2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

ADAPTIVE DETECTING FAKE PROFILES IN ONLINE SOCIAL NETWORKS

Mr.G.KARUNAKAR[1], A. YASASWINI[2], B.K.S.MADHURI[3], K.DHANYA NAGASREE[4]

1. Associate Professor, NRI Institute of technology, 2, 3, 4 Students, NRI Institute of technology

ABSTRACT Online social networking sites became an important means in our daily life. Millions of users register and share personal information with others. Because of the fast expansion of social networks, public may exploit them for unprincipled and illegitimate activities. As a result of this, privacy threats and disclosing personal information have become the most important issues to the users of social networking sites. The intent of creating fake profiles have become an adversary effect and difficult to detect such identities/malicious content without appropriate research. The current research that have been developed for detecting malicious content, primarily considered the characteristics of user profile. Most of the existing techniques lack comprehensive evaluation. In this work we propose new model using machine learning and NLP (Natural Language Processing) techniques to enhance the accuracy rate in detecting the fake identities in online social networks. We would like to apply this approach to Facebook by extracting the features like Time, date of publication, language, and geoposition.
Keywords: Social Networks, Threats, Fake Profiles, Malicious, Comprehensive, Machine learning and NLP

I. INTRODUCTION

Online Social Networks are most popular through which information can be exchanged throught the world. Social Networks being the center of attraction for many applications and they incorporate a range of new information and communication tools to the user community. 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. Because of the great reputation of social intelligence, social networking sites such as Facebook, YouTube, Twitter, LinkedIn, Pinterest,Google+, Tumblr and Instagram have become the preferred means of communication and information sharing tools amongst a diverse set of users including individuals and companies. The users of the social networks will play a vital role and they are completely responsible for the contents being exchanged in the networks. Users share information by interesting websites, videos and files. People share confidential data through the set-up of great faith and others have the same faith in the data shared. The rush of online social

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal


networks' reputation and the accessibility of huge amount of data enable them simple objective to the opponents. These objectives mainly include stealing individual user's details without seeking any permission.

1.1 Information Extraction Information extraction is the process of identifying key words and relationships in the text. It uses pattern matching algorithms to search for predefined sequences within the text. The software used for information extraction draws new relationships among known community and locations. And also it provides significant user information over time. These tools are extremely helpful while working with large amounts of data. Conventional data mining tools presume that the data being extracted is stored in the form of tables. Unfortunately, for most of the current applications, the only means of accessing digital information is by natural language processing [14].

1.2 Natural Language Processing NLP is a field of artificial intelligence and computational linguistics concerned with how information systems can be used to understand and process natural language documents.NLP research main objective is to gather information about how people comprehend and use natural language to accomplish the required job [15]. The origin of Natural Language Processing depend on most promising areas, such as computer and information sciences, linguistics, artificial intelligence and robotics ,mathematics, psychology, etc. NLP applications include a number of research areas like natural language text processing machine translation, language information retrieval, summarization, user interfaces, multilingual and cross speech recognition, artificial intelligence, and expert systems etc.[15]

1.3 Pre-processing methods Preprocessing techniques play a vital role in text mining. Preprocessing is the beginning step in the text mining approach. Preprocessing is done in three steps namely, stop words removal, stemming and lemmatization and Tokenization.

II. RELATED WORK The availability of data in social networks has drawn many research concerns encountered by online users. A Substantial research work has been carried out for a variety of social network problems like spam filtering, information diffusion and community detection. In[21] the researchers presented the possibility of information distribution without disclosing confidential data via graph models. In the research [22], they investigated "topological characteristics of Twitter" and presented that the behavior of information distribution in online networks known by examining "retweets".In the paper[23],they elaborated a report on "click-stream data in online networking sites" and proved that click-stream data provides a means to use rich information for drawing social relations .They also proved that most of user actions in online networks include browsing. Likewise in [24] the researchers examined social communications of user community in online social networks and initiated that most of the communications in online social networks are hidden and evident actions take place infrequently. Various research efforts

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

have been also turned towards the identification of malicious content in social networks. In the paper [25] the researchers planned a real-time spam detection scheme for Twitter social network in which they registered browser activities while loading a page for an URL.One more significant work for identifying spam on online social networking sites is proposed in [26] .In this proposed method, they created honey-profiles based on nationality, time ,age etc.This research is aimed at different accounts representing different areas . The researchers in [27] also made an attempt to use social honeypot to entice spammers on Twitter. In [28], the researchers described a significant attempt to typify various spams on Twitter social network.

