Detection of Online Spread of Terrorism

Anagha Jagtap[1], Amrita Nayak[2], Manaswee Adwant[3], Reetika Kerketta[4]

[1]*Student, School of Engineering, MIT ADT University, Pune*
[2]*Student, School of Engineering, MIT ADT University, Pune*
[3]*Student, School of Engineering, MIT ADT University, Pune*
[4]*Assistant Professor, School of Engineering, MIT ADT University, Pune*

---***---

Abstract - *Terrorist growth has increased in certain parts of the world. Terrorist groups use Facebook, WhatsApp, and messages to spread their information on the social network. With development in technology, internet has become a medium of spreading terrorism through speeches and videos. It is essential to detect terrorism and prevent its spreading before a certain time. Terrorist groups are utilizing the internet as a medium to convince innocent people to take part in terrorist activities by infuriating the people through web pages that inspire the individuals to take part in the terrorist organization. The basic idea of this project is to reduce or stop the spread of terrorism and to remove all these accounts. This needs a lot of human effort to implement this project that will collect the information and find the terrorist groups. To reduce human effort, we implement a system which detects terrorist activities in social media.*

***Key Words*: Twitter, Terrorism, Machine Learning, Sentiment analysis**

1.INTRODUCTION

Since the late 1980s the internet has proven to be highly dynamic means of communication. The benefits of internet technology are numerous, starting with its unique suitability for sharing information and ideas. It must also be recognized that the same technology that facilitates such communication can also be exploited for the purpose of terrorism. Terrorism has grown its roots quite deep in certain parts of world. The Internet is used by spreading speeches, videos, URLs, etc. to persuade the youth and spread hatred among them.

The use of the internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism. Data Analytics, Artificial intelligence, Machine learning etc. is turning out to be helpful in protecting humankinds from such threats.

“Detection of Online spread of terrorism” works on Twitter data to find terrorism related tweets. Sentiment analysis is used in this software to classify the terrorism tweets as threat tweets and awareness tweets. The purpose of the detector is to help the authorities find the threat tweets in order to remove them from social media.

2. RELATED WORK

The spread of terrorism spread via social media platforms like twitter, Facebook, Instagram has been increasing. According to research papers, there are many machine learning algorithms, which help us identify the terrorists who use the social media platforms to provoke and scare the general public: [1] Used two classification techniques: One, binary – testing of positive and negative statements and second, three way – positive vs negative vs neutral.

It was also found that, tree kernel and feature based model outperform the standard unigram baseline. Feature analysis revealed that most important features are those that combine prior polarity of words with POS. [2] Confirm the fact that the best performance on the data is obtained replacing the modifiers and the words found in affect dictionaries with generic labels, using unigrams and bigrams as and eliminating those n-grams that appear only once. The best features to be employed in sentiment analysis in tweets are unigrams and bigrams together. Use of generalizations, by employing unique labels to denote sentiment-bearing words and modifiers highly improves the performance of the sentiment classification. [3] ANN gave better accuracy in both datasets as compared to Naïve Bayes and SVM. Parameters used for calculating the best method: F measure, precision, sensitivity and accuracy. Naïve Bayes gave the least accuracy.

3. METHODOLOGY

The methodology involved in making this project started initial from retrieval of tweets using the Twitter API and collecting them in the database for further pre-processing of data. The process is:

1. Gathering twitter data - The training set and testing set of data is gathered in this step.

2. Creating the dataset - We have prepared a manual dataset of a streamline of twitter output.

3. Pre-processing the data - Social media data is unstructured and needs to be cleaned before using it to train a sentiment analysis model – good quality data will lead to more accurate results. It includes removal of emojis, blank spaces and special characters.

4. Deciding algorithm for sentiment analysis - In this we tried to solve our case using two algorithms: One was SVM giving 74% accuracy and second - Naive Bayes giving 86.68% accuracy, hence we decided to move forward with the Naive Bayes algorithm.

5. Analyzing the result - Naive Bayes gives a better accuracy for classifying tweets into positive and negative ones.

4. PROPOSED SYSTEM

To stop this online spread of terrorism we propose a web data mining system to check whether the websites and the contents on internet are spreading or promoting terrorism activities. We propose a website to check the contents on twitter. The user can enter any hashtag and number of tweets to be retrieved from twitter. The system detects patterns, keywords and information relevant to terrorism which helps to determine whether the tweet is terrorism-related or legitimate. To analyse these keywords or patterns, sentiment analysis technique is performed on the data. The system provides a dashboard where the user can see the details like the number of tweets retrieved, number of tweets analyzed, suspicious tweets etc. in the form of graphs and pie charts. The system proves useful in anti-terrorism sectors and helps the cops to track the suspicious content on social media.

Machine learning algorithms:

Sentiment analysis -

Sentiment analysis or opinion mining is a natural language processing technique used to determine whether data is positive, negative or neutral.

In the system, we have used sentiment analysis to classify the tweets terrorism-related tweets and legitimate tweets, this will help to understand the data more properly and will be helpful for organizations to take actions.

