International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9, Issue-7, May 2020

Sentiment Analysis of Social Network Feeds for Threat Protection

Nameer Khan, Aqeel Khalique , Tabrej A. Khan, Imran Hussain

Abstract*: Social Network becomes widely accepted by the users and active communication tool in 21st century. In this paper, we use test data of Twitter, for sentiment analysis. Users may post vulnerable tweets which can result in threats; hence we analyze these tweets to determine threat warnings from specific group of users or organizations. We discuss brief literature review and present our methodology for doing sentiment analysis. We find several users most active and regularly mentioning other users. Based on our results, we present our analysis in the paper. Dataset was requested from Kaggle for research purposes.

Keywords : Sentiment Analysis, Online Threat Protection, Social Network Feeds, Community Protection

I. INTRODUCTION

Social networking sites such as Facebook and Twitter can be a sounding board for the desires, aggravations and pure rage of members. It is easy to let one's emotions get out of control while venting online and comments can be interpreted in ways or to degree that can be considered threatening. It is everyone's right to share their opinion and connect to the world on social media but using technology to threaten and sharing and connecting that may not be considerate is downright deleterious. A simple threat can leave repercussions on multiple lives and it should be considered as an out-an-out coercion. From cyber bullying on personal grudges over internet to radical organization using the same media to fill people with hatred and hence should be monitored. Social network has been connecting people from all around the world. Growth of users on social networking sites has been exponentially since last decade. There are 7.7 billion people in the world, out of this huge population 3.5 billion are online i.e. two out of every three people using internet are connected over social networking platforms. Figure 1 below shows the number of people using social media platforms in 2019. Facebook has 2.3 billion users and Twitter has 330 million users.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Nameer Khan*, Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India. Email: nameer3865@gmail.com
Aqeel Khalique*, Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India. Email: aqeelkhalique@gmail.com
Tabrej A. Khan, Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India. Email: tabrejsmvdu@gmail.com
Imran Hussain, Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India. Email: ihussain@jamiahamdard.ac.in

Social feeds posted by the user have become voice of these users in the digital world [1]. In this paper, we discuss related literature on sentimental analysis of social network feeds in Section 2. In Section 3, we present our methodology and shown implementation in Section 4. Further, we discuss results and analysis in Section 5 and conclude in Section 6.

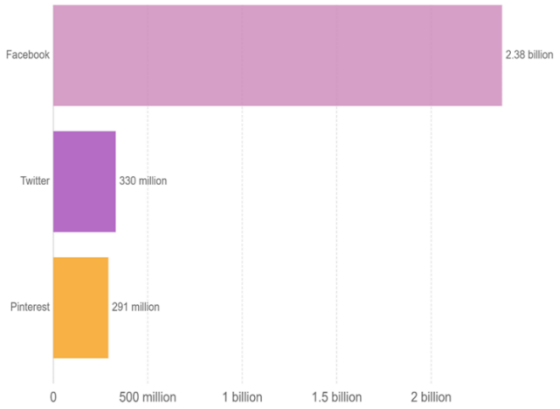

Fig. 1. No of people using Social Media platform, 2019

II. SENTIMENTAL ANALYSIS OF SOCIAL MEDIA FEEDS

In the modern world of today, many organizations have been using social network such as Facebook. Twitter etc. to spread news and using digital marketing to spread propaganda and target the audience. Social networking giants do not have any real countermeasure to identify any person with major suspicious activity. They have to maintain a balance of privacy and security. These social giants ban users, but it is technically difficult to combat violent messages. However, open source analysts' community overcomes these limitations of identifying violent messages. The open source programmers and analysts' community can identify these alarming hidden messages and also raise notification to ensure scrutinized surveillance. Once these messages are identified, action can be taken against the user or the organization and also prevent any threat could have happened into an attack in the very future.

There are certain groups in the entire geography of the world which are funding threat activity and collect huge amount of responses from the users through social network especially social feeds/posts. Hence, these social feeds can be studied or monitored to determine the intention of any person, any group of people or any organizations with malicious intentions.

In this section, we have done a brief literature survey related to sentiment analysis of Twitter feeds called as tweets.

In A. Go et. al. [2], researchers take twitter data with emotion and classified it into positive or negative using machine learning algorithms (Naive Bayes, Maximum Entropy and Support Vector Machines) on the basis of query expression. This paper accuracy is above 80% when trained with emotion data.

