Detection of the spread of terrorism using Social media

Vishwadish Desale[1], Shubham Patil[2], Dr. Suvarna Pansambal[3]

[12](Student, Department of Computer Engineering , Atharva College of Engineering/Mumbai University, India)

[3](Assistant Professor, Department of Computer Engineering, Atharva College of Engineering/Mumbai University, India)

Abstract-

Terrorist groups have increasingly used social media to further their goals and spread their message. Social media allows them to engage with their networks. Terrorism using the social media, has become one of the most concerning issues across the world. Social media has helped in spreading their ideological thoughts, propaganda and their activities across the world.

1. Introduction

Terrorism, using the social media, has become one of the most concerning issues across the world. There is interplay between home-grown terrorist groups and international terrorist organisations which is playing the central role in accelerating the situations. Terrorist organisations are using social media platforms for recruiting, training and communicating with their followers, supporters, donors, as it is cheaper, easier, faster and effective method of communication. The members of the terrorist organisations are spreading their ideological thoughts, propaganda and their activities across the world, using social media platforms. It is approximated that around 90% of the members of ISIS were recruited through social media.
There are lots of people are directly or indirectly affiliated with terrorist organisations who are on Twitter. They openly tweet in favour of these organisations. Thus it is important to track them down. Thus, the objective of this project is to detect key player in the detection in terrorism.

2. Review of Literature

Key Player identification In Terrorism-related Social Media Networks Using Centrality Measures:

This proposed method first created a social network of Twitter users with the keywords used by the Caliphate state propaganda. The method then used Mapping Entropy Betweeness (MEB), to find the most influential player in the created network. [1,2]

Detecting Key Player In Terrorist Network:

This method again created a social network of Twitter users with the help of provided keywords. It then finds the central figure by applying different centrality measures to find the central player of the network.

Twitter data analysis: temporal and term frequency analysis with real time event:

This paper discussed about different twitter APIs used for accessing real time tweets, user profile and data mining techniques to extract relevant data from raw data of tweets. Further, we performed temporal and term frequency analysis on the extracted data, which shows the most happening events of the match as well as most popular keywords that were used.

Key Player Detection Algorithm:

Betweenness Centrality:

Betweeness centrality plays an important role in analysis of social networks, computer networks , and many other types of network data models. In the case of communication networks the distance from other units is not the only important property of a unit. What is more

important is which units lie on the shortest paths (geodesics) among pairs of other units. Such units have control over the flow of information in the network. Betweenness centrality is useful as a measure of the potential of a vertex for control of communication.
Betweenness centrality indicates the betweenness of a vertex in a network and it measures the extent to which a vertex lies on the shortest paths between pairs of other vertices. In many real-world situations it has quite a significant role. Determining betweenness is simple and straightforward when only one geodesic connects each pair of vertices, where the intermediate vertices can completely control communication between pairs of others. But when there are several geodesics connecting a pair of vertices, the situation becomes more complicated and the control of the intermediate vertices gets fractionated.

The concept of betweenness centrality was first introduced by Bavelas in 1948. The importance of the concept of vertex centrality is in the potential of a vertex for control of information flow in the network. Positions are viewed as structurally central to the degree to which they stand between others and can therefore facilitate, impede, or bias the transmission of messages. Freeman in his papers classified betweenness centrality into three measures. The three measures include two indexes of vertex centrality—one based on counts and one on proportions—and one index of overall network or graph centralization.

Betweenness centrality $C(B)v$ for a vertex v is defined as ,
$C(B)v = \sum \sigma st(v)/\sigma st$

3. Proposed System

In this paper, we presented a framework for detecting key players from twitter data, for a certain set of keywords.
Employing real-world twitter data as the basis, we performed a 360 degree analysis of the types of tweets from terrorists, relationship between the other users. To fully leverage social media content and social information of users' tweets, we proposed a model which uses the algorithm of betweeness centrality to detect key players in a network. After researching we have discovered several intriguing phenomena. We found that a good number of users were already blocked by twitter due to their tweets. This goes to show that our system is on the right path. The results show that the proposed model is effective and efficient on detecting the spread of terrorism on social media.

There are many people who tweet openly with keywords supporting or endorsing terrorist organisations. The system that has been developed first stores all the tweets fetched for certain keywords in a file. From there we analyse them and perform certain actions.

i) Find key players from the network
ii) Perform time-frequency analysis and display a graph
iii) Display heat map of the locations mentioned tweets
iv) Display a graph showing nodes which represent the users and the entire network

