TERRORISM PREVENTION

and

HUMANITARIAN EFFORTS

<u>DMPA LAB MINI PROJECT</u>

Name: - PRIYANSHU PRANAY

Registration No: - 200953170

Section: - CCE – B2

Roll No.: -44

TABLE OF CONTENTS: -

INTRODUCTION: -

This project is an examination of a subset of a dataset containing information on known terrorist occurrences in INDIA over the previous 50 years. All of these instances fit the criteria for being classified as terrorist acts.

The reason this topic was chosen for the project is that it is easier to apply data mining efforts and is also interesting enough to extract some conclusions, as opposed to other topics that included concepts that were difficult to understand and thus would have made it too difficult to develop meaningful conclusions with our analysis results.

Furthermore, the fact that data is made up of incidents that occur in a given location allows for the creation of maps that represent it with different aims in mind, providing an interesting alternative to graphs for displaying the data in different ways.

DATASET and DATA SELECTION: -

The Global Terrorism Database dataset was uploaded by the START (Study of Terrorism and Responses to Terrorism) Consortium. The collection is available at: **https://www.kaggle.com/START-UMD/gtd.**

On September 20, 2022, the dataset was downloaded from Kaggle. The sole requirement was that a Kaggle account is created, and the option to sign up through Google was picked. Despite having information on incidences on a global scale, the scope was limited to INDIA due to the volume of data. Because there were many categorical attributes expressed twice: once with a numerical code and again with the actual word of the category, the repeated columns that gave the same information were cleansed. The textual ones were maintained since the numerical ones indicated the same thing but required looking at an external table to understand.

LITERATURE SURVEY: -

1. Terrorist assaults are the world's most difficult problem, requiring the full attention of researchers and practitioners to deal with them deliberately. Because of the scarcity of precise terrorist data, predicting the terrorist group responsible for attacks and operations is a difficult challenge. This study is based on predicting terrorist groups responsible for attacks in Egypt from 1970 to 2013 by using a data mining classification technique to compare five base classifiers namely; Nave Bayes (NB), K-Nearest Neighbor (KNN), Tree Induction (C4.5), Iterative Dichotomiser (ID3), and Support Vector Machine (SVM) based on real data represented by the Global Terrorism Database (GTD) from the National Consortium for the Study of Terrorism (START). The purpose of this work is to offer two distinct techniques for dealing with missing data, to provide a full comparison examination of the classification algorithms employed, and to evaluate the findings achieved using two different test options. Experiments are run on real-world data using WEKA, and the final evaluation and conclusion are based on four performance measures, which show that SVM is more accurate than NB and KNN in the mode imputation approach, ID3 has the lowest classification accuracy despite performing well in other measures, and in the similar deletion approach; KNN outperforms the other classifiers in accuracy, but SVM's overall performance is acceptable compared to other classifiers.

2. Following the "9/11" terrorist attacks, more advanced information technologies in the counter-terrorism arena have been created to improve the performance of early warning systems. Machine learning-based data mining can be used to predict terrorist events buried within terrorist attack events, allowing specialists to acquire a clear image of what terrorists are thinking to strengthen defenses against these organized activities. This research focuses on using data mining techniques to forecast terrorist occurrences using the Global Terrorism Database (GTD). In this paper, Support Vector Machine (SVM), Naive Bayes (NB), and Logistic Regression (LR) are used. To increase classification accuracy, two feature selection methods are used: Minimal-redundancy maximal-relevancy (mRMR) and Maximal relevance (Max-Relevance). Finally, a detailed comparison of classification performance is shown, with classifier LR reaching a classification precision of 78.41% with seven optimal feature subsets, validating the feasibility of applying machine learning to the topic of terrorism. We have emphasized that the classification methods can be utilized to map various inherent forms of terrorism

with great accuracy and rapidity. Furthermore, a well-chosen feature set can lead to a reduction in classification errors.