The authors in[29] elaborated that the attacks of social junction were efficient and cheaper to get private information of an individual. Further in [30] the authors presented an approach to detect the users who are involved in malicious activities on Facebook. There are two stages in this mechanism. In first stage semantic analysis was done.In second stage spatiotemporal analysis was done.

III. PROPOSED WORK In our proposed model we would like to detect and classify fake users and real users using Machine learning and Natural Language Processing Techniques. In this work we present some steps that describe the process to distinguish fake users from legitimate users through a flowchart. Figure 1 show the working paradigm of our proposed work. In first step data set will be collected through Facebook using API. After the collection of data set in next step we are applying NLP pre processing techniques like Tokenization, Stop words removal, Stemming and lemmatization to extract features of users profile. After the extraction of the features we use reduction phase to reduce the dimensionality of the dataset. We would like to filter the profiles with tokenization, stemming and stop words to optimize the outcome before reduction. For reduction we apply Principal Component Analysis(PCA) algorithm.After the reduction phase we apply appropriate learning algorithm for classification.At the end we would like to use evaluation parameters like True positive rate (TPR) ,false positive rate (FPR) and AUC(Area Under ROC Curve) for determining the legitimate users and the malicious users.

Depending on AUC we calculate True Positive Rate and False Positive Rate.If True positive rate is higher than False positive rate then it as a legitimate us will be considered as legitimate user otherwise it will be treated as a fake user.In our work we would like to propose a frame work using Machine Learning and NLP Techniques .We would like to apply this frame work for social networking sites like Facebook and others.The main objective of our model is to increase the accuracy in identifying the spam or fake identities in online social networks.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

IV. WORKING PRINCIPLE OF PROPOSED WORK

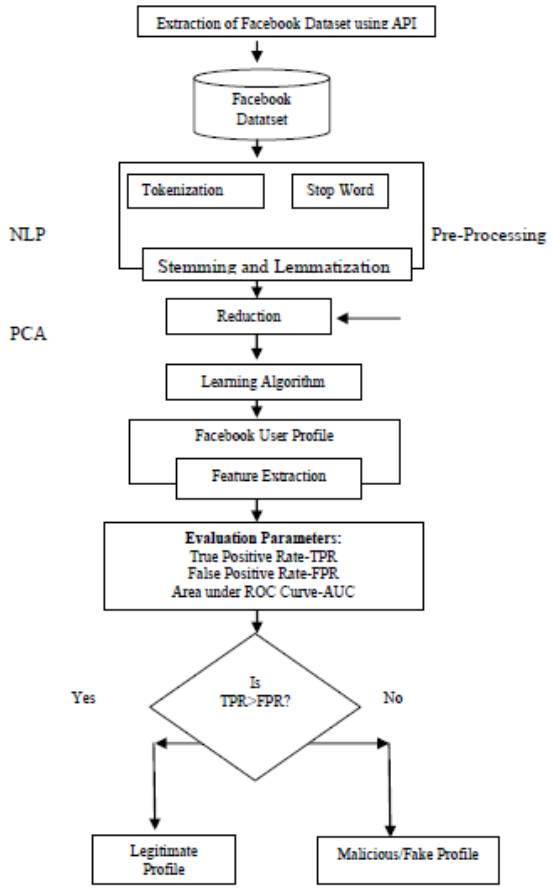
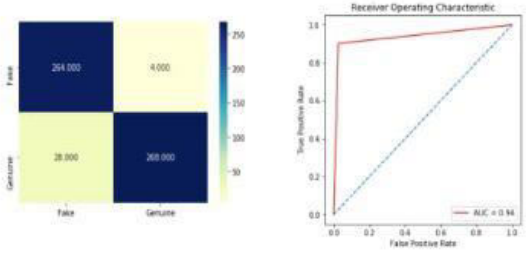
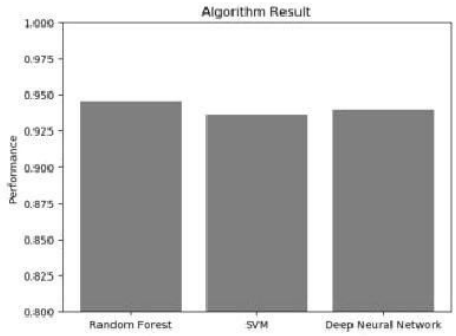