In H. Saif et. al. [3], researchers come up with semantic representation of words called SentiCircle. SentiCircle gathers the contextual semantic of words from their co-occurrences. SentiCircle updates the sentiment of words based on their contextual semantics.

They proposed approach on three Twitter datasets using three different sentiment lexicons to derive word prior sentiments. Results show significant performance in accuracy and F-measure for entity-level subjectivity (neutral vs. polar) and polarity (positive vs. negative) detections.

For tweet-level sentiment detection, this approach performs better than the state-of-the-art SentiStrength by 4-5% in accuracy in two datasets, but falls marginally behind by 1% in F-measure in the third dataset.

In A. Muhammad et. al. [4], researchers proposed sentiment analysis model called SMARTA which is lexicon based approach to find sentiment of section of text, in first step polarity from sentiment lexicon is calculated and then by combining polarity of a section of text.

In M. Z. Asghar et. al. [5], researchers proposed framework which combine information theory concepts and revised term weighting measures for predicting and assigning modified scores to domain specific words.

They evaluated the model on subject area specific data. This model try to improve on general knowledge sentiment lexica and have the edge of being comparably robust, while discerning domain-specific words and assigning accurate polarity scores.

In Siegel et. al. [6], researchers performed a separate dataset of over 70 million tweets comprising tweets between February 2015 and April 2016. They explore the effectiveness of the media campaign of the Islamic State and the degree to which the group reaches its aims of gaining a global audience reporting its strategic victories.

In Agarwal et. al. [7], researchers presented a practical approach for analyzing sentiments of tweets by using polarity where text is classified into positive, negative and neutral.

In T. B. Mirani et. al. [8], researchers analyzed hashtags associated with ISIS and captured the sentiment of the tweets. They presented a novel process for sentiment analysis on the ISIS related tweets and to organize the opinions with their geolocations. Jeffrey Breen algorithm was used for sentiment analysis in their research.

III. PROPOSED SOLUTION

In this paper, we have performed sentiment analysis on tweets to determine positive and negative emotions of users. With the help of sentiment analysis, we determined or predicted intention of the user.

The methodology of the proposed solution for doing sentiment analysis on tweets is presented in workflow diagram as shown in Figure 2.

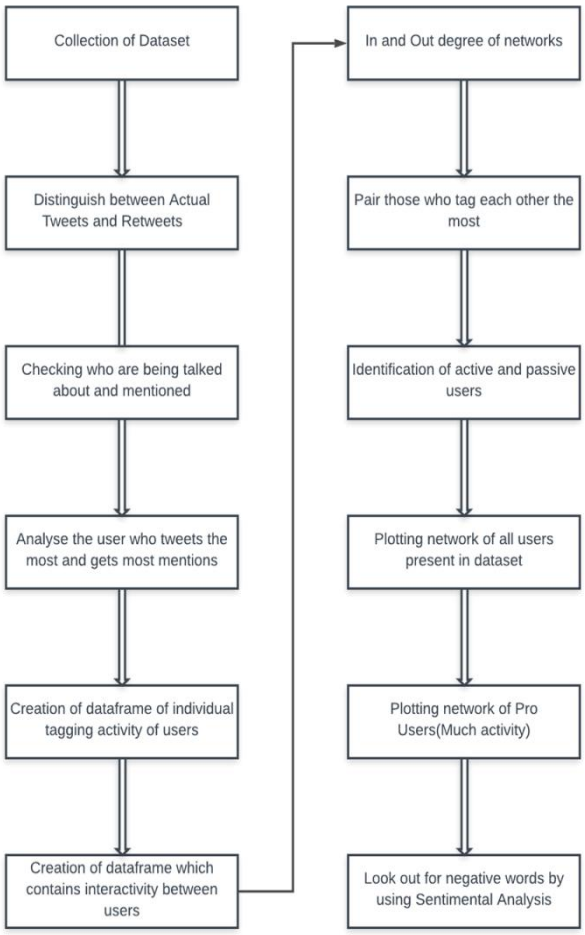

Fig. 2. Workflow Diagram of the Methodology

IV. IMPLEMENTATION

For implementation, we collected over 17,000 tweets from 100+ pro-ISIS fan boys from all over the world since the November 2015 Paris Attacks [9] (Figure 3) from the source agency. In order to maximize our impact, we need assistance in quickly analyzing message frames.

