2013 Second International Conference on Advanced Computing, Networking and Security

Detection of User Cluster with Suspicious Activity in Online Social Networking Sites

Sharath Kumar A and Sanjay Singh
Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal University
Manipal-576104, India
sharathkumara@yahoo.co.in, sanjay.singh@manipal.edu

***Abstract*—Online social networking sites such as Facebook and Google+ among others are the great way to be in touch with our near and dear ones. Nonetheless, the power of social networking sites can be exploited for the purpose of illegal activities such as planning terrorism related activities or spreading some sorts of hate message in the society. So if there is systems which can identify such activities and the persons involved, then that system will prove to be a boon for the law enforcement people.**

This paper proposes 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. The proposed system is also able to identify group of people who are discussing about same topics which may be about a suspicious activity.

***Index Terms*—Social Networking Site, Content Analysis, User Cluster, Suspicious User.**

I. Introduction

Social Networking Sites (SNS) are web-based services that facilitates individuals to construct a profile, which is either public or semi-public. SNS contains list of users with whom we can share a connection, view their activities in network and also converse[1]. SNS users communicate by messages, blogs, chatting, video and music files.

Social Networking Sites plays very important role in human life now a days, it is becoming a main communication media among individuals and organizations. The other advantages includes keeping contact with friends and family members. For entrepreneurs it acts as a resource to set up a global presence. Employers now a days use SNS as useful and effective recruitment tool. Some SNS provides low cost advertising for business owners. However with all these advantages, SNS also have many disadvantages such as information is public, security problem, cyber bullying and misuse and abuse of SNS platform.

Power of SNS can be abused for wrong objective such as, terrorists may use SNS to spread hate messages. If a task requires a group of people then, that group should communicate properly. If people in a group are located far distance from each other, they should use any media to exchange information, most common media is telephone, which is not cost effective if group members are located at different geographical location with different time zones. One of the best and cost effective media is the Internet. Internet technology makes it easy for an individual to communicate quickly and effectively. Most of the people communicate by Email or by SNS which provide good environment for user to exchange messages.

The Internet is often utilized to promote and support acts of terrorism. Planning an act of terrorism typically involves remote communication among several parties. Internet technology may be used to facilitate communications within and between organizations across the globe promoting violent extremism [2]. Criminal activities coordinated via Social Media, Online Social Media Sites (OSMS) has long been used for the purpose of planning and organizing criminal activities [3]. According to a report released by United State Army [4], 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 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 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] and NIA [7] etc.

There are few works done in the area of Social Networking Sites and Content Analysis. Julei Fu and Jian Chai [8], have proposed six-element analysis method for terrorist activities based on social network. 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. Erlin et al. [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. Mary Amala Bai et al [10], has presented the experimental study of common document clustering techniques, which organizes documents into groups

978-0-7695-5127-2/13 $31.00 © 2013 IEEE
DOI 10.1109/ADCONS.2013.17

such that each group contains documents with similar content. However they have used stored data set from Reuter-21578 collection.

Skillicorn and David [11], has used matrix decomposition techniques, where they applied to message-word and message - rank matrices. This technique can be used to filter out interesting subset from the set of all messages. However they have shown results only for artificial small dataset and particular modifications to it. Sattikar and Kulkarni [12], have proposed a natural language processing (NLP) based techniques for rating the blogs and posts in social networking with automated extractions of extremely offensive and insulting contents from them. However it is not fully automated, to achieve this system requires supplemental user involvement. In a design proposed by R. Layfeild and B. Thuraisingham [13], 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.

Therefore, there is a need of a system for content analysis of social networking sites in real time, which is able to identify the anomalies activities on social networking sites. Currently such a system is far from requirements, so in this area more research is required. This paper has tried to address these problems and successful in getting some motivating results. In this paper, we propose a system design, which identify the cluster of people in SNS, whose behaviors are suspicious. We have also focused on finding the cluster of users who are discussing about same thing, this is done by finding the similarity in messages which are being exchanged among them. Then analyze the user's behavior in SNS, what is the role of each user, their importance in that network etc. Also we have found the suspicious users in a organization, who are leaking the confidential information to outside world. The remaining paper is organized as follows. Section II describes the proposed system. Section III discusses the results obtained and finally section IV concludes this paper.