Figure-1: Working Paradigm of Proposed Work

DEEP NEURAL NETWORKS



ACCURACY



V. CONCLUSIONS AND FUTURE WORK

Our proposed work presents various classification , mining and pre-processed techniques to detect malicious users , extract features, reduce the dimensionality and to prevent users from fake profiles. In this work pros and cons of each existing technique have been discussed and alternate method was proposed. After implementation of proposed technique using Machine Learning and Natural Language Processing concepts, we evaluate performance by TPR,FPR and AUC. We try to show that our techniques are most efficient as compared to existing research in terms of accuracy and performance by taking advanced features like geoposition and date of publication. In future work we concentrate on availability of social networking sites datasets and we try to propose a new enhanced model to identify fake profiles on social networks. We are planning to collect dataset using Facebook Graph search API.Important features to be considered: Time, date of Publication or posts, language and geoposition. We are also working on other attributes like typescript of

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

user name, size, case and locality.

REFERENCES

[1.] Michael Fire et al. (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). "neuralnet: Training of neural networks." The R Journal 2(1): 30-38.

[2.] Source:ALLFacebook-2012.

[3.] Source:CNN.

[4.] 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.

[5.] Howard Rheingold (2000). The Virtual Community: Homesteading on the Electronic Frontier, MIT Press.

[6.] Source:eBizMBA2017.

[7.] Kontaxis, G., et al. (2011). Detecting social network profile cloning. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on,IEEE.

[8.] Krombholz, K., et al. (2012). "Fake identities in social media: A case study on the sustainability of the Facebook business model." Journal of Service Science Research 4(2): 175-212.

[9.] Cao, Q., et al. (2012). Aiding the detection of fake accounts in large scale social online services. Proc. of NSDI.

[10.] Bilge, L., et al. (2009). All your contacts are belong to us: automated identity theft attacks on social networks. Proceedings of the 18th international conference on World wide web, ACM.

[11.] Jin, L., et al. (2011). Towards active detection of identity clone attacks on online social networks.Proceedings of the first ACM conference on Data and application security and privacy, ACM.

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

[13.] Bradbury, D. (2011). "Data mining with Linkedin." Computer Fraud & Security 2011(10): 5-8.

[14.] Vishal Gupta and Gurpreet S. Lehal, A Survey of Text Mining Techniques and Applications, JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 1, NO. 1, AUGUST 2009.

[15.] S.Jusoh and H.M. Alfawareh, Natural language interface for online sales, in Proceedings of the International Conference on Intelligent and Advanced System (ICIAS2007). Malaysia: IEEE, November 2007,pp.224–228.

[16.] M.F. Porter, An Algorithm for Suffix Stripping, Program, vol. 14, no. 3, pp. 130-137, 1980.

[17.] Ms. Anjali Ganesh Jivani, A Comparative Study of Stemming Algorithms, Anjali Ganesh Jivani et al, Int.J.Comp.Tech.Appl.,Vol(6),1930-1938,ISSN:2229-6093.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

[18.] Deepika Sharma, Stemming Algorithms, A Comparative Study and their Analysis, International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Foundation of Computer Science FCS, New York,USA,Volume4–No.3,September2012–www.ijais.org.

[19.] C.Ramasubramanian and R.Ramya, Effective Pre-Processing Activities in Text Mining using Improved Porter‟s Stemming Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013, ISSN (Online) : 2278-1021.

[20.] Shalinda Adikari and Kaushik Dutta, IDENTIFYING FAKE PROFILES IN LINKEDIN, PACIS 2014 Proceedings,AISeL Sala, L. Cao, C. Wilson, R. Zablit, H. Zheng, B. Zhao, Measurementcalibrated graph models for social network experiments, in: Proceedings of the 19th International Conference on World Wide Web, ACM,2010,pp.861–870.