The dataset includes the following:

1) Name
2) Username
3) Description
4) Location
5) Number of followers at the time the tweet was downloaded
6) Number of statuses by the user when the tweet was downloaded
7) Date and timestamp of the tweet
8) The tweet itself

The general approach is to isolate every single user to serve as a node by their username. The username has been chosen as the associated data for each node [10]. A combination of the number of followers and the number of tweets they produce will influence the node scale. This combination will ensure the identification of active and popular users rather than identifying those who tweet a lot and have a small number of followers or vice versa. The

name	username	description	location	followers	numberstatuses	time	tweets
War BreakingNews	warrnews	we provide fresh news from every battlefield	world	7271	6872	3/7/2016 11:30	RT @Hamas_Mujahid_: 7/03/2014.\n\nBritish #Ham...
كتكات كوكونة	Uncle_SamCoco	Here to defend the American freedom and also ...	Texas, USA	1772	5304	4/13/2016 22:30	@Metammorph vous etes un mélange de Ali-Baba e...
Ibn Kashmir	IbnKashmir_	Preparing For Gazwa-e-Hind	Wilayah Kashmir	71	28769	3/25/2016 9:06	RT @x_need1: #وكالة_أعماق فصائل المعارضة السور...
Anaksabil97	nvor85j	NaN	NaN	238	133	5/12/2016 11:29	#Breaking\nSyrian regime tank destroyed and it...
Rain Qattal	1515Ummah	21:15 For they fled from the Swords, from the ...	Punch, Jammu And Kashmir	214	169	2/17/2016 21:51	RT @malle111elf: Aamaq:\n#IS fighters killed 1...

Fig. 3. Sample of Dataset

relationship between each user is determined at the moment, as well as the number of followers, as these followers will be useful in defining the relationship between the different users. One relationship criterion can be scrapping user tweets for mentions and then linking nodes via this metric to multiple mentions that increase the weight of an edge between two users.

We use Matplotlib [11] to provide statistical visualizations gathered from the data and NetworkX [12], a useful graph library that allows graphs to be visualized. NetworkX drawing functions are linked directly to Matplotlib so that similar visualizations can be created.

The first interesting statistic is to determine how many users tweet each other in the dataset. The first two print commands will verify that there are no duplicate tweets that would distort outcomes. The only drawback is that it is based on an exact string match, if the retweets were followed by an RT then the duplicates would not be picked up.

Using a regex expression, we can capture and count those tweets which contain 'RT' at the beginning of the tweet (indicating a retweet). Compared with the previous check, we can see that approximately 6000 tweets are not really useful because they are retweets as seen in Figure 4. Given this, they are useful in checking which connection criteria to use for future reference.

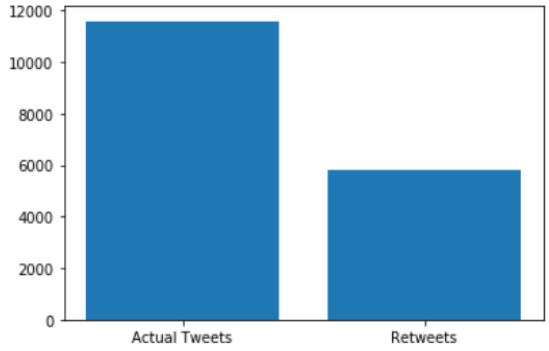

Fig. 4. Seperation of Retweets and Actual Tweets

Initially, retweets and actual tweets have been separated and then actual tweets are grouped with their usernames so as to perform sentiment analysis. The amount of interactions of a tweet enables us to make a statement about its influence. Hashtags are used to generate groups of tweets and to tag important keywords. New trends can be identified by monitoring frequently used Hashtags on Twitter [13].

Further, we iterate from them through any username listed in tweet and scrapped tweet (where the user does not mention them himself). Such usernames are then calculated whether or not they are users from within the dataset. From the bar chart below in Figure 5 (a), it is clear that most of the users listed are outside dataset's reach. Hence, as this is a smaller group of users to deal with, we should concentrate on those found only within the dataset.

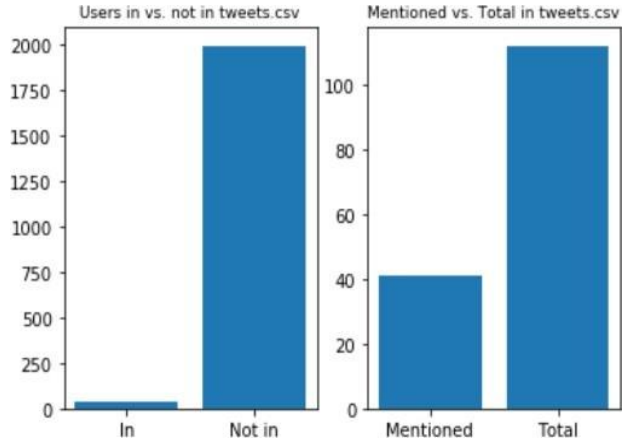

Figure 5 (a) Users in tweets or not, (b) Contrast between users mentioned in tweets or not

Figure 5 (b) shows how many users in the dataset have been mentioned by other users within the dataset. There is a reasonable amount of communication between these different set of users.