II. Proposed System

Objective of our proposed system is to analyze the messages in the SNS and 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 'Manipal Net'. 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:

- Online data monitoring system and Database
- Suspicious message identification using NLP/Keyword system
- Latent semantic analysis (LSA) system
- Suspicious users identification system
- Visual representation of suspicious users

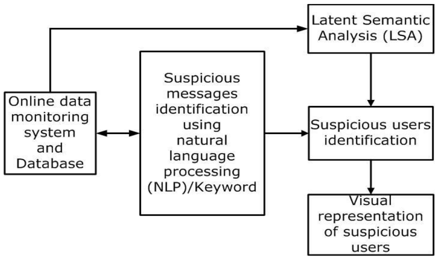
Latent Semantic Analysis (LSA)
Online data monitoring system and Database
Suspicious messages identification using natural language processing (NLP)/Keyword
Suspicious users identification
Visual representation of suspicious users

Fig. 1. Diagram showing the components of proposed system.

A. Online 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. 'Online 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. The design of database for this system is shown in Fig. 2.

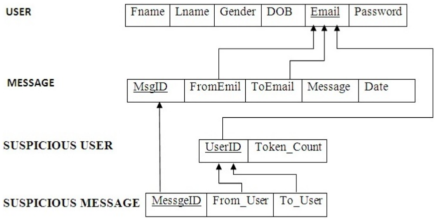

Fig. 2. Diagram showing the database design of proposed system.

In the proposed system, email address is used as username, later same will be processed and at the end suspicious user are highlighted with this username. The table 'USER' will hold the user's personal details. Table 'MESSAGE' holds the message details which are exchanged between the registered users. To keep information about suspicious users 'SUSPICIOUS USER' table is used, attribute of this table are UserID, which is registered email address, and one more field is Token_Count, which keep track of the counter value of suspicious user, because it is not correct to point out a person as suspicious user by single message which is sent or received, as there may be chance of false positive, so the attribute Token_Count keeps a count of suspicious message for a suspicious user. When system finds suspicious messages, those messages has to be kept separately for future reference. The table 'SUSPICIOUS MESSAGE' is for maintaining those details.

B. Suspicious Message identification system using NLP / Keyword

Figure 3. shows the components of suspicious message identification system. This module is responsible for identification of suspicious message in communication text. Input to this sub system is the entire message. For the time being we are finding the suspicious users based on some specific topics, some of the topic we have chosen are 'Hate Messages', 'Terrorist Activity', 'Delhi Gang Rape' and 'Harm to Society', 'Narendra Modi' and 'Confidential Keyword Based Suspicious Message Exchange from Organization'. In future by combining many topics make the system into general purpose one, i.e. system to identify all suspicious users. This module have following sub-modules:

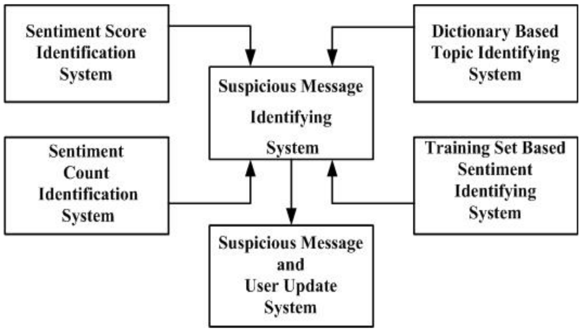
Sentiment Score Identification System
Dictionary Based Topic Identifying System
Suspicious Message Identifying System
Sentiment Count Identification System
Training Set Based Sentiment Identifying System
Suspicious Message and User Update System

Fig. 3. Diagram showing the **'Suspicious message identification using NLP'** sub system.

