ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Detection of User Cluster with Suspicious Activity in Social Networking Sites using Natural Language Processing

Ameena A

P.G student, Dept. of C.S.E, SBCE, Pattoor, Alappuzha, India

ABSTRACT: Now a days, the social life of everyone has become associated with the Social Networking Sites. These sites have made a drastic change in our social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake profiles, security problem, cyber bullying, online impersonation have also grown. SocialNLP is a new inter-disciplinary area of natural language processing (NLP) and social computing. Apart from common word processor operations that treat text like a mere sequence of symbols, SocialNLP process human language in terms of its meaning. This paper proposes a SocialNLP system for performing trust analysis in messages, likes, shares and web URL's exchanged over social networking sites using NLP techniques .The proposed system is also able to identify user cluster who are discussing about suspicious activities. So if there is a system which can identify such activities and the persons involved, it will prove to be a boon for the law enforcement people.

KEYWORDS: Social Networking Sites, Social NLP, Trust analysis, Suspicious activity, Natural Language Processing

I. INTRODUCTION

Social Networking Sites (SNS) plays very important role in human life now a days, it is becoming a main communication media among individuals and organizations. SNS contains list of users with whom we can share a connection, view their activities in network and also converse. SNS users communicate by messages, blogs, chatting, video and music files.

With social media services' rise of popularity, including general-purpose Microblogs such as Facebook, Plurk and Twitter, goal-oriented services such as Linkedln (for professional occupation), Del.icio.us. (a social bookmarking service) and Foursquare (a check-in service for mobile devices), and Web 2.0-based large-scale knowledgebase such as Wikipedia and common-sense corpus, now researchers can assess heterogeneous information of the target human/object that includes not only text content but also meta-data, or even the social relationships among persons.

Furthermore, the content on social media and Web 2.0 platforms is different from that on others in terms of style, tone, purpose, etc. For instance, posts on twitter are limited in size, thus can contain jargons, emoticons, or abbreviations which usually do not follow formal grammar. It is not suitable to apply existing natural language techniques on such content because they are not tailored to do so. For instance, standard summarization techniques might not be suitable for Plurk posts that are relatively short and contain responses from multiple friends; and sentiment dictionaries learned from news corpus might not be suitable for sentiment detection tasks on Microblogs.

As it is generally believed social media has become one of the major means for communication and content producing, while such trend is not likely to fade away, being able to process content from social media platforms does bring a lot of values in real-world applications. Furthermore, due to the change of the style to the content and the availability of heterogeneous resources (e.g. social relationship among people) one can obtain, novel Natural Language Processing (NLP) techniques that are designed specifically for such platform and can potentially integrate or learn information from different sources are highly demanded.

Power of SNS can be abused for wrong objective such as, fake profiles, security problems, cyber bullying, online impersonation and terrorists may use SNS to spread hate messages. If people select SNS to spread hate messages in a group which harms the society or organizations, then behavior of such users in SNS deviate from the normal. If there is a system which is able to identify these changes in user's behavior and give clue, then immediate

DOI: 10.15680/IJIRCCE.2015. 0310052

action can be taken so that there is more chance to avoid the wrong things, that may happen in future, or if wrong things has happened, then this can be a clue for tracking criminals which could be used by investigation agency like CBI and NIA etc.

SocialNLP is a new inter-disciplinary area of natural language processing and social computing. Apart from common word processor operations that treat text like a mere sequence of symbols, SocialNLP process human language in terms of its meaning. This paper proposes a SocialNLP system for performing trust analysis in messages , likes ,shares and web URL's exchanged over social networking sites using NLP techniques. The proposed system identifies suspicious user cluster, which is a combination of trust analysis and NLP techniques. NLP gave the sentence level meaning of the message. Using trust analysis we find whether user is suspicious or not. So if there is a system which can identify such activities and the persons involved, it will prove to be a boon for the law enforcement people.

II.RELATED WORK

In [1] authors discussed about "detection of user cluster with suspicious activity in online social networking sites". They proposed a system for detection of the sentiments in online messages and comments exchanged over social networking and blogging sites, which monitors communication between users and identify the messages of individuals who exhibits anomalies behavior over time. They had proposed and devised algorithms to analyze the message exchange over social networking sites to identify the cluster of people indulged in topic wise suspicious activities. In [2] authors discussed about "Natural language processing for content analysis in social networking". They describe a combination of HTML DOM analysis and Natural Language Processing techniques for rating the blogs and posts with automated extractions of abusive contents from them. But for higher accuracy in content extraction, the analyzing software needs to mimic a human user and understand content in natural language similar to the way humans intuitively do in order to eliminate noisy content. In a design proposed by [3], the system is to be built such that, it is an active monitoring agent that resides at major message communication hub and responsible for each message that passes through the hub is reconstructed to acquire basic information. If the message passed has unusual properties, then anomalies characteristics are noted and recorded. However their proposed system acquires input through a fixed database of e-mail. This e-mail was drawn from the Enron e-mail dataset. According to a report released by United State Army [4], Online Social Media Sites (OSMS) could become an effective coordination tool for terrorists to launch attacks, they highlighted that 90% of the terrorist activities carried out on the Internet are organized through SNS. Now a days, law enforcement officers using OSMS for investigation [5].

