SURVEY ON SHAMING SENTENCE DETECTION ON SOCIAL NETWORK

Sapana Chavanke[1], Avanti Soonawane[2], Bhavana Pandey[3],Piyush Kumar[4], Mrs.Aseema Jana[5]

[1,2,3,4]UG. Student at Of computer Engineering, Dr DY PATIL SOET, PUNE

[5]Professor at Dept. Of computer Engineering, Dr. D. Y. Patil SOET - DYPSOET, Pune

-- ***--

Abstract: - Now a day's social platform are becoming an main part of life. Almost everyone with smart phone using online social network. Terrorist organizations use different social media as a tool for spreading their views and influence general people to join their terrorist activities. Twitter is the most common and easy way to reach mass people within a small amount of time. In this paper, we have focused on the development of a system that can automatically detect terrorism-supporting tweets by real-time analyzation. In this system, we have developed a frontend for real-time viewing of the tweets that are detected using this system. We have also compared the performance of two different machine learning classifiers, Support Vector Machine (SVM) and Multinomial Logistic Regression and found the first one works better. As our system is highly dependent on data, for more accuracy we added a re-train module. By using this module wrongly classified tweets can be added to the training dataset and train the whole system again for better performance. This system will help to ban the terrorist accounts from twitter so that they can't promote their views or spread fear among general people.

KEYWORDS: *Terrorism, Social Network, Attacks, Performance Analysis*

---***---

I INTRODUCTION

One of the most important threats to today's civilization is terrorism, which has affected the quality of lives of people in the whole world [1]. Terrorism means the use of intentional indiscriminate and illegal power and violence for creating terror amongst general population in order to gain some political, monetary, religious, or legal objectives. The definition of terrorism according to Hoffman [2] is "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change." The objectives of terrorism are to create instability by creating fear, anxiety, and uncertainty on a larger scale compared to a single individual. According to Global Terrorism Database (GTD), in 2019 alone 1,411 different terrorist attacks have happened, causing 6,362 fatalities and badly affecting the quality of life of individuals in the society. A visualization of world map showing different terrorist activities is given in Figure 1 (image source: https://www.start.umd.edu/gtd/). The orange color shows high intensity value as a combination of incident fatalities and injuries. The map shows a very high rate of terrorism in South Asia and the Middle East.

The response of terrorist events is constant sense of fear, feeling helpless, experiencing fear and anger, and intolerance or aggression towards certain ethnicity or religious groups. It is equally important that the emotional reactions of the population is understood in regard to terrorist events so that we are able to design assistance to effectively help those who are suffering

from these issues or they do not react to carry out another terrorist activity as a revenge. Terrorism has been studied for decades to understand the major factors causing the act of terrorism or understanding how to perform counterterrorism or understanding the social and economic effects of terrorism [3, 4]. However, because of the complex nature of terrorism, it is difficult to find an effective solution that can be used as a counterterrorism to protect the lives of individuals. Identification of terrorist ideologies and prediction of future terrorist attacks have been proven to be of great importance and time-consuming process.

Machine learning algorithms have been used recently to study the different factors of terrorism [5, 6]. NN and particularly DNN are getting popularity mainly because of the fact that a huge amount of labelled data is available recently. The advancements in computer technologies [7–9] have been able to create much powerful computer systems to perform the required computation in DNN. In this paper, NN and DNN models are used to make predictions of different factors that lead to terrorist activities. The model is helpful for law enforcement agencies to make prediction before an incident actually happens and potentially causes the loss of precious lives. The predicted factors are explained below.(i)Suicide: to predict whether a terrorist activity is going to be suicide or not.(ii)Success: to predict whether a terrorist activity will succeed or not.(iii)Weapon type: to make a classification of the general type of weapons used in terrorist activity.(iv)Region: to classify the region that will be targeted by the terrorist

activity.(v)Attack type: to classify the type of attack carried out as a terrorist activity.

These predictions are important to understand in order to perform counterterrorism. Deep learning can make these predictions efficiently and can help law enforcement agencies to devise mechanisms to deal with terrorists and protect the lives of individuals. With the help of these tools, a terrorist activity can be stopped before it can actually happen and make destructions in terms of lives, infrastructure, or law.