3. Suicide bombings are a major worry for every country in the globe today. They are a highly destructive criminal activity called terrorism, in which an individual detonates a bomb linked to himself or herself, generally in a public place, killing many people. Terrorist activity in different parts of the world is dependent on geopolitical events and key regional considerations. There has previously been no significant work undertaken using the Pakistani suicide attack dataset, and no data mining-based solutions have been provided for suicide attacks. By extracting hidden patterns from suicidal bombing assault data, this article wants to contribute to the counterterrorism initiative for the safety of the globe against suicide bomb attacks. To investigate the psychology of suicide bombers and discover a link between suicide strikes and the prediction of the next likely location for terrorist activities, visualization analysis and data mining techniques such as classification, clustering, and association rule mining are used. To distinguish specified attributes, the Nave Bayes, ID3, and J48 algorithms are used for classification. The classification results demonstrate great accuracy against all three algorithms used, 73.2%, 73.8%, and 75.4%. We use the K-means technique to do clustering, and as a result, the risk of blast intensity at a certain location is discovered. The Apriori method is also used to obtain frequent patterns for the association rule to determine the components associated with suicide attacks.

4. We began by outlining some of the obstacles associated with using data mining for counter-terrorism. These include false positive and false negative elimination, multimedia data mining, real-time data mining, and privacy. Following that, we addressed numerous threats. In other words, we presented a rather thorough review of numerous risks and counter-terrorism tactics. First, we talked about natural disasters and human faults. The dangers were then classified as non-information-related terrorism, information-related terrorism, and biological, chemical, and nuclear threats. We also talked about risks to key infrastructure. Following that, we talked about counter-terrorism tactics for all forms of threats. For example, we must collect information about terrorists and terrorist organizations, mine the data, and discover patterns. In the case of bioterrorism, we must deploy sensors to prevent terrorist strikes. Following that, we offered a thorough review of data mining for counter-terrorism. The terms data mining and web data mining have been used interchangeably. Again, we may expect much of the data to be on the web, whether on the Internet or corporate intranets and so mining the web's data sources and

databases to detect and prevent terrorist acts will become necessary. These databases could be public or private in nature. We began by discussing data mining for non-real-time threats. The objective is to collect data, create terrorist profiles, learn from examples, and ultimately detect and prevent attacks. The issue here is to discover real-world instances because in many cases, a specific attack has never occurred before. Then we talked about real-time data mining. The difficulty here is creating models in real-time. Finally, we addressed data mining outcomes and approaches for counter-terrorism, with a focus on link analysis.

5. Terrorist group prediction utilizing historical data of attacks has received less attention because of a lack of thorough terrorist data containing terrorist groups' attacks and activities. The reasons could be confidentiality and sensitivity. We demonstrated a terrorist group prediction model (TGPM) in this research to forecast the terrorist group involved in a specific attack. To anticipate the responsible group, this program first learns similarities between terrorist episodes from diverse terrorist acts. The experimental results have validated the model. The model's overall performance demonstrates a high level of accuracy.

6. Terrorism has become one of the most difficult crises to deal with and a major threat to humanity. Several research projects are building efficient and precise solutions to improve counter-terrorism, and data mining is no exception. Massive amounts of data are floating around in our lives, yet the scarcity of actual terrorist incident data in the public domain complicates the battle against terrorism. This paper examines data mining categorization techniques and the role of the United Nations in counter-terrorism. It examines the performance of classifiers such as Lazy Tree, Multilayer Perceptron, Multiclass, and Nave Bayes for detecting trends in terrorist acts around the world. The database for experiment purposes was compiled from several public and open access sources for the years 1970-2015, and it contains 156,772 reported attacks that resulted in large losses of life and property. This study enumerates the losses that happened, trends in attack frequency, and locations that are more vulnerable to it, using the attack responsibilities as an assessment class.