3.1 System Architecture

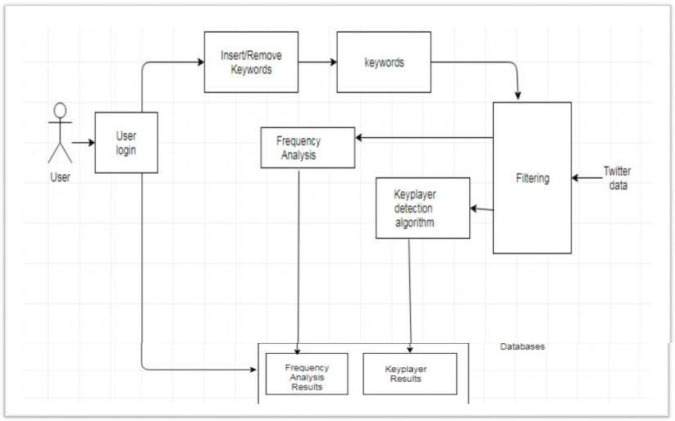

Fig.1

3.2 DFD

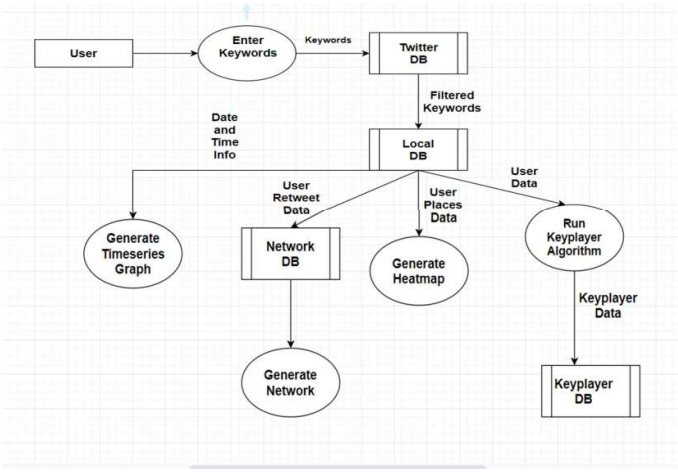

Fig.2

3.3 Use Case

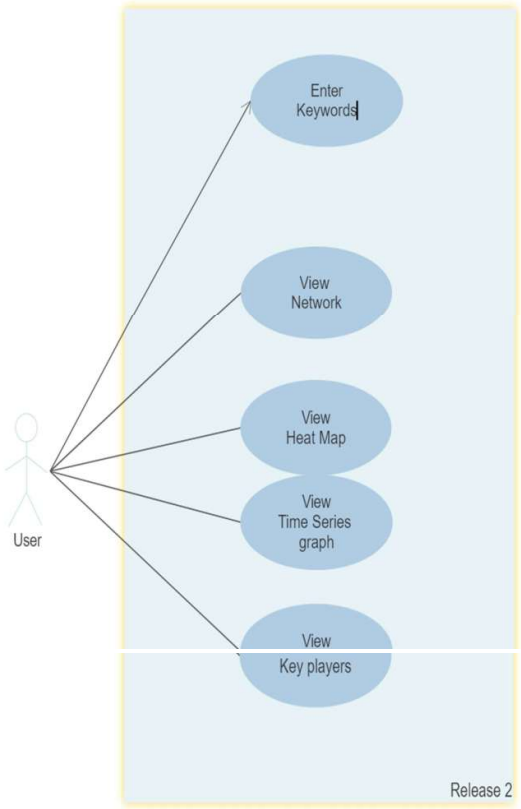

Fig.3

4. Result and Analysis

4.1 List of Key Players:

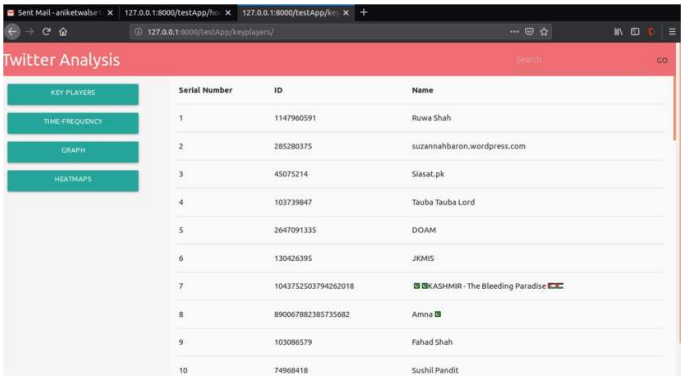

Fig.4

The first part of the system gives the list of key players involved. Here the list is arranged in descending order of the scores calculated. There are 3 columns here, serial number, ID and the name. Serial number is unique for every user ID is the actual Twitter ID of the user name is the name of the user used on twitter.

4.2 Search Information:

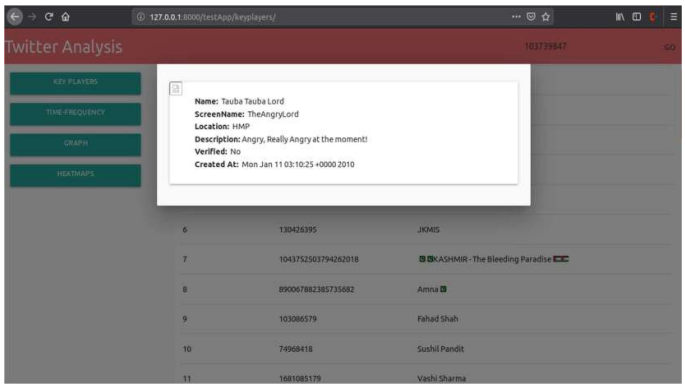

Fig.5

At the home page, there is a search bar. We can enter the id of any user we want from the key player list. After we select "go", complete information of the user is displayed.