V. RESULTS AND ANALYSIS

To determine the most influential (most tweeted) users, we need to count how many times they are mentioned. This is done via counting the in_set list, as can be seen below the most tweeted user currently is 'Rami' as shown in Figure 6. Initially, 'WarReporter1' was the most tweeted user but after removing tweets where the sender and receiver was same user, count has dropped drastically.

By checking the description of the top 5 receivers, we find that they are mostly "unbiased" news sites.

1.Username:RamiAlLolah - Real-Time News, Exclusives, Intelligence & Classified Information/Reports from the ME. Forecasted many Israeli strikes in Syria/Lebanon. Graphic content.

2.Username:Nidalgazaui - 17yr. old Freedom Activist/Correspondence of NGNA /Terror Expert/Middle East Expert. Daily News about Syria / Iraq / Yemen / Middle East

3.Username: MilkSheikh2 - Muslim, Iraqi, Banu Zubid, Qahtani, Chef, Engineer, remaining until the best of them, Figure hts al-Dajjal, Translate Old stuff mostly

4.Username: WarReporter1 - Reporting on conflicts in the MENA and Asia regions.

5.Username: _IshfaqAhmad - Medico at GMC Srinagar • Pro-Khilafah • Anti-Democratic • Anti-Nationalistic • Anti-Rafidah • Innocent Bystander of the Conflict in Middle East • Cricketist

```
[('MaghrabiArabi', 49), ('WarReporter1', 30), ('AsimAbuMerjem', 27), ('Uncle_SamCoco', 27), ('moustiklash', 20)]
[('RamiAlLolah', 53), ('Nidalgazaui', 34), ('MilkSheikh2', 26), ('WarReporter1', 15), ('_IshfaqAhmad', 15)]
```