II LITERATURE REVIEW

Sr. NO	Year	Paper Title	Author	Description
1	JUNE 2018	Examining Convergence Behaviour During Crisis Situations in Social Media- A Case Study on the Manchester Bombing	M.Mirbabaie, D.Bunker,A.De ubel and S.Stiegliz{International Conference on TDIT 2018, Portsmouth, UK }	A model to predict information flow size and survival was developed by [1], with the help of data fetched from one of the popular social networking website Twitter. The information flow size and survival were modeled using zero truncated negative binomial (ZTNB) regression method and Cox regression technique respectively. Using a sample of 427,330 Twitter data, they reported a novel outcome that identified the sentiment expressed in the tweet which was found to be statistically predictive of both size as well as survival of information flows of such nature.
2	2018	Cyberhate on social media in the aftermath of Woolwich: A case study in computational criminology and big data	M. L.Williams Burnap {British Journal Criminology}	In a similar study, [2] reported how investigation of an open source communications data gathered through social media platforms could elucidate the inter and inter community conflict dynamics, surfacing in the wake of such unfortunate events. They claimed that the Twitter data gathered after the murder of Fusilier Lee Rigby, convincingly supports the Collins three phases of conflict dynamics.
3	2018	Ten Rs of Social Reaction:Us ing Social Media to Analyse the Post-Event Impacts of the Murder of Lee Rigby, Terrorism& Political Violence	Martin Innes, Colin Roberts, Alun Preece and David Roggers{ESRC}	Analysis of social reactions to the murder of Lee Rigby, was studied by [4] using data collected by systematic monitoring of twitter. They investigated a number of online behaviors with offline effects.
4	2019	Tracking Changes in Resilience and Level of Coordination in Terrorist Networks	Vasanthn Raghavan,& Alexander G. Tartakovsky {IEEE }	In this paper, they pursue an alternate statistical nonparametric approach for spurt detection in activity profiles. the approach is based on binning the count data of activity to form observation vectors that can be compared with each other. Motivated by a MAJORIZATION theory framework, these vectors are then transformed via certain functionals and used in spurt detection and classification.

III PROPOSED SYSTEM

Proposed system is working as steps given below:

Step 1: Twitter Data collection using twitter streaming API and Facebook comments collection using online tools like extractcomments.com, etc.

Step 2: Tweets/Data cleaning like removal of duplicate tweets, stop words.

Step 3: Data normalization using porter stemming algorithm.

Step 4: Data loading on Dataset.

Step 5: Design and Implementation of map reduce program for per day tweets analysis (volume analysis).

Step 6: Design and Implementation of program for per hour frequency of tweets (volume analysis).

Step 7: Design and Implementation of program for geolocation wise frequency of tweets (volume analysis).

Step 8: Design and Implementation of map reduce program for trending views using Random Forest algorithm

Step 9: Tweet Classification.

Step 10: Send Alert to nearest Authority if Terrorist supporting tweet detected.

Feature Selection

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) has prepared a dataset known as Global Terrorism Database (GTD) (https://www.start.umd.edu/gtd). GTD contains information about terrorist activities from 1970 until 2018, including more than 181,000 different instances of terrorism. In this paper, 34 attributes (some attributes are redundant and hence discarded) are taken for the analysis.

Prediction of Different Factors of Terrorist Activities:

The following are different factors that neural network and deep neural network will be trained to learn.

•Suicide. This field indicates whether the attack is suicide or not suicide. $1 =$ "Yes" means that the incident was a suicide attack. $0 =$ "No" means there is no indication that the incident was a suicide attack. Dimension of the dataset is . 90% data is used for training (315,104 instances) and 10% is used for testing (35,012 instances). Both "Yes" and "No" classes have 175,058 instances.

Success. This field indicates the success of a terrorist strike. $1 =$ "Yes" means that the incident was successful. $0 =$ "No" means that the incident was not successful. Dimension

of the dataset is . 90% of the dataset is taken as training (290,937 instances) and 10% is taken as testing (32,327 instances). Each class has 161,632 instances.
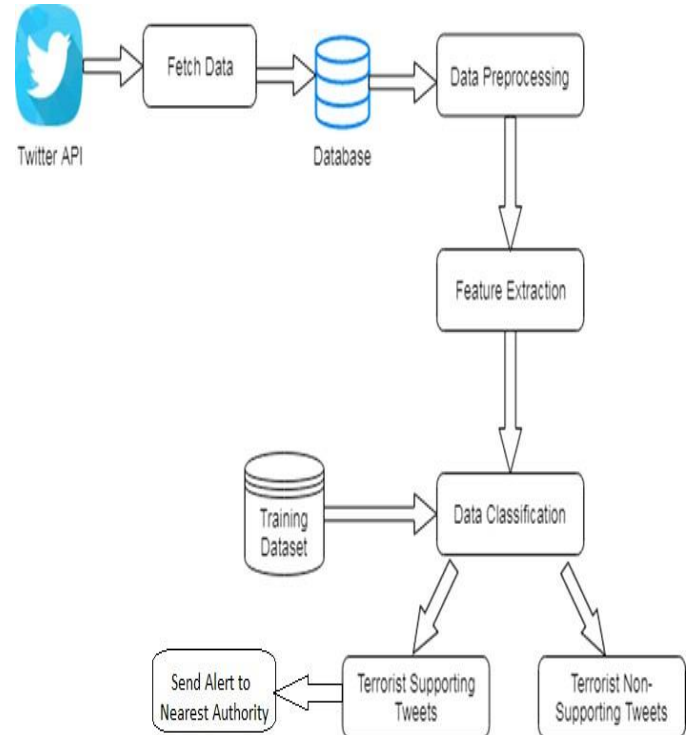

Fig. 1 System Architecture

Weapon Type. This field indicates the general type of weapon used in the incident. In the dataset, 13 different labels are used to represent different type of weapon. These labels are explained below.

