Detecting Suspicious Accounts Responsible For Posting Forgery Multimedia Contents Using Trust Model

Shruti Varmora[1], prof. Namrata Shoff[2]
[1]Dept of Computer Engineering
[2]Asst. Prof., Dept of Computer Engineering
[1, 2] GEC gandhinagar

Abstract- *Internet activities have various communication ways and Social networking is one of the most popular way, with millions of users from around the world. And now a days people spent lots of time on social sites like twitter, Facebook or LinkedIn, and the scenario of using social sites for communication is constantly increasing at an impressive rate. At the same time, users describe their online profile with their personal information that completely represent their accurate identity, and using their profile they interact with other users and perform various activities like content sharing, news reading, posting messages, product reviews and discussing events etc.*

So as the number of users of social networking sites and e-comers sites are impressively increasing and as they have millions of interaction between them, so it would be difficult to identify genuine users and their respective post among them. There various techniques used to detect suspicious accounts, like Trust Model for multimedia social network is useful to detect the suspicious accounts responsible for posting fake multimedia contents.

Keywords- OSN, trust Model, Classifire, Graph properties

I. INTRODUCTION

social networking sites has the prelim importance for communication in today's world. In web based services Users are allow to create a public or semi public profile within a community or a group. articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.

Creating fake profiles or stolen the legitimate user's identity by fraudsters against a number of popular social networking sites is a critical issue now a days. There are various types of user accounts which are not the legitimate users, like Cloned Profiles, Compromised Profiles, Sock Puppets, Sybil Accounts, Bots etc[2].

Users must be aware about that they are with legitimate users not with fake ones, To communicate in any social relationships, internet intruders has favourable activity to Attack OSNs for Example, in Profile Hijacking the intruder can stole the existing legitimate user's profile and obtain the control over them within OSN platform. In Profile Attacking intruder control the existing user's profile and collect their information about OSN activities. For gathering multimedia information Retrieval and Analysis attack is another malicious behaviour. However OSN platforms have to deal with various types of attacks but Sybil attacks are the most usual and practical attacks among them. In Sybil Attack, the fraudsters stolen the identity of real users and pretend to be the same across OSN and without the aware of a specific user or a specific community they obtain their trust.

So to detect such type of fake profiles There various techniques used to detect suspicious accounts, like clustering, classification, finite automata and Trust Model. Various classifiers are used in classification technique. And trust model for multimedia social network is useful to detect the suspicious accounts responsible for posting fake multimedia contents. here is the brief explanation of various methodology which are used to detect fake profiles in social networks. Like Clustering, Classification, finite Automata, trust Model.

II. RELATED WORK

There are various techniques which are used to detect fake users from social media. And represent their result according to their utilized technique.

Clustering is a type of approach which is used to finding group of fake accounts. So identify those groups which include fake accounts it can consider various parameters to detect their identity. And this would applied by Cao Xiao, David Mandell freeman, Theodore hwa in 2015, to classify those entire clusters of accounts which are legitimate or fake researchers used the technique which is called supervised machine learning pipeline.

Other techniques which used for spam reviews detection by analyzing the reviews and comments given by the user for specific product. For that researchers used the technique called classifiucation, which would be applied by authors named as jitendra kumar Rout, smriti singh, sanjay kumar jena1, sambit bakshi1 in 2016, and applied supervised learning, semi-supervised learning and unsupervised learning techniques. Using this technique campared the user profiles as well as this are also used to detect spam reviews in promotion or demotion of social network websites or for any product. For these classification various classifier are used like neive bayes, SVM(Support Vector Machine) and Dicision tree.

OSN platforms have to deal with various types of attacks but Sybil attacks are the most usual and practical attacks among them. In Sybil Attack, the fraudsters stolen the identity of real users and pretend to be the same across OSN and without the aware of a specific user or a specific community they obtain their trust. This issue is resolved by Mohamed torky, Ali Maligy hani Ibrahim in 2017. Advancement in this research, author of this paper present a novel detection technique called Fake Profiles Recognizer (FPR). There are two key approaches of this proposed detection methodology are: Regular Expression and Deterministic Finite Automaton (DFA).

Finally surya Nepal, Cecil paris, Vanita sherchan describes the trust model concept in social network in 2012. Author contrast the trust community which is created by considering their members privacy and security so that they can gives their opinion, share their thoughts, and talks about their experience in an open and honest way without the fear of being judge, where Social network trust models introduced various terms to calculate trust are *social trust* and *social capital*. And they calculate two types of trust like; Popularity trust and engagement trust.