If people select SNS to spread hate messages in a group which harms the society or organizations, then behaviour of such users in SNS deviate from the normal. If there is a system which is able to identify these changes in user's behaviour and give clue, then immediate action can be taken so that there is more chance to avoid the wrong things, that may happen in future, or if wrong things has happened, then this can be a clue for tracking criminals which could be used by investigation agency like CBI [6] . In [7] authors discussed about different classification techniques for detection of fake profiles in social networking sites.The classifier used for classifying the profiles are: Naive Bayes classification , Decision Tree classification, Support Vector Machine classification. In [8] authors have proposed six-element analysis method for terrorist activities based on social network. A variety of sub-networks are constructed according to the correlation among the six elements people, organization, time, location, method and event. However they have applied and analyzed this method on data obtained from previous years incidents, which they gathered from 420 web pages to get the information of the terrorist events incited by East Turkistan. [9], proposed a concept to integrate between Content Analysis (CA) and Social Network Analysis (SNA). In this approach they proposed a method to analyze communication transcripts. It is used to filter out related messages from unrelated messages, but according to them, the research is limited to analyze asynchronous discussion for students participating in a course. In [10] authors has presented the experimental study of common document clustering techniques, which organizes documents into groups such that each group contains documents with similar content. However they have used stored data set from Reuter-21578 collection.

III. PROPOSED SYSTEM

Objective of our proposed system is to analyze the messages, message share, message like, message unlike, message comment, comment like, comment unlike in the SNS and perform trust analysis to identify cluster of suspicious users indulged in suspicious activities.

Assumptions: Access to SNS data is difficult and this authority is given to only law enforcement people. For the experimental purpose we have created a private social network called ’Trust Social Site’. Once the proposed system works well with the data obtained from this network, then it is assumed that it will work in any social network, if all the information is provided.

Design of Proposed System: Figure 1. shows the design of our proposed system. Proposed system is collection of five sub system:

- Social data monitoring system and Database
- Suspicious message identification system
- Trust analysis system
- Suspicious users identification system
- Visual representation of suspicious users

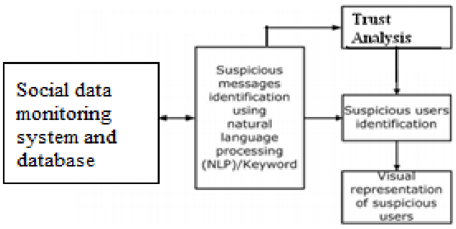

Trust Analysis
Social data monitoring system and database
Suspicious messages identification using natural language processing (NLP)/Keyword
Suspicious users identification
Visual representation of suspicious users

Fig. 1. System design

A. Social data monitoring system and Database

According to the proposed system design, data is obtained from social networking sites. This data has been obtained through online monitoring system that monitors the communication between the users and captures the information passing between them. The information includes message sender, message receiver, actual message, date and time stamp when message was sent. ’Social data monitoring system’is responsible for this job, for this purpose the system also includes database part. From this database, information are accessed for processing to identify suspicious message. In the proposed system, suspicious users are highlighted with their username. The table ’userinfo’ will hold the user’s personal details. Table ’MESSAGE’ holds the message details which are exchanged between the registered users.

B. Suspicious Message identification system

Input to this module is the data collected from Social Data Monitoring System and Database. Then NLP techniques like Stop word removal, Tokenization, Stemming are applied to find suspicious words. Once the suspicious words are found then the message or comment is considered as suspicious. The metadata is monitored for identifying from and to which Email-id the suspicious words belong. User details like email-id ,phone Number,age and other relevant information are traced by browsing their profiles from database, which are provided during the creation of account in SNS. This module have following sub-modules:

- *Stop Word Removal:* Sometimes, some extremely common words which would appear to be of little value are excluded from the vocabulary entirely. These words are called stop words. Commonly used stop words are and,a, the, was, were, for, from, at, be, by etc. From the data , stop words are removed and pass this data as the input to next step.