It shows:
Name of the twitter user.
The screen name of the user.
The location of the user.
The description of the account.
It shows whether the account is verified or no, and also gives the date of creation.

4.3 Time- Frequency Analysis:

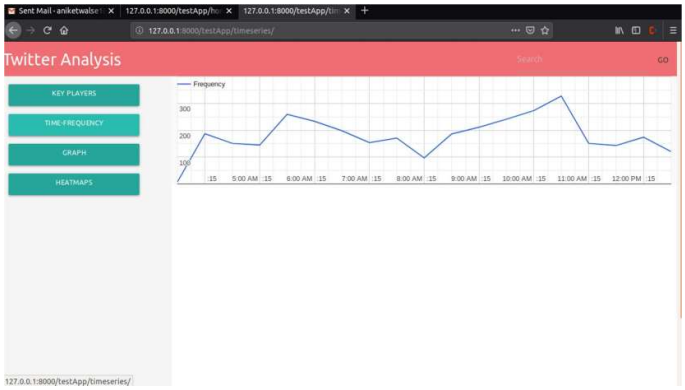

Fig.6

It gives number of words count with respect to time in whole file. From, term frequency analysis we can check the words that are commonly and most frequently used

by users and become trendy for that real-time event. From these terms, we can also see the ranking of players by popularity. It is an important factor for the people to understand the key influencers on social media platform while searching. That is why, this analysis is carried out. Our analysis shows the graph of trending frequency terms with respect to the time as shown in the figure. Also we can use this analyze the tweets pre and post an event and may actually also predict if an event may occur in the future.

4.3 Graph:

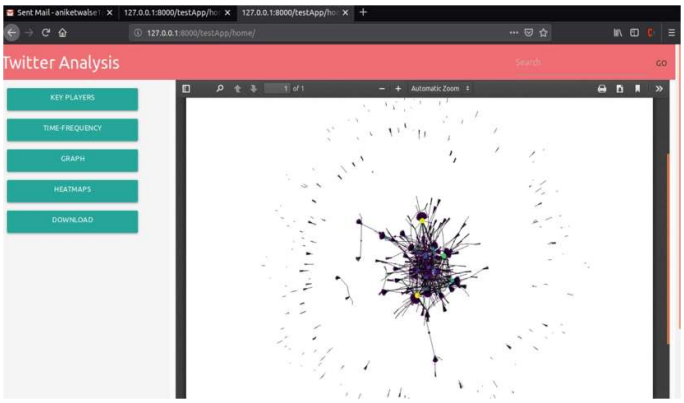

Fig.7

The above figure shows the different nodes and the relationship between these nodes. The nodes shown here are the twitter users. The unique twitter id is written on every node. An edge is formed between the nodes when a user retweets the tweet of the other user. Due to this we get a huge network of tweets. The nodes are represented with different colors. The node which is the most influential is shown by a dark purple color.

5. Future Scope:

We can use to system to detect fake news. We can use keywords of the fake news and we can block the accounts which are playing an important role in spreading it. The system can find out who is spreading rumours by giving keywords related to the rumours. This
can then find the most influential account which is spreading the rumours. Big business organizations can use the system to detect the social media trends and analyse the connections between the nodes. They can then predict as to who is most likely to but their products.

6. Conclusion

In this paper, we presented a framework for detecting key players from twitter data, for a certain set of keywords. Employing real-world twitter data as the basis, we performed a 360 degree analysis of the types of tweets from terrorists, relationship between the other users. To fully leverage social media content and socialinformation of users' tweets, we proposed a model which uses the algorithm of betweeness centrality to detect key players in a network. After researching we have discovered several intriguing phenomena. We found that a good number of users were already blocked by twitter due to their tweets. This goes to show that our system is on the right path. The results show that the proposed model is effective and efficient on detecting the spread of `terrorism on social media.

7. References

i) Detecting Key Players in Terrorist Networks
Berzinji, A., Kaati, L., & Rezine, A. (2012). Detecting Key Players in Terrorist Networks. 2012 European Intelligence and Security Informatics Conference. doi:10.1109/eisic.2012.13
https://ieeexplore.ieee.org/document/6298852

ii) Key player identification in terrorism-related social media networks using centrality
measures
Ilias Gialampoukidis, George Kalpakis, Theodora Tsikrika, Stefanos Vrochidis and Ioannis Kompatsiaris Information Technologies Institute Centre for Research and Technology Hellas
https://ieeexplore.ieee.org/document/7870202

iii) Twitter data analysis: temporal and term frequency analysis with real-time event
Garima Yadav, Mansi Joshi and R Sasikala
https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042081

iv) Social network analysis of terrorist organizations in India
Aparna Basu
(https://www.researchgate.net/publication/228962297_Social_network_analysis_of_terrorist_organizations_in_India)