III. DATASET REPRESENTATION AND GRAPH PROPERTIES CALCULATION

There are various types of datasets format which are used in real world like, Edge list, Pajek format, Graphml format, Gexf format, .Net format. Every datasets format has different attributes. And cording to our requirements we have to chose appropriate dataset format. In this proposed framework we required Users information with appropriate attributes so Edgelist format is suitable for this proposed work. And there are so many graph analysis tools, and gephi is one of the most suitable tool for graph analysis and manipulation. And also networkX would also be used for this analysis.

This is how different type of dataset shown in graph format:

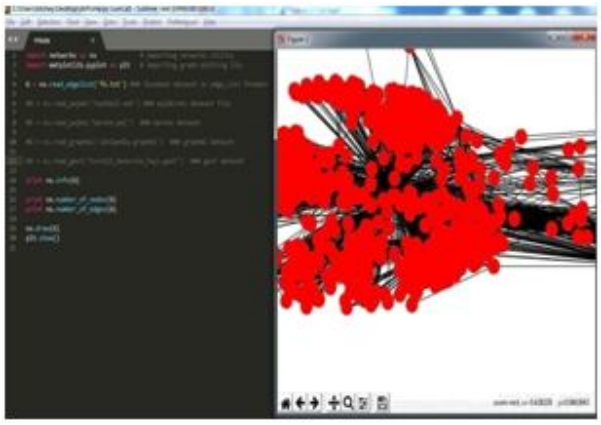

Figure 1: Edgelist format dataset representation

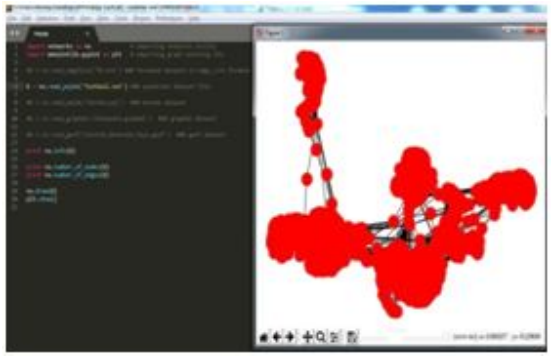

Figure 2: .NET format dataset representation

Graph analysis would help us for this proposed work because various graph properties like number of nodes, number of Edges, Average network degree, clustering coefficient, network Density will help us to describe characteristics of Users of Social network datasets.

Average network degree of a graph says that number of other connected to a particular one node. If degree of a node is high then more number of nodes connected to this particular node, otherwise there is less number of nodes connected to a particular node. If we compare it with social network datasets then nodes represents User and Edges represent their communication or interaction. And degree of node represents their trust value so as the degree is high trust value of a node is high so it can be a genuine user.

Figure 4: Social media dataset Analysis and graph properties calculation

IV. IMPEMENTATION RESULTS

Now finally for detection of fake accounts we implement our proposed methodology and there are aome attributes considered for our proposed detection process of fake accounts. Some of them are listed here.

Considerable Attributes:

1> Friend list(Total number of friends)
2> Male/Female(Gender)
3> Number of tagged photos
4> About me(description length)
5> Carrier profile(Education & Work life)
6> Status of relationship(single/double)
7> Number of wall post posted by others
8> Number of uploaded photos

And based on this basic considerable attributes we can also predict some result which gives the algorithm efficiency, which is given by below formula

Algorithm Efficiency (Ω) =

$$\frac{\text{Number of Correct prediction}}{\text{Total Number of prediction}}$$

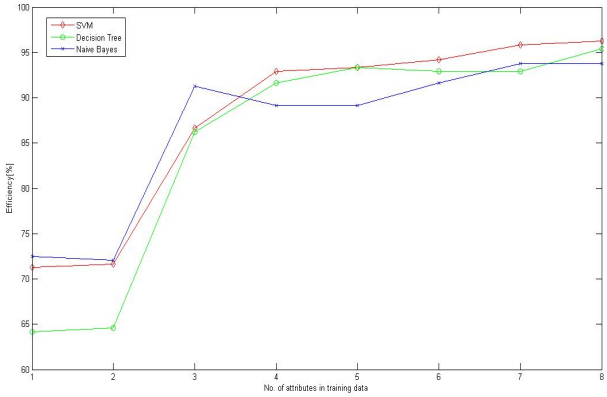

Figure 5 efficiency of algorithm

This result shows that how efficiency of algorithm will differ according to the classifier used by algorithm and in this proposed work we compare three classifier named as Dicision tree, naive Byse and Support vector machine. And in this graph we can see that SVM classifier gives the best efficiency for this proposed algorithm.