- *Sentiment Score Identification System*: This sub-system gives a sentiment score to the message based on each word weight. A word set from SentiStrength [14] has been used to assign score to each word, this data set contains 2546 words. 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.
- *Sentiment Count Identification System*: Input to this sub-component is message. This subsystem finds the probability of positive and negative sentiment word occurrence in the message passed based on words in a set of 2230 positive words and 3905 negative word [15].
- *Training Set Based Sentiment Identifying System*: This is the most important component in 'Suspicious Message Identification using NLP' system. This sub-system apply sentiment analysis[16] on message and find the sentiment of the message based on training sets. Each topic having positive and negative training set which are collected from different source, such as Recorded Future [17], CNN news [18], The Hindu news [19], Black Friday film [20] and hate speeches of different people [21]. This subsystem uses the results obtained from 'Sentiment Score Identification System' i.e. maximum matching topic, to decide which training set has to be applied to use sentiment analysis. This sub-system uses the probabilistic classifier and the output of this subsystem is sentiment which may be positive or negative.
- *Dictionary Based Topic Identifying System*: Input to this system is message, this sub-component assigns separate matching score to each topic with the help of topic dictionary which was made from topic wise information.

From this we have found topic-wise suspicious message and respective suspicious users. Based on this information details of suspicious database is updated, which is having all the details of suspicious message and suspicious users. Natural Language Processing [22] [23] has been used to flag the message as either suspicious or normal for further processing is done. The pseudo code to find Suspicious message identification using NLP given below.

Algorithm 1. **Pseudo code to find Suspected message By Natural Language Processing**

```
ID ← ProcessedMsgCounter()
for each messageDetails fetched do
    Extract message from messageDetails
    PosSentiScr,NegSentiScr ← findSentiScore(msg)
    PosSentiCnt,NegSentiCnt ← findSentiCount(msg)
    TopicScr ← topicDictionaryBasedScore(msg)
    for each topic in EntireTopics do
        if topic = SpecTopic AND TopicScr ⩾ thld then
            senti ← fndSenti(msg,TopPosFil,TopNegFil)
        end if
        if senti == Negative AND (NegSentiScr < 0 OR NegSentiCnt > 0 ) then
            getUser(MsgID, SpecTopic)
            updateTrainingSet(msg,senti,SpecTopic)
        end if
    end for
end for
ProcessedMsgCounterUpdate()
```

C. Latent Semantic Analysis (LSA)

The proposed system finds group of people who, themselves involved in abnormal activities which is organized with the help of SNS. In that case the message they send and receive are having some similarity even though the messages are not having similar words. So once, one message is found to be suspicious and if other message in network is found which is similar to the suspicious message, then we can group those messages which are having some relationship with each other. This means that those messages are related to the same topic. By using these group of messages, we can find the group of users among whom those messages are exchanged. By this it is possible to identify the group of people who are discussing about the same topic, so that we can identify the group of users, who are involved in same activity as a group. We have used Latent Semantic Indexing (LSI)[24] to identify the similarity between messages, even though they seems totally different. LSI uses the concept of singular Value Decomposition (SVD) [25] to establish the latent relationship between two differently looking words.

D. Suspicious User Identification System

The results obtained from 'Suspicious message identification using NLP' and 'Latent Semantic Analysis' module, are used to identify cluster of suspicious users. The sub components of 'Suspicious user identification system' are Shown in Figure 4.

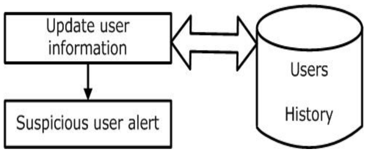

Fig. 4. Diagram show components of **'Suspicious user identification'** system.

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 user information regarding suspicious activities are stored in the database 'Users History'. While analyzing users, those information are fetched from the database; current and previous information are processed to update the suspicious users information. This is done in 'Update user information' sub system. In 'Suspicious user alert' sub section proper decision is made by considering all activities in communication network and by taking a threshold value. Main function of this sub component is to alert about suspicious user for further processing, which is done in 'Visual representation of suspicious users system'.