- *Tokenization:* Tokenization is the process of breaking up the given text into units called tokens. The tokens may be words or number or punctuation mark. Tokenization does this task by locating word boundaries. Ending point of a word and beginning of the next word is called word boundaries. Tokenization is also known as word segmentation. In English Language most of the words are separated from each other by white spaces.
- *Stemming:* After tokenization stemming is performed. Stemming is the process for reducing inflected (or sometimes derived) words to their word stem, base or root form generally a written word form. Example : kidnapped is stemmed to kidnap.
- *Sentiment Score Identification System*: This sub-system gives a sentiment score to the message based on each word weight. A word set has been used to assign score to each word. Each word in data set is assigned with score ranging from 1 to 5. Positive word is having positive score +1 to +5 and negative word is having negative score -1 to -5.

C. Trust Analysis

Trust analysis between users speak about the similarity in opinions between the SNS users. Trust metrics allows to easily cluster users based on trust.

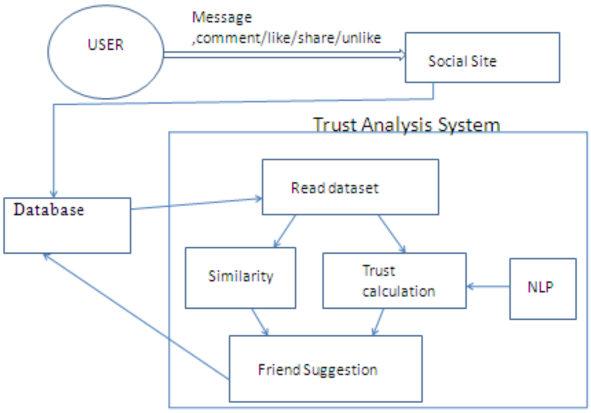
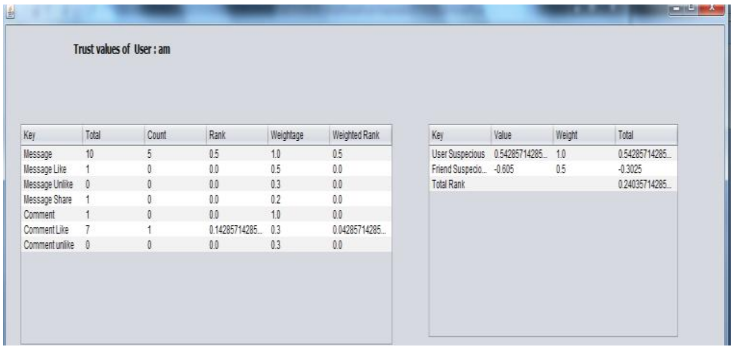


Fig.2. Trust analysis system

User access Social networking site and post messages, like messages, unlike messages, share messages, comment on messages, like comments , unlike comments. These datas are stored in a database and the trust analysis system read dataset from the database . Then trust calculation is permormed using NLP techniques and similarity is find. Based on similarity and trust calculated friend suggestion can be done and is updated in database. Users with positive trust value is considerd as trust users and users with negative trust value is considerd as suspicious.



Trust values of User : am

Key	Total	Count	Rank	Weightage	Weighted Rank
Message	10	5	0.5	1.0	0.5
Message Like	1	0	0.0	0.5	0.0
Message Unlike	0	0	0.0	0.3	0.0
Message Share	1	0	0.0	0.2	0.0
Comment	1	0	0.0	1.0	0.0
Comment Like	7	1	0.14285714285...	0.3	0.04285714285...
Comment unlike	0	0	0.0	0.3	0.0

Key	Value	Weight	Total
User Suspecious	0.54285714285...	1.0	0.54285714285...
Friend Suspecio...	-0.605	0.5	-0.3025
Total Rank			0.24035714285...

Fig.3. Trust analysis

D. Suspicious Users Identification System

Once the message is found to be either suspicious or normal, users of the corresponding messages are flagged either as suspicious or normal. Since there may be a chance of getting false positive result by single message process and marking the user as suspicious, the trust analysis values are also considered. Users with positive trust value is considered as trusted users and users with negative trust value is considered as suspicious.

E. Visual representation of suspicious users

Once system identifies the suspicious users in network, these users and their importance in that network are identified; it is possible to obtain graphical representation of user network, which comprises of node and edges. In this network each node represents users and edge represents connection between users in terms of trust analysis. By using this, we can analyse each users behaviour in that network. The results obtained from that are shown to the law enforcement officers by highlighting those suspicious users cluster to take appropriate action. To find cluster of users in network who are discussing about suspicious activities, first we have to find correlation among the messages which are exchanged in network and later from that find the cluster of people. Visual representation of suspicious users are shown in Figure 4.