(1) Biological

(2) Chemical

(3) Radiological

(4) Left as blank

(5) Firearms

(6) Explosives

(7) Fake weapons

(8) Incendiary

(9) Melee

(10) Vehicle (not to include vehicle-borne explosives, i.e., car or truck bombs)

(11) Sabotage Equipment

(12) Other

(13) Unknown

Text to Numbers

In the GTD dataset, some features are in text format, for instance, group name, country name, etc. It is not possible to process features with text data in NN or DNN. There exist

multiple techniques to convert text data to numbers, e.g., TFIDF, Word2Vec, GloVe, One hot encoding, etc. In this paper, LabelEncoder class of sklearn library is used to convert nonnumeric data to numeric data, as the labels are hashable and comparable to numerical labels.

Missing Data

The dataset contains many missing values, i.e., the cell does not contain any data, which results into NaN when processed by NN. Different interpolation techniques can be used to fill the missing data. In this paper, SimpleImputer of sklearn library is used to fill the missing data. We have replaced the missing values by mean along each column.

•Purpose

As we know large number of population using social network like facebook,tweeter etc. now a days. Number of Terrorist organizations use different social media as a tool for spreading their views and influence general people to join their terrorist activities. Twitter is the most common and easy way to reach mass people within a small amount of time. And due to this ist a need to earlier detect such group and stop innocent people getting into trap , But to do this task manually will needs unfeasible number of human moderators. And hence there is need to automate the task of public terrorist activities detection in Twitter from the perspective of victims and explore terrorist. This proposed system will help to ban the terrorist accounts from twitter so that they can't promote their views or spread fear among general people.

•Motivation

This work about the use of social media during a time of terrorist attack with a view to address how to use social media for public communication with emergency organization and military or police during terrorist attack, how to perform post-attack social media analytics and how to detect acts of terrorism, unrest and hatred using social media analytics.

4.3   Algorithm 1

```
k-Nearest Neighbor
Classify (X, Y, x) // X: training data, Y: class labels of X, x: unknown sample
for i = 1 to m do
    Compute distance d(X_i, x)
end for
Compute set I containing indices for the k smallest distances d(X_i, x).
return majority label for {Y_i where i ∈ I}
```

Algorithm 2

Input: Users tweets and user id(t0,t1,…tn)

Output: Classification output(terrorist/normal tweet) Process:

Step1: Take tweet as a imput (t0,t1,…tn)

Step2: Preprocess tweet

Step3: tokenization of tweet using NLTK module Step4: Remove stopwords using stopword dataset Step5: CNN Training phase on data

Step 6(b): ReLU Layer. ...

Step 7: Pooling. ...

Step 8: Flattening. ...

Step 9: Full Connection. ...

Step 10 - Convolution Operation. ...

Step 11(b): The Rectified Linear Unit (ReLU) ...

Step 12 - Max Pooling. Step 13: Classify tweet

Step14: Alert send using KNN.

IV CONCLUSION

In this Paper, We have Detection framework to detect tweets that support terrorism from real- time tweets stream. Our framework collects real time tweets by using twitter streaming API and tweet. It can categorize the tweet into three category and based on the category of the tweet, it is stored and shown in the different screen of our web application. We have also created a re-train module which will be used to retrain our model so that it can perform more accurately.

REFERENCES

[1]IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS MAY 2019 Tracking Changes in Resilience and Level of Coordination in Terroris NetworkS Vasanthan Raghavan , Senior Member, IEEE, and Alexander G. Tartakovsk Senior Member, IEEEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS MAY 2019

[2] Behaviour During Crisis Situations in Social Media-A Case Study on the Manch-esteR Bombing 2017, In International Working Conference on Transfer and Dif-fusion of IT,Springer, Cham. pp. 6075, June 2018.

[3] M. L. Williams and P. Burnap, Cyberhate on social media in the aftermath of Woolwich: A case study in computational criminology and big data, British Journal of Criminology, vol. 56(2), pp. 211238, 2015

[4] 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February, 2019 978-1-5386-9111-3/19/$31.00 ©2019 IEEE A Framework for Analyzing Real-Time Tweets to Detect Terrorist Activities

[5] M. L. Williams and P. Burnap, Cyberhate on social media in the aftermath of Woolwich: A case study in computational criminology and big data, British