E. Visual representation of suspicious users

Once system identifies the suspicious users in network, these users and their importance in that network are identified with help of social network analysis and visualization tool Gephi [26]. By using Gephi, 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 message exchanged. By using this tool, we can analyze each users behavior 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 same topic, first we have to find correlation among the messages which are exchanged in network and make the cluster of messages, later from that find the cluster of people. The pseudo code for the same is shown below.

Algorithm 2. **Pseudo code to find Cluster of Users**

```
ID ← msgCounterFetch()
for each each message fetched do
    Extract the messageID from fetched message
    if EntireClust is EMPTY then
        EntireClust ← [messageID]
    else
        msg_Id ← findMaxSimilarMsg(messageID)
        if msg_Id == -1 then
            Add messageID into EntireClust as a SubClust
        else
            for each SubClust in EntireClust do
                if msg_Id == messageID then
                    EntireClust [SubClust] ← msg_Id
                end if
            end for
        end if
    end if
end for
findUserCluster()
msgCounterUpdate()
```

Each message in network uniquely identified by message id, which is generated automatically by the system. Once the system gets message ID of new message which are to be precessed, finds the message ID of the maximum related message which are already processed by using latent semantic indexing and cosine similarity [25]. Then find the respective sender and receivers of message to make cluster of users. The pseudo code for the same is given below.

Algorithm 3. **Pseudo code to find Maximum Similarity Message**

```
Fetch the message from CurMsgId
Fetch all messages except message with ID CurMsgId
for each subgroup of msgs including curMsg do
    for each message in subgroup do
        Remove non-alphanumeric characters
        Remove non-whitespace characters
        Convert to lower case
        Split the string at all whitespace
        Remove stopwords
        Create term-doc matrix for small message group
        Using LSI for message find maxCosineSim score
    end for
end for
if similarity score ⩾ threshold then
    return message ID of Max-similar message
else
    return -1
end if
```

Once we find the correlation between the messages it is possible to form the cluster of message-ID, from this message-ID cluster it is possible to find the respective user cluster.

III. Results and Discussion

By analyzing the network we can study the characteristics of each user in network, for example what is the role of each user in network, their importance and influence to other people in the network. Figure 5, shows the graphical representation of network of all users in our private social networking site 'Manipal Net' where, graph is plotted based on messages exchanged between all users for a duration which is generated by tool Gephi. While analyzing this graph, each node represents users and edge represents the people with whom they communicated. The size of each node is directly proportional to the degree of users that is, with how many people a particular user has communicated. Edge thickness is proportional to the message sent and received between those users. Here interesting thing we can observe is that, in the graph some nodes are grouped together e.g. The group colored with magenta color and the users are 'sathish@yahoo.com', 'sharathmulki@gamil.com' and 'dam@yahoo.com', these user cluster represents how close these users are, that is these users communicated more within this group than the other people in the network, for this reason these users forms one cluster. Similarly in our example five more user clusters are present they are colored with green, dark blue, yellowGreen , red and sky blue.

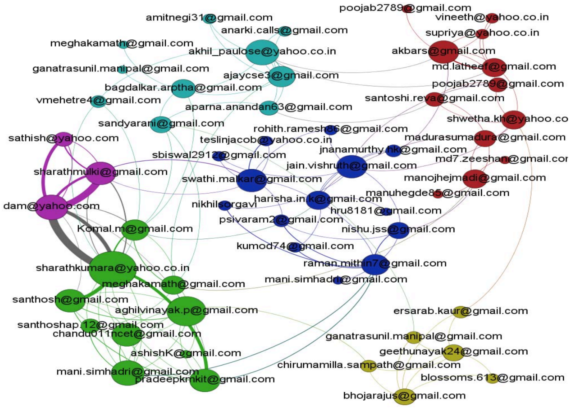

Fig. 5. Diagram shows network of 'Manipal net' private social networking site.

Depending on the message similarity, cluster of message is formed followed by the cluster of users. Figure 6 shows the users clusters formed from the messages which are exchanged in private social network 'Manipal Net'. Here only three group are shown out of many group of this network. In a network each user belongs to one or more group, for example message content of a person who communicate with family members is different as compared to his or her communication with the business partner. So in a network each user's behavior changes depending on the other people with whom they communicate. A single person do normal communication within one group, but in some other group, the same person may be using network to discuss about some abnormal activity.