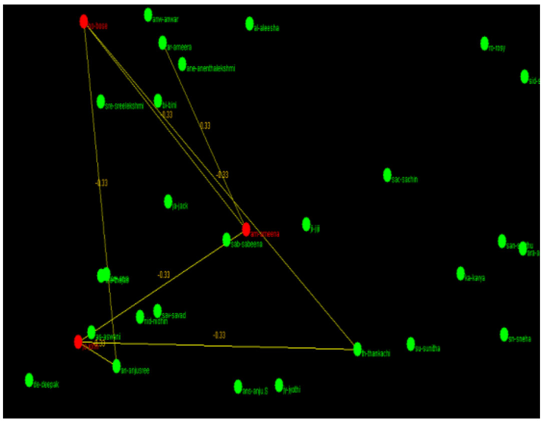


Fig.4 .Visual representation of suspicious users

IV. PROPOSED ALGORITHM

Algorithm for Trust analysis

```
1.  Set tuning parameters
2.  for each message M of Ui
3.              if  M is Suspicious add M to Ui.Sus_M
4.  for each messagelike ML of Ui
5.         if  M is Suspicious add M to Ui.Sus_ML
6.  for each messageunlike ML of Ui
7.         if  M is Suspicious add M to Ui.Sus_MU
8.  for each message share MS of Ui
9.          if  M is Suspicious add MS to Ui.Sus_MS
10.  for each comment C of Ui
11.          if  C is Suspicious add C to Ui.Sus_C
12.  for each commentlike CL of Ui
13.          if  C is Suspicious add C to Ui.Sus_CL
```

```
14.  for each comment unlike CU of Ui
15.        if  C is Suspicious add C to Ui.Sus_CU
16.  M_Sus(Ui) =   size of (sus_M)
                   Total M of Ui
17.  MyRank=M*M_wt+ML*ML_wt+ MU*MU_wt+MS*MS_wt+ C*C_wt+ CL*CL_wt+ CU*CU_wt
18.  Set  FriendSuspeciousRank =0
19.  for i=0 to num_of friends
20.  FriendSuspeciousRank =  FriendSuspeciousRank +
              MyRank*Friend[i].MyRank

21.  TotalMyRank=MyRank_Prefernece*MyRank+TotalFriendSuspeciousRank*FriendRankPrefernce;
```

V. Simulation Results

Users get friend suggestion based on the trust analysis value generated from their friend lists. Trust analysis value greater means more closely related users. Users with positive trust value is considered as trust users and users with negative trust value is considered as suspicious ones. Friend suggestion between users was expressed by using the graph shown below.

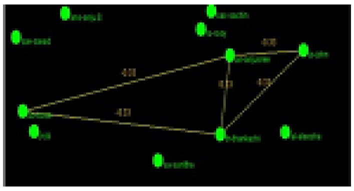


Figure 5.1: Visual representation of normal users based on trust

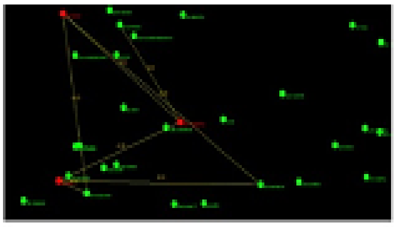
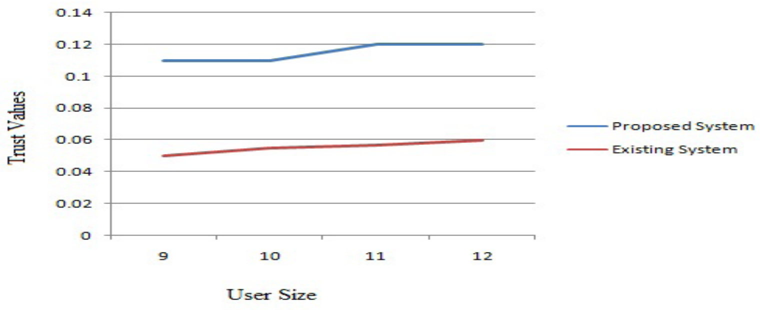


Figure 5.2: Visual representation of suspicious users based on trust



The graph above compares the existing system and proposed system. From graph analysis it is concluded that the proposed system performs better than existing one. Existing systems only considers message communication. Proposed system considers not only message passing but also message like, unlike, comments, comment like, comment unlike ,share etc. Also trust analysis is performed. So performance of existing system is better.