Fig. 6. Top 5 senders and receivers respectively

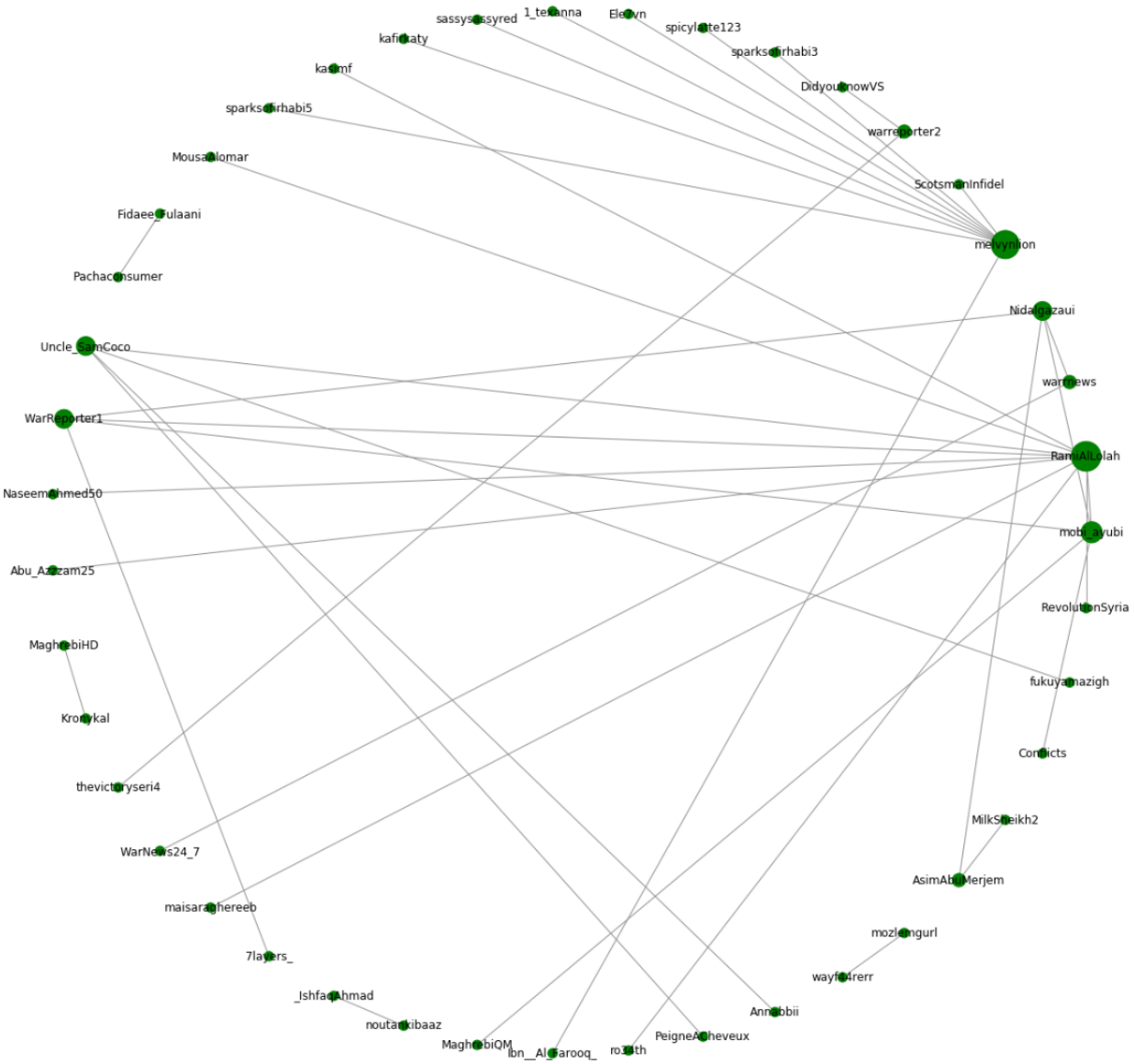

Fig. 7. Passively involved users visualisation.