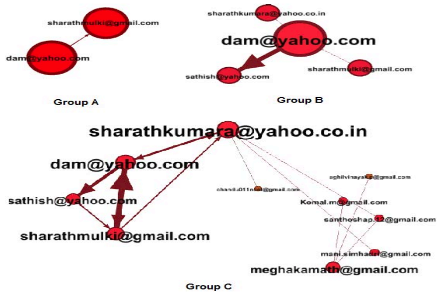

Fig. 6. Diagram shows cluster of users among them same type of message are exchanging.

From Figure 6, it can be observed that, the users 'dam@yahoo.com', 'sharathkumara@yahoo.co.in', 'sathish@yahoo.com' and 'sharathmulki@gmail.com' form one cluster which is shown in Group B. The cluster formed is based on the content of the messages exchanged between these people having similarity, in this cluster user 'dam@yahoo.com' is playing main role, for this reason node size of this user is bigger and the direction of edge leaving from this user node indicates more message is sent by this user. From Group A we can notice that, user 'dam@yahoo.com' and 'sharathmulki@gmail.com' form different cluster, it implies that, messages exchanges between these people have similarity, by that we can predict these people are discussing about some other topic, which is not having any similarity with message exchanged in Group B and Group C user cluster. From this we can get a clue that, the user 'dam@yahoo.com' and 'sharathmulki@gmail.com' discussing some thing different. Here we also see these users are part of Group B and Group C also, it means in this group they discuss something different topics than the topics which are being discussed among Group A user cluster.

From 'Suspicious message identification using NLP' component we will get topic specific user cluster, from LSA component we will get user cluster based on message similarity. By processing these results in subsequent steps, get the cluster of suspicious users in the entire network. Among the topics we selected, most important one is terrorism, Figure 7 shows the cluster of suspected user among them messages exchanging are related to terrorist activity.

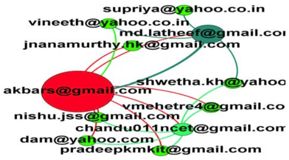

Fig. 7. Suspicious user cluster related to terrorist activity.

Here each person plays different role. The user 'akbars@gmail.com' plays very important role, because of that node size more compared to other people, next is 'md.latheef@gmail.com', then 'chandu011@gmail.com' and so on. One more thing we can observe in this graph edge color distribution, the edge color assigned based on sender node i.e. source node color, for example red color edge represents the message sent from 'akbars@gmail.com' to other users in this cluster, similarly other edges.

Figure 8 shows all the cluster of suspicious users in the entire social network based on different topics which we have considered. Here each sub-cluster is with respect to each topic. Since each person's behave differently with others, one person may participate in different activity in network. For example from the graph we can observe, the user 'akbars@gmail.com' is playing main role in one cluster which is colored with sky blue, and also he is having contact with the other cluster members too. From this analysis we get the information like contacts of each person, what is the role of each person in the cluster, to which cluster the person will fit most etc.

Results obtained from our research work, can be used in applications like, to find suspicious user clusters in social networking site, to study what is the role of individual users in SNS, to find the group of people among them how messages are exchanging etc.

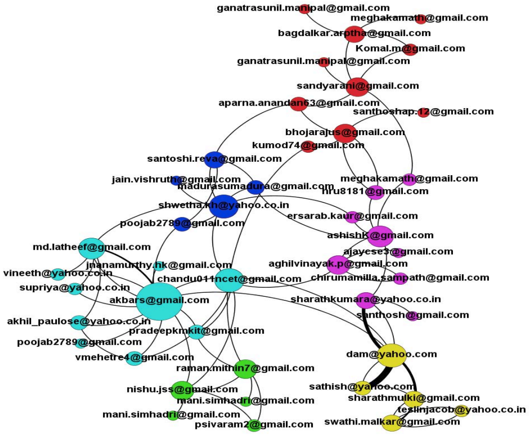

Fig. 8. Diagram shows all suspicious users in the network.