VI . Conclusion and Future Work

The simulation results showed that the proposed algorithm performs better than existing system. Social networking sites has emerged as the most important source of communication in the world. But a huge controversy has continued in full force oversupervising offensive content on internet pages. Often the abusive content is interspersed with the main content leaving no clean boundaries between them. Therefore, it is essential to identify abusive contents exchanged through SNS. This paper proposed and devised algorithms to analyze the message exchange over social networking sites and perform trust analysis to identify the cluster of people indulged in suspicious activities,also friend suggestion is made. So the proposed system can be used by crime investigation agencies to identify suspicious users in SNS. As a future work, some suggestions are made. The proposed system can be used by crime investigation agencies to detect people indulged in suspicious activities. Also it can be used to provide highly secure social networking to end users. They are

- Suspicious message identification can be implemented in real time.
- Implement methods to analyze encrypted messages .

References

1. Sharath Kumar A and Sanjay Singh, “Detection of User Cluster with Suspicious Activity in Online Social Networking Sites,” *Second International Conference on Advanced Computing, Networking and Security 2013* .
2. A. A. Sattikar and R. V. Kulkarni., “Natural language processing for content analysis in social networking,” *International Journal of Engineering Inventions, September 2012.*
3. R. Layfeild, B. Thuraisinghami, L. Khan, M.Kantarcioglu, and J. Rachapalli.,“Design and implementation of a secure social network system”*IEEE International Conference June,2009.*
4. Weimann and Gabriel., “Terror on facebook, twitter, and youtube,” The Brown Journal of World Affairs, vol. 16, pp. 45–54, 2010.
5. M.Alderson., “Facebook: a useful tool for police?” Connectedcops. 25 January 2011. Web. 3, February 2011.
6. CBI. (2013) Central Bureau of Investigation (CBI)-the national investigation agency of India. [Online]. Available: http://cbi.nic.in/
7. Ameena.A and Reeba .R [7],”Different classification techniques for detection of fake profiles in social networking sites”,*current issue,ijarse,* ISSN 2319- 8354, vol 4, march 2015.
8. F. J. Fu, J. Chai, and S. Wangl., “Multi-factor analysis of terrorist activities based on social network,” BIFE, 2012 Fifth International Conference on 18-21 Aug.2012, pp. 476–480, 2012.
9. Erlin, Y. Norazah, and A. Rahman., “Integrating content analysis and social network analysis for analyzing asynchronous discussion forum,” Information Technology, 2008. ITSim 2008.
10. V. Amala Bai and D. Manimegalai, “An analysis of document clustering algorithms,” in Communication Control and Computing Technologies (ICCCCT), IEEE International Conference on, 2010.
11. Skillicorn and David, “Keyword filtering for message andconversation detection,” Queen’s University.
12. Sentistrength - sentiment strength detection in short texts. [Available Online]http://sentistrength.wlv.ac.uk.
13. N. Caren. An introduction to text analysis with python. [Available Online] http://nealcaren.web.unc.edu/ .
14. I. Guy, I. Ronen, and E. Wilcox, “Do you know?: Recommending people to invite into your social network,” in *Proc. 14th Int. Conf. Intell. User Interfaces*, 2009, pp. 77–86.
15. C.-W. Hang, Z. Zhang, and M. Singh, “Shin: Generalized trust propagation with limited evidence,” *Computer*, vol. 46, no. 3,2013.
16. NIA. (2013) National Investigation Agency (NIA). [Online]. Available: http://www.nia.gov.in/
17. J. Leskovec, D. P. Huttenlocher, and J. M. Kleinberg, “Predicting positive and negative links in online social networks,” in *Proc. 19th Int. Conf. World Wide Web*, 2010, pp. 641–650.
18. I. Varlamis, M. Eirinaki, and M. D. Louta, “A study on social network metrics and their application in trust networks,” in *Proc. Int. Conf. Adv.Social Netw. Anal. Mining*, Aug. 2010, pp. 168–175.
19. Recorded future: Creating an insightful world. [Available Online]. https://www.recordedfuture.com/.
20. Magdalini Eirinaki, Malamati D. Louta and Iraklis Varlamis,“A Trust-Aware System for Personalized User Recommendations in Social Networks,” *IEEE transactions on systems, man, and cybernetics: systems, vol. 44, no. 4,* April 2014.

BIOGRAPHY

Ameena.A is a Post Graduate (M. Tech) student in the Computer Science and Engineering Department, Sree Buddha College of Engineering, Pattoor, Kerala University, India. She received B.Tech degree in 2012 from CEKNPY, Karunagappally, Kerala, India.