2011, pp

[10] Saeed Abu-Nimeh, T. M. Chen, and O. Alzubi, **"Malicious and Spam Posts in Online Social Networks,"** Computer, vol.44, no.9, IEEE2011, pp.23– 28.

[11] J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y. Dai, B. Zhao, **Understanding latent interactions in online social networks, in: Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement,** ACM, 2010, pp. 369–382.

[12] Kazienko, P. and K. Musiał (2006). **Social capital in online social networks. Knowledge-Based Intelligent Information and Engineering Systems, Springer.**