IV. Conclusion

Social networking sites are modern popular platform of communication. However, with all the goodness of online socializing, its power can also be abused for the purpose of illegal activities like planning a terrorist activities or spreading rumors or hate message, do activities which is harmful to the society. In this paper we have 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. So the proposed system can be used by crime investigation agencies.

References

[1] D. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, vol. 13, no. 1-2, Nov. 2007. [Online]. Available: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[2] UNODC, "The use of the internet for terrorist purposes," Report by United Nations Office on Drugs and Crime, September 2012.

[3] R. Frank, C. Cheng, and V. Pun., "Social media sites: New fora for criminal, communication, and investigation opportunities," Research and National Coordination Organized Crime Division Law Enforcement and Policy Branch Public Safety Canada, 2011.

[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] NIA. (2013) National Investigation Agency (NIA). [Online]. Available: http://www.nia.gov.in/

[8] F. J. Fu, J. Chai, and S. Wangl., "Multi-factor analysis of terrorist activities based on social network," *Business Intelligence and Financial Engineering (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. International Symposium on 26-28 Aug. 2008*, vol. 3, pp. 1–8, 2008.

[10] V. Amala Bai and D. Manimegalai, "An analysis of document clustering algorithms," in *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on*, 2010, pp. 402–406.

[11] Skillicorn and David, "Keyword filtering for message and conversation detection," Queen's University.[Available Online] http://www.cs.queensu.ca/home/skill/beyondkeywords.pdf, 2005.

[12] A. A. Sattikar and R. V. Kulkarni., "Natural language processing for content analysis in social networking," *International Journal of Engineering Inventions*, vol. 1, pp. 6–9, September 2012.

[13] R. Layfeild, B. Thuraisinghami, L. Khan, M. Kantarcioglu, and J. Rachapalli., "Design and implementation of a secure social network system," *ISI 2009, IEEE International Conference on , 8-11 June,2009*, 2009.

[14] Sentistrength - sentiment strength detection in short texts. [Available Online]http://sentistrength.wlv.ac.uk.

[15] N. Caren. An introduction to text analysis with python. [Available Online]http://nealcaren.web.unc.edu/.

[16] B. Gokulakrishnan, P. Priyanthan, T. Ragavan, N. Prasath, and A. Perera, "Opinion mining and sentiment analysis on a twitter data stream," in *Advances in ICT for Emerging Regions (ICTer), 2012 International Conference on*, 2012, pp. 182–188.

[17] Recorded future: Creating an insightful world. [Available Online]https://www.recordedfuture.com/.

[18] Voices of the mumbai terror siege: Police taped chilling phone conversations between suicide terrorists and their pakistani handlers. [Available Online]http://transcripts.cnn.com/TRANSCRIPTS/0911/15/fzgps.01.html.

[19] The hindu: Audio of 26/11 tape: Zabiuddin ansari briefs terrorists. [Available Online]http://www.thehindu.com/news/resources/article3568903.ecel.

[20] Black friday:the shocking truth behind the 1993 bombay blast film conversation subtitle. [Available Online]http://www.subtitles.net/en/ppodnapisi/podnapis/i/206775/black-friday-2004-subtitlesl.

[21] Hate speeches by different persons. From Youtube.

[22] D. Jurafsky and S. Bethard, *Speech and Language Processing, An Introduction to Natural Language Processing,Computational Linguistics and Speech recognitionl*. Pearson Education,Inc., 2009.

[23] S. Bird, E. Klein, and E. Loper, *Natural Language Processing with Python*. 1005 Gravenstein Highway North, Sebastopol: OReilly Media, Inc., 2009.

[24] S. Deerwester, S. T. Dumais, G. W. Furnas, T. K. Landauer, and R. Harshman, "Indexing by latent semantic analysis," *JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE*, vol. 41, no. 6, pp. 391–407, 1990.

[25] C. D. Manning, P. Raghavan, and H. Schütze, *Introduction to Information Retrieval*. New York, USA: Cambridge University Press, 2008.

[26] Gephi: Network analysis and visualization. [Online] Available at: https://gephi.org/.