[21.] H. Kwak, C. Lee, H. Park, S. Moon, What is twitter, a social network or a news media?, in: Proceedings of the 19th International Conference on World Wide Web, ACM, 2010, pp. 591–600. 26

[22.] F. Benevenuto, T. Rodrigues, M. Cha, V. Almeida, Characterizing user behavior in online social networks, in: Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement, ACM, 2009, pp. 49–62.

[23.] 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.

[24.] K. Thomas, C. Grier, J. Ma, V. Paxson, D. Song, Design and evaluation of a real-time url spam filtering service, in: IEEE Symposium on Security and Privacy, 2011.

[25.] G. Stringhini, C. Kruegel, G. Vigna, Detecting spammers on social networks, in: Proceedings of the 26th Annual Computer Security Applications Conference, ACM, 2010, pp. 1–9

[26.] K. Lee, B. Eoff, J. Caverlee, Seven months with the devils: A longterm study of content polluters on twitter, in: Proceedings of the AAAI Conference on Weblogs and Social Media (ICWSM), 2011.

[27.] C. Grier, K. Thomas, V. Paxson, M. Zhang, @ spam: the underground on 140 characters or less, in: Proceedings of the 17th ACM Conference on Computer and Communications Security, ACM, 2010, pp. 27–37.

[28.] Puttaswamy KPN, Sala A, and Zhao BY,” Starclique: Guaranteeing user privacy in social networks against intersection attacks”, in: Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, CoNEXT ’09. ACM 2009, New York, NY, USA, pp.157-168

[29.] 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,” in Computer Networks and Information Technology (ICCNIT),2011 International Conference on, July, pp. 35–390.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

[30.] 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.

[31.] 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.

[32.] Stein T, Chen E, Mangla K," Facebook immune system. In: Proceedings of the 4th workshop on social network systems", ACM 2011, pp.1-8.

[33.] Kuzma J," Account creation security of social network sites", Inter J Appl Sci Technol 1(3):2011, pp. 8–13.

[34.] Debar D, Wechsler H," Using social network analysis for spam detection", In: Proceedings of the third international conference on social computing, behavioral modeling, and prediction (SBP'10). Springer-Verlag, Berlin, Heidelberg 2010, pp. 62–69.

[35.] Cukierski WJ, Hamner B, Yang B,"Graph-based features for supervised link prediction. In: IEEE International Joint Conference on Neural Networks (IJCNN)", IEEE 2011, pp. 1237–1244.

[36.] Anwar M, Fong PW,"A visualization tool for evaluating access control policies in Facebook-style social network systems", In: Proceedings of the 27th annual ACM symposium on applied computing, ACM 2012, pp. 1443–1450.

[37.] Rahman M, Huang T, Madhyastha H, Faloutsos M," Efficient and scalable socware detection in online social networks", In: Proceedings of the 21st USENIX conference on security Symposium 2012, USENIX association, pp. 32–32.

[38.] Rahman MS, Huang TK, Madhyastha HV, Faloutsos M,"Frappe: detecting malicious Facebook applications", in: Proceedings of the 8th international conference on emerging networking experiments and technologies,ACM2012,pp.313–324.

[39.] F. Ahmed and M. Abulaish, "An MCL-Based Approach for Spam Profile Detection in Online Social Networks," IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications2012,pp.1–7.

[40.] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference. ACM Request Permissions, 2012,pp.1–9.

[41.] Cao Xiao,David Mandell Freeman and Theodore Hwa,Detecting Clusters of Fake Accounts in Online Social Networks,ACM-2015,ISBN-978-1-4503-3826-4/15/10

[42.] F. Ahmad and M. Abulaish, A Generic Statistical Approach for Spam Detection in Online Social Networks,

[43.] Computer Communications, 36(10-11), Elsevier, pp. 1120-1129, 2013

[44.] Shalinda Adikari and Kaushik Dutta, IDENTIFYING FAKE PROFILES IN LINKEDIN,AISeL,PACIS-2014