7. Pattern-based data analysis has the potential to be useful in counterterrorism in the long run, if research into its applications continues. As will be explained further in the following section, data-mining research must reveal meaningful patterns that can forecast an incredibly unusual activity—terrorist planning and assaults. 18 It must also determine

how to distinguish the "signal" of a pattern from the "noise" of innocuous data activity. If pattern-based searches can be perfected, they may reveal hints of "sleeper" activity by unknown terrorists who have never engaged in activities that would link them to known terrorists. Pattern-based searches, unlike subject-based inquiries, do not require a relationship to a known suspicious subject. Pattern-based searches that could be useful include looking for specific combinations of lower-level behavior that are predictive of terrorist action. A "sleeper" terrorist might be someone in the nation on a student visa who buys a bomb-making book and 50 medium-sized tonnes of fertilizer. If it is feared that terrorists will use large trucks for attacks, automated data analysis could be performed regularly to identify people who have rented large trucks, used hotels or drop boxes as addresses, and fall within certain age ranges or have other characteristics that are part of a known terrorist pattern. Significant trends in e-mail traffic could be identified, revealing terrorist involvement and "ringleaders." Pattern-based searches may also be beneficial in response and outcome management. Searches of hospital data for reports of specific combinations of symptoms, or other databases for patterns of behavior, such as pharmaceutical purchases or job absence, could, for example, provide an early warning of a terrorist strike employing a biological weapon.

8. The techniques and strategies used by the United States in its "War on Terrorism" have been widely denounced as deviations from the principles of how a democratic government should conduct itself. Reforms are thus deemed necessary to bring the "War on Terror" within the rule of law and defend civil freedoms. This article seeks to refute that viewpoint. Using predictive data mining—a technology at the heart of the US National Security Agency's (NSA) surveillance scandal—as an example, it argues that, rather than a break with the past, the Bush Administration's anti-terrorism tactics represent an extension of a type of future-oriented power referred to as "security" or "government" by Foucault (2008). And, while individual civil freedoms are certainly in danger, they are not equally so for everyone. Predictive data mining discriminates by design, labeling certain groups as more dangerous than others. As a result, people from the Middle East and North Africa will bear a disproportionate share of the burden of this surveillance technology and the numerous errors it generates. Finally, the rule of law appears to give little hope of resolving the matter. The War on Drugs, immigration policy, and previous international confrontations with "terrorist regimes" have all contributed to a "crime jurisprudence" (Simon 2007) that legitimizes such discrimination. The real chance for reform, paradoxically and pessimistically, rests in the crisis of legitimacy that could come from the greater application of such discriminatory technology or the benign reign of an executive branch imbued with authority beyond its conventional limitations.

9. This work compares two classification methods, Decision Tree and Nave Bayesian, for predicting the 'Crime Category' attribute, which has labels of 'Low,' 'Medium,' and 'High.' Accuracy, Precision, and Recall for the Decision Tree are 83.9519%, 83.5%, and 84%, respectively. The Accuracy, Precision, and Recall numbers for Nave Bayesian, on the other hand, are 70.8124%, 66.4%, and 70.8%, respectively. The experimental findings for both algorithms show that the Decision Tree outperformed the Nave Bayesian on the crime dataset using WEKA. This experiment included 10-fold cross-validation. Law enforcement agencies can benefit greatly from employing machine learning algorithms like Decision Tree to combat crime and terrorism. There is a plan for future studies to apply various categorization algorithms to the crime data set and evaluate their prediction performance. Another avenue for future research is to employ alternative feature selection strategies and investigate their impact on the prediction performance of various algorithms.

10. . This article investigates the issues of exploiting big data in the humanitarian sector in support of UN SDG 17 "Partnerships for the Goals." The full promise of Big Data is based on the implicit premise that the heterogeneous 'exhaust trail' of data is contextually relevant and detailed enough to be mined for value. This promise, however, is dependent on relationality - that patterns can be drawn by integrating distinct bits of data with appropriate information or that effective mechanisms exist to reconcile discrepancies in detail. We provide empirical work integrating eight diverse datasets from the humanitarian area to demonstrate the inherent complexity and difficulty caused by varying levels of data granularity. In explaining this dilemma, we investigate the reasons for its manifestation, present options for tackling it, and suggest five proposals to direct future research as our main contribution.