V. CONCLUSION

Privacy and security of a individual's profile is primary concern of social networking site for communication. But, As users are gradually increasing in social and e-comers site now a days. This is tedious job to identify legitimate users and to detect fake profiles. Detection of trusted profiles is important for safe and useful communication. This paper proposed various methodologies of graph analysis which are useful for detection of suspicious account. In this project work, social media fake profile detection is begin carried out using data mining algorithms, & as per the result the facebook fake profile can be detected with 90-95% efficiency as shown in graph with proposed algorithms,

VI. FUTURE WORK

In today's Scenario there are various attacks are introduced in all social networking sites. And various risk are there to apply any methodology to detect fake accounts so directions for future work is to conduct study of various Risk strategy and anti attack mechanisms to increase the effectiveness of proposed work.

VII. ACKNOWLEDGEMENT

I grateful to all my advisors for their expertise and endless helpful advice, and me guide to support me and advice me. I also thankful to all the authors and reviewers for their comments and feedback to my work. Work is done under the expert opinion and guidance.

REFERENCES

[1] Mauro Conti, Radha Poovendran, Marco Secchiero, "FakeBook: Detecting Fake Profiles in On-Line Social Networks", 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, added to IEEE Xplor on 4th Feb 2013.

[2] Cao Xiao, David Mandell Freeman, Theodore Hwa, "Detecting Clusters of Fake Accounts in Online Social Networks", University of Washington and. LinkedIn Corporation, oct 16,2015

[3] Mohamed Torky, Ali Meligy, Hani Ibrahim, "Recognizing Fake identities in Online Social Networks based on a Finite Automaton approach", computer Engineering Conference(ICENCO), 2016- 12th international, 28-29 Dec, 2016, Added to IEEE Xplor on 16th feb 2017.

[4] Jitendra Kumar Rout, Smriti Singh, Sanjay Kumar Jena1, Sambit Bakshi1, "Deceptive review detection using labelled and unlabeled data", Multimedia Tools And Applications on February 2017.

[5] Surya Nepal, Cecile Paris, Vanita Sherchan, "Surya Nepal, Cecile Paris, Vanita Sherchan",

[6] Zhiyong Zhang • Kanliang Wang, "A trust model for multimedia social networks", Social Network Analysis and mining on December 2013.

[7] Todd Bodnar, Conrad Tucker, Kenneth Hopkinson, Sven G. Bil´en, "Increasing the Veracity of Event Detection on Social Media Networks Through User Trust Modeling",

[8] Sajid Yousuf Bhat & Muhammad Abulaish," Communities Against Deception in Online Social Networks", *Communities Against Deception in Online Social Networks, Computer Fraud and Security, 2014, Elsevier, Feb. 2014.*

[9] Mudasir Ahmad Wani*, Suraiya Jabin, "A sneak into the Devil's Colony- Fake Profiles in Online Social Networks"

[10] Simon Fong, Yan Zhuang, Maya Yu, Iris Ma, "Quantitive analysis of trust factors on Social Networks using data mining Approach", 2012- IEEE

[11] M. Daiyan1, Dr. S. K.Tiwari2, M. A. Alam3, "Mining Product Reviews for Spam Detection Using Supervised Technique", International Journal of Emerging Technology and Advanced Engineering, August 2014.

[12] Sahil Puri1, Dishant Gosain, Mehak Ahuja, Ishita Kathuria, Nishtha Jatana,
"Comparison And Analysis Of Spam Detection Algorithms" IJAIEM, April 2013

[13] Michail Tsikerdekis, "Identity Deception Prevention using Common Contribution Network Data", IEEE,2015

[14] Guowei Wu1, Zuosong Liu1, Lin Yao1,∗, Jing Deng2 and Jie Wang, "A Trust Routing for Multimedia Social Networks", The Computer Journal Advance Access published October 4, 2014.

[15] Ali M. Meligy, Hani M. Ibrahim, Mohamed F. Torky, A Framework for Detecting Cloning Attacks in OSN Based on a Novel Social Graph Topology, *I.J. Intelligent Systems and Applications,* 2015,

[16] Lijun Yang, Zhiyong Zhang, Weili Tian, Qingli Chen, "Advance on Trust Model and Evolution Method in social network", 2012 Sixth International Conference on Genetic and Evolutionary Computing.

[17] http://www.yourarticlelibrary.com

[18] https://www.scribd.com /doc/14790526/Trust-Models

[19] Data Mining Concepts and Techniques/third Edition/ Jiawei Han, Micheline Kamber, Jian Pei

[20] Data mining/ Practical machine Learning Tools and Techniques/ Ian H. Written and eibe frank