With the sentiment analysis tokenization, lemmatization, stemming, these NLP concepts are used, the introduction to these concepts can be given as -

Tokenization: Tokenization is the process of turning sensitive data into non sensitive data called "tokens" that can be used in a database or internal system without bringing it into scope. Tokenization can be used to secure sensitive data by replacing the original data with an unrelated value of the same length and format.

Lemmatisation: Lemmatisation in linguistics is the process of grouping together the inflected forms of a word so they can be analyzed as a single item, identified by the word's lemma, or dictionary form.

Stemming: In linguistic morphology and information retrieval, stemming is the process of reducing inflected words to their word stem, base or root form—generally a written word form.

For sentiment analysis, set of words are created for analysis purpose, called as Bag of Words

Bag of words: The bag-of-words model is a simplifying representation used in natural language processing and information retrieval. In this model, a text is represented as the bag of its words, disregarding grammar and even word order but keeping multiplicity.

Naive bayes -

Naive Bayes is a classification algorithm based on Bayes theorem.

It is a collection of algorithms that gives the probability of an event occurring.

The principle that is followed by this algorithm is that every pair of features that have been classified is independent of each other. The probability of the features is considered with the probability of an individual feature occurring divided by the probability of the remaining feature. This states the Bayes' Theorem on which Naïve Bayes' is made.

Support Vector Machine -

The Support Vector Machine can be described as a binary classifier. It attempts to find a hyperplane that can separate two classes of data by the largest margin.

Random forest algorithm-

Random forest algorithm consists of a large number of individual decision trees that operate together. Each individual tree in the random forest gives a class prediction and the class with the most votes become our model's prediction.

K-nearest Neighbors-

K nearest neighbors is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure. KNN algorithm can be used for Regression as well as for Classification but mostly it is used for the Classification problems.

Table -1: Algorithms and their accuracy

Detection of online spread of terrorism		
SR. NO.	Algorithm	ACCURACY (%)
1	Naïve Bayes	92.66
2	SVM	74.46

3	Random Forest	85.60
4	KNN	80.42

Considering all this information and accuracy rates of the algorithms, for our dataset we decided to choose naive bayes algorithm as it predicted to give the 92.66% accuracy for our data.

Below figure shows the simplified flow of the application. Application is designed for the federal agents and authorities to keep track of terrorist activities on social media and take action to stop them.

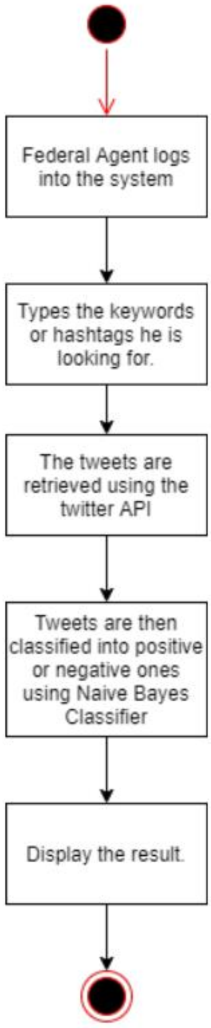
Federal Agent logs into the system
Types the keywords or hashtags he is looking for.
The tweets are retrieved using the twitter API
Tweets are then classified into positive or negative ones using Naive Bayes Classifier
Display the result.

Fig -1: Activity Diagram

4. RESULTS

This system results in methods to detect suspicious activities and their supporters who support these activities on social media by making use of ML and NLP techniques. This system further analyzes the data and gives details about the suspicious data. Analyzed data is shown with the help of charts and graphs. This system can be used in anti-terrorism sector to track contents on social media.

5. CONCLUSIONS

In this era of the internet saving mankind from malicious activities has become important. Everyone from children to senior citizens have access to the internet and social media. The hold of these technologies over human life is huge and therefore it becomes easy to manipulate people by making use of different social platforms. Fight against terrorism has taken crucial form, stopping such terrorist activities is the duty of each and everyone around the globe. Taking help of recent technologies to stop this spread of terrorism will help countries to work effectively and efficiently.

6. FUTURE WORK

The web of technology is growing day by day, with the ease in lifestyle comes threat to the human being. Considering the purpose of the application, we can add more security features in the future, which will help authorities to bring the stop to spread terrorism activities more effectively and efficiently.

In future advanced search features can be added to the website for the user to search for a specific content more efficiently. Additional features like IP address tracking can be introduced, this feature will allow the authorities to track the exact IP address through which the activity is observed and can take action on it, location of the content uploaded on social media can be added so that it is easy for the government officers to keep track of the content and the user who uploaded the content.

REFERENCES

[1] Sentiment Analysis of Twitter Data: Apoorv Agarwal, Boyi Xie, Ilia Vovsha, Owen Rambow, Rebecca Passonneau

[2] Sentiment Analysis in Social Media Texts: Alexandra Balahur

[3] Sentiment Analysis with Machine Learning Methods on social media: Muhammet Sinan Başarslana, Fatih Kayaalp