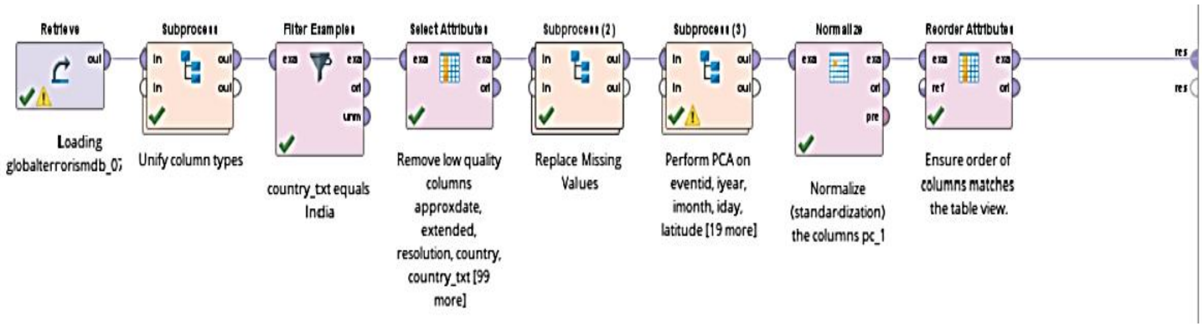
METHODOLOGY: -

PRE-PROCESSING: -

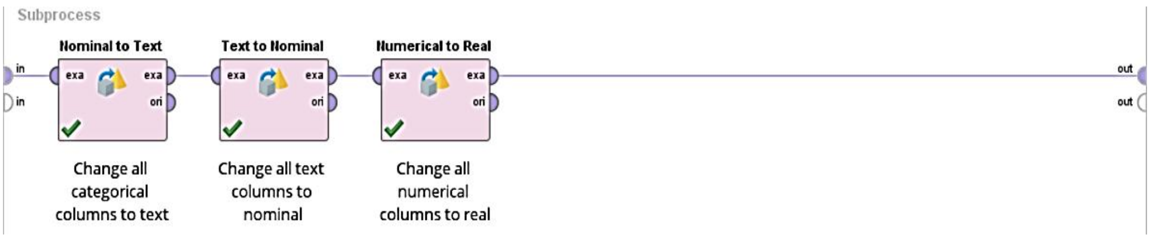
Because there were too many variables, rows, irrelevant or didn't have enough instances to use them, misplaced numbers, and so on, a significant amount of preparation work was required for this project. The majority of the pre-processing was done in **RAPIDMINER STUDIO** utilizing *Turbo-Prep*, which is reflected in the final dataset.

The **'Country_txt'** column is first filtered using the criteria "*Equals To '**INDIA**'*" and the following procedure, which comprises *deleting low-quality columns*, *replacing missing values*, *PCA*, and *Normalization (pc_1 column)*.

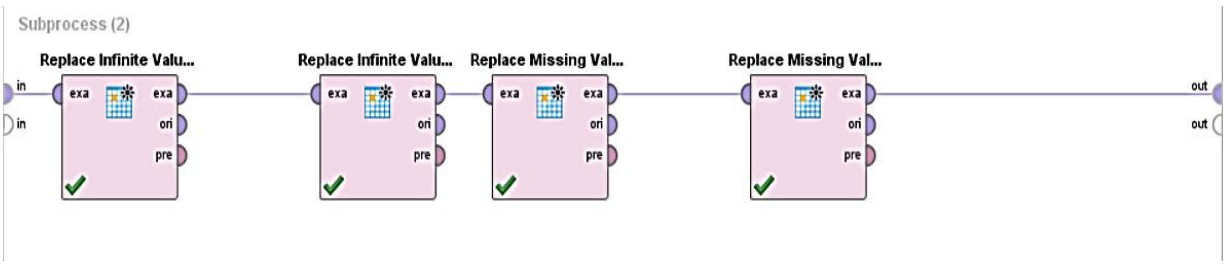
Process:



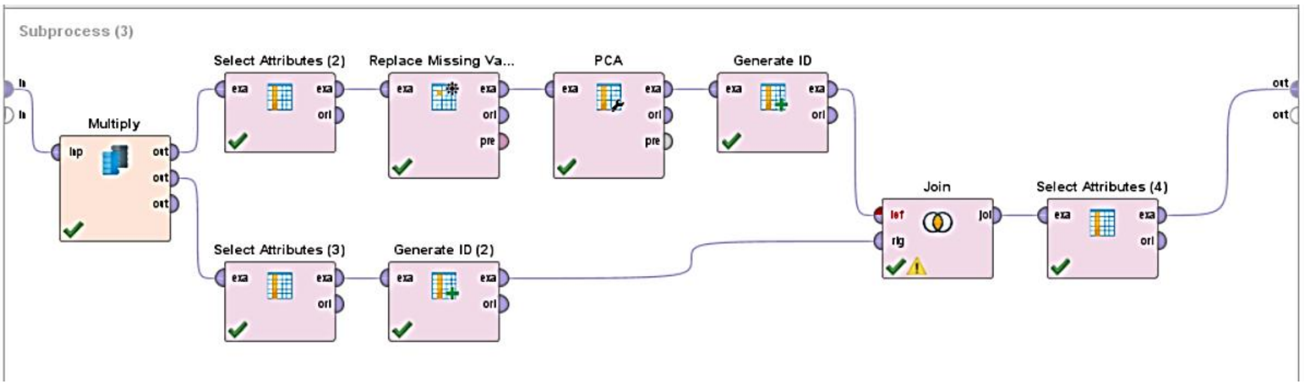
Subprocess 1:



Subprocess 2:



Subprocess 3:



There were originally 135 columns (78 nominal and 57 numerical) and 93286 rows. The dataset comprises 8 columns (1 numerical and 7 nominal) and 5062 rows after cleansing.

APRIORI ALGORITHM: -

Applied to obtain a common item set with minimum support of 10 to determine the frequency of weapon type and city. This aids in the development of infrastructure upgrades that are specific to each location.

Apriori Algorithm was written in Python programming language.