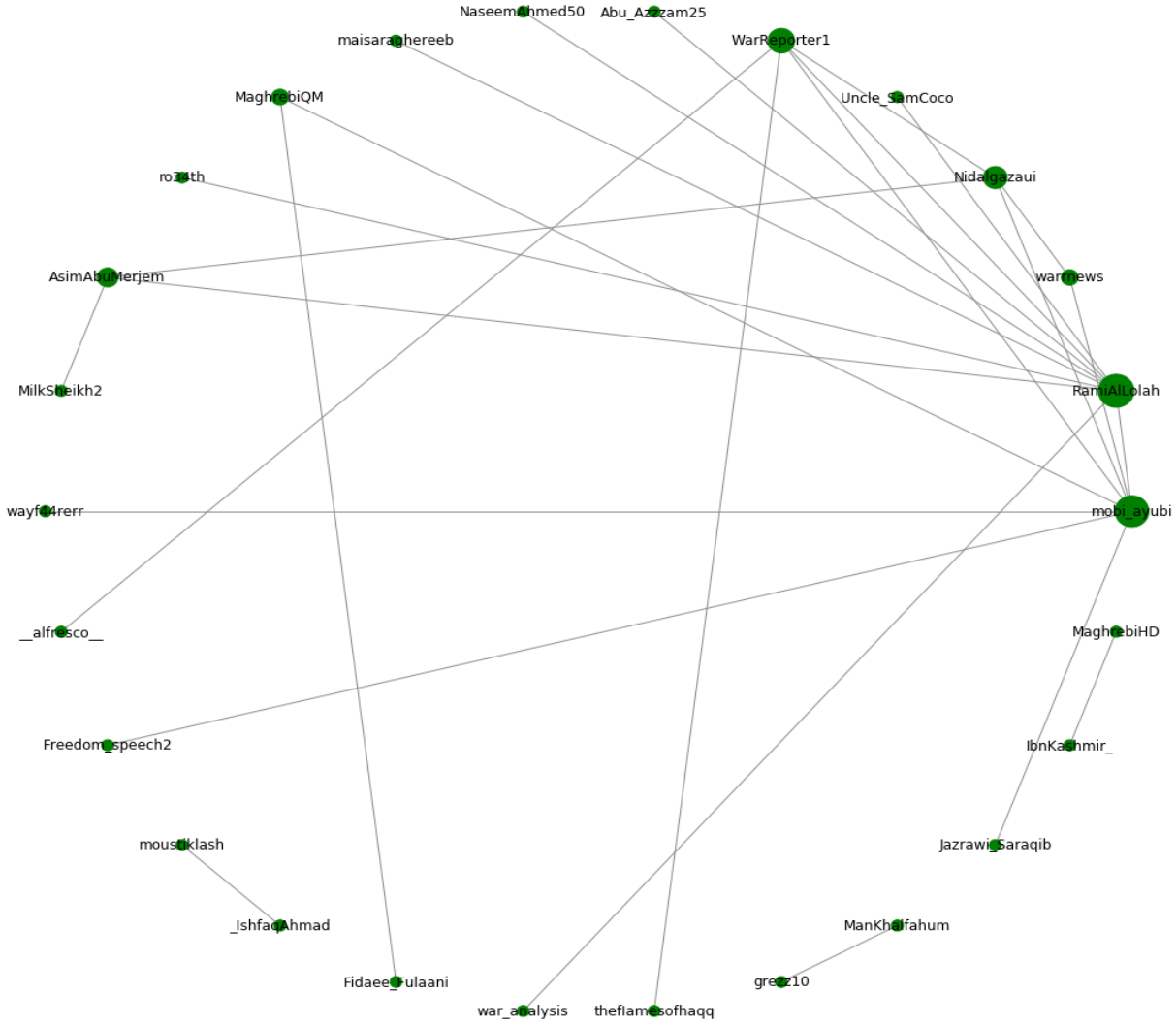

Fig. 8. Actively involved users visualisation.

In obtaining the results, we first create a data frame which contains the information of individual tagging activities in each row. Then, a similar data frame is created that only contains the interactivity between users in the data frame. It is done to determine how many times a user mentions other users and how many times a user is mentioned other users. For targeting the malicious user, in and out degree on social media is a helpful indicator. In ISIS social networks, both actively and passively involved should be paid with attention. User 'melvynlion' always tag the other user in tweets as shown in Figure 9.

Now, data can be visualised and observed for passively involved ISIS twitter handlers by plotting a weighted graph as shown in Figure 7 using NetworkX. In Figure 7, some nodes have really intensive links from/to the other users such as 'RamiAlLolah', 'WarReporter1' and 'Melvynlion'.

Further, from the graph obtained in Figure 7, we can determine passively connected users to each other. We have shown in Figure 10 by clustering to determine which users are connected to whom and shown a network graph between them in Figure 8.

	Mentions	User	Weight
0	RamiAlLolah	mobi_ayubi	195
1	Nidalgazaui	warrnews	184
2	ScotsmanInfidel	melvynlion	79
3	DidyouknowVS	warreporter2	70
4	sparksofirhabi3	melvynlion	63
5	spicylatte123	melvynlion	61
6	Ele7vn	melvynlion	58
7	1_texanna	melvynlion	56
8	sassysassyred	melvynlion	54

Fig. 9. The 10 most frequent tagged user pairs.

Also, we determine tweets and opinion of most active users by doing sentiment analysis. By capturing the negative words used by these users, if they have been using these negative words more often, then there is a need to put these users under surveillance. For analysis, “tidytext” package in the notebook for tokenization is used and joined with lexicon “bing” to classify the tokens as positive and negative [14] as shown in Figure 11 and Figure 12.

Word count of words like ‘attack’, ‘killed’ is very much high. This might give exclusive important information about the intention of these users.

The word ‘holy’ has also been used maximum times because these target young audience to recruit in their organization on the basis of religion by using positive exclamations.

	Mentions	User	Weight
0	RamiAlLolah	mobi_ayubi	195
1	Nidalgazaui	warrnews	184
2	Nidalgazaui	mobi_ayubi	45
3	RamiAlLolah	Uncle_SamCoco	40
4	WarReporter1	mobi_ayubi	38
5	RamiAlLolah	Abu_Azzzam25	34
6	RamiAlLolah	NaseemAhmed50	34
7	RamiAlLolah	WarReporter1	32
8	RamiAlLolah	maisaraghereeb	28

Fig. 10. Most frequent tagged user pairs actively involved.

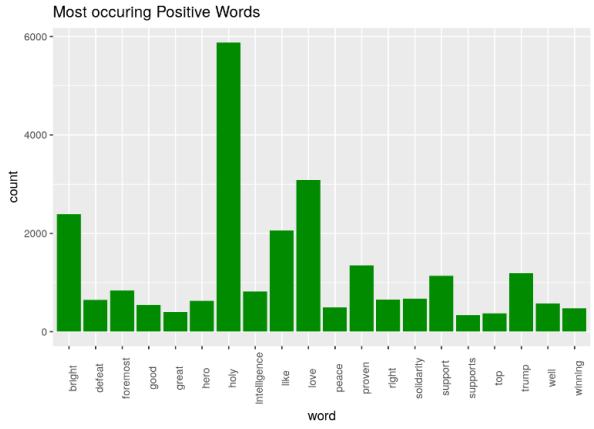

Fig. 11. Most occurring positive words.

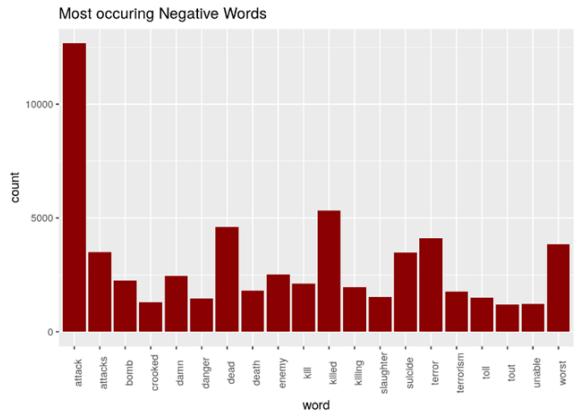

Fig. 12. Most occurring negative words.

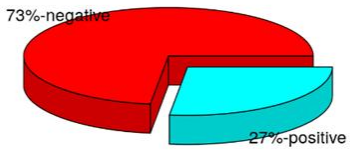

Fig. 13. Percentage of positive and negative words in the tweets.

Hence, Figure 13 shows percentage of positive and negative words in the tweets and top 10 words contributing to different sentiments can be visualised as shown in Figure 14.

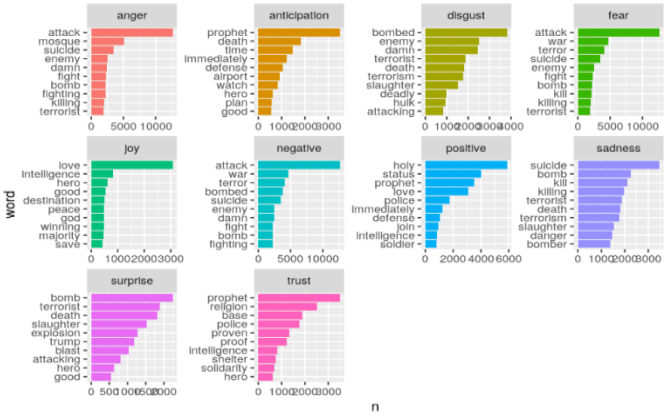

Fig. 14 Actively involved users’ visualisation.

Analysis has been performed on negative and positive sentiment for our test data of ISIS tweets. The most interesting insight determine from the implementation is small number of users are primarily thought leaders and network influencer. Some users generate the content, share and act as connections between content producers and content recipients. We need to find these users and monitor their suspicious activity. We will be able to monitor major social networking organisation such as Facebook, Twitter etc. The research determines suspicious activity on historical data will be tested on run time data as well which may lead to huge success on our result. By analysing big data, one can look at the whole picture and not just covering a single incident, like the unfortunate incident of Paris attack being covered far more enormously by CNN and Al-Jazeera. By keeping a check on real time dataset, we might be able to predict to an extent anything suspicious that may happen in the near future. Moreover, by studying a country specific and culture specific views on any organisation, we might be able to study how these organisations respond on the same and may distinguish between the negative, positive or neutral attitude of these organisations.

VI. CONCLUSION

Social network now become a platform where any user can raise up its voice or opinion which can be noticed by other users who are following them. In this paper, we have accessed test data of Twitter posts called as 'tweets'. We have performed sentiment analysis on these tweets for identifying vulnerable, malicious or threat containing tweets. Users posting these malicious tweets are often part of dangerous or suspicious organizations and many a times malign or misled other users who are following them. These users are influencers and they must be kept on high surveillance for any suspicious tweets. In implementation, we use Matplotlib and NetworkX for identifying active and passive users (who retweet). Further, we determined most frequent tagged pairs who are actively involved. Lastly, we did sentiment analysis for identifying most occurring positive and negative words. Hence, we visualized actively involved users with malicious intention or threatening tweets. Once these users are identified, it is relatively easy for monitoring personnel to catch these users and protecting the community from threats of specific group of users.

REFERENCES

1. M. Mazarr, R. Bauer, A. Casey, S. Heintz, and L. Matthews, "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment," 2019.
2. A. Go, R. Bhayani, L. Huang, "Twitter sentiment classification using distant supervision"CS224N Project Report, Stanford ,2009.
3. H. Saif, Y. He, M. Fernandez, and H. Alani, "Contextual semantics for sentiment analysis of Twitter," Information Processing & Management, vol. 52, no. 1, pp. 5–19, 2016.
4. A. Muhammad, N. Wiratunga, and R. Lothian, "Contextual sentiment analysis for social media genres," Knowledge-Based Systems, vol. 108, pp. 92–101, 2016.
5. M. Z. Asghar, A. Khan, S. Ahmad, I. A. Khan, and F. M. Kundi, "A Unified Framework for Creating Domain Dependent Polarity Lexicons from User Generated Reviews," Plos One, vol. 10, no. 10, 2015.
6. A. A. Siegel and J. A. Tucker, "The Islamic State's information warfare," Journal of Language and Politics Re/constructing Politics Through Social & Online Media, vol. 17, no. 2, pp. 258–280, 2017.
7. A.Agarwal, B. Xie, I.Vovsha, O.Rambow,and R.Passonneau,"Sentiment Analysis of Twitter Data," in Proc of ACL HLT Conf, 2011.
8. T. B. Mirani, S. Sasi, "Sentiment Analysis of ISIS Related Tweets Using Absolute Location," 2016 International Conference on Computational Science and Computational Intelligence (CSCI), 2016.
9. Find Open Datasets and Machine Learning Projects. Retrieved from https://www.kaggle.com/datasets. [Accessed: 31-Mar-2020].
10. Wisdom, Vivek. (2016). An introduction to Twitter Data Analysis in Python. 10.13140/RG.2.2.12803.30243. "(PDF) An introduction to Twitter Data Analysis in Python."[Online]. Available:https://www.researchgate.net/publication/308371781_An_introduction_to_Twitter_Data_Analysis_in_Python. [Accessed: 31-Mar-2020].
11. Visualization with Python. Retrieved from https://matplotlib.org/
12. Hagberg, Aric &Swart, Pieter &Chult, Daniel. (2008). Exploring Network Structure, Dynamics, and Function Using NetworkX. Proceedings of the 7th Python in Science Conference. "Exploring Network Structure, Dynamics, and Function using ..." [Online]. Available: http://conference.scipy.org/proceedings/scipy2008/paper_2/full_text.pdf. [Accessed: 31-Mar-2020].
13. S. D. Ruhrberg, G. Kirstein, T. Habermann, J. Nikolic, and W. G. Stock, "#ISIS—A Comparative Analysis of Country-Specific Sentiment on Twitter," Open Journal of Social Sciences, vol. 06, no. 06, pp. 142–158, 2018.
14. J. Silge and D. Robinson, "tidytext: Text Mining and Analysis Using Tidy Data Principles in R," The Journal of Open Source Software, vol. 1, no. 3, p. 37, Nov. 2016.

AUTHORS PROFILE

Nameer Khan currently pursuing B.Tech in Computer Science Engineering from Jamia Hamdard, New Delhi. His interest includes Data Science and Analytics.

Aqeel Khalique completed his M.Tech. in CSE from IIT Roorkee. Aqeel has several publications in domain such as Information Security, Pervasive Computing, IoT, Scalable Security, Sustainable Computing etc. Aqeel is currently working as Assistant Professor in Deptt. of CSE, Jamia Hamdard, New Delhi. Aqeel is in Editorial Board of International Journal of End-User Computing and Development (IJEUCD). Aqeel is also member of many research bodies such as ISTA, ACM etc.

Tabrej A. Khan completed his M.Tech. in Information Security from NIT Jalandhar. Tabrej has publications in domain such as Information Security, Image Processing, Data Science and Analytics, Sustainable Computing etc. Tabrej is currently working as Assistant Professor in Deptt. of CSE, Jamia Hamdard, New Delhi. Tabrej is also member of many research bodies such as ISTA, ACM etc.

Dr. Imran Hussain, Ph.D., is an Assistant Professor in the Department of Computer Science and Engineering at Jamia Hamdard (New Delhi). His research interests include Cloud Computing, Cyber Security, Big data, analysis, and CPS. He has focused in the last few years on analysis, designing, and performance evaluation of e-learning platforms and their integration with open source tools. He has published in international journals and conferences. He is associated with ACM, CSTA, EAI.