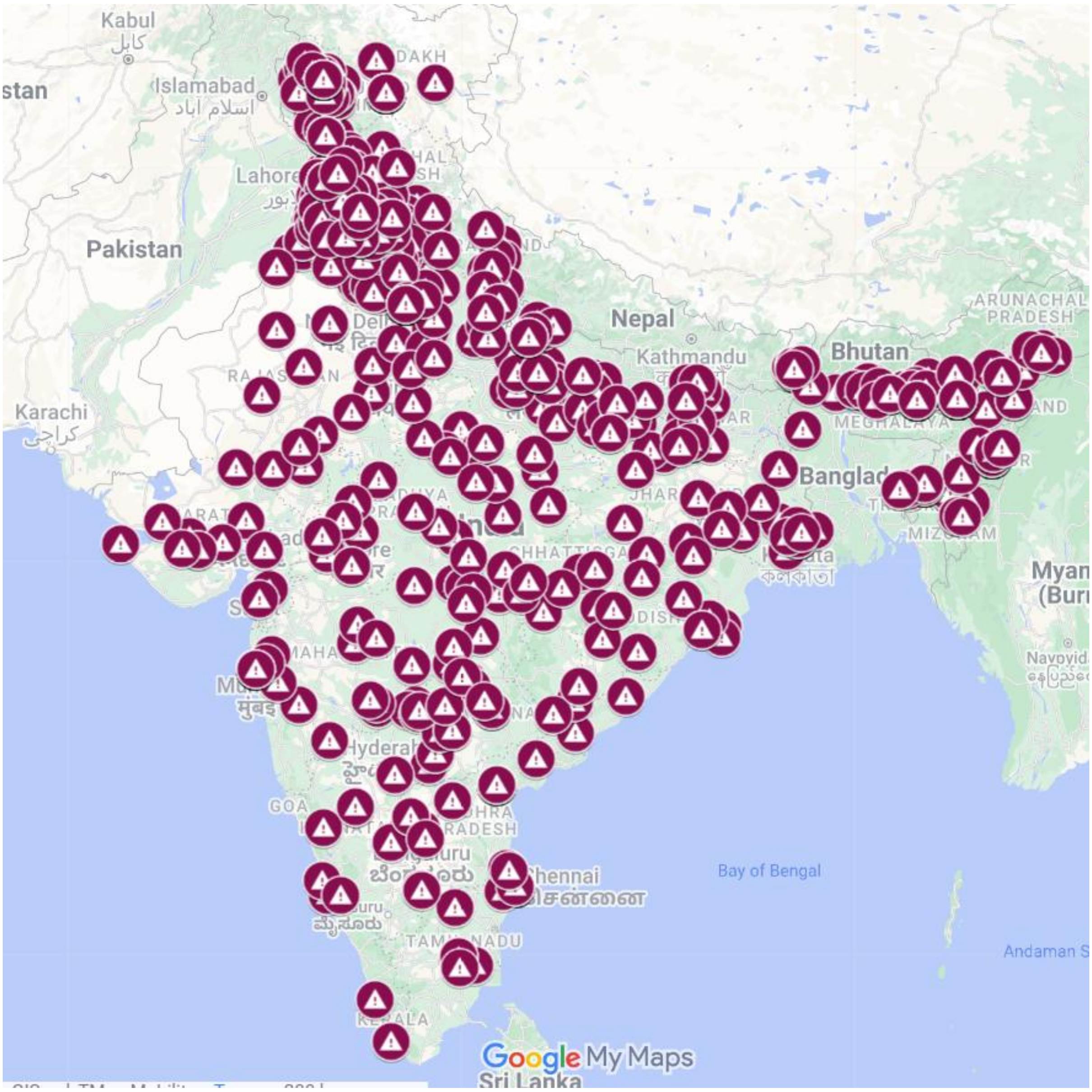
```
import numpy as np
import matplotlib.pyplot as plt
import itertools
import copy
import csv
records = []
row_count=0
cols=0
row_count = sum(1 for row in csv.reader( open('Book2.csv',"rt") ) )
min_support=int(input("Enter minimum support: "))
with open('Book2.csv', 'r') as f:
    reader = csv.reader(f)
    records=list(reader)
for i in records:
   while ' ' in i:
      i.remove(' ')
   while '' in i:
      i.remove('')
c1=[]
for i in range(0, len(records)):
   for j in range(0,len(records[i])):
      if records[i][j] not in c1:
         c1.append(records[i][j])
freq={}
for i in range(0, len(records)):
   for j in range(0,len(records[i])):
      if records[i][j] not in freq:
```

```
            freq[records[i][j]]=1
        else:
            freq[records[i][j]]=freq[records[i][j]]+1
l=[[]]
print("First frequent item set is: ")
for i in range(0,len(c1)):
    if freq[c1[i]]>=min_support:
        l[0].append(c1[i])
c2=list(itertools.combinations(l[0], 2))
for k in c2:
    for i in range(0, len(records)):
        if k[0] in records[i] and k[1] in records[i]:
            if k not in freq:
                freq[tuple(k)]=1
            else:
                freq[tuple(k)]=freq[tuple(k)]+1
x=[]
l.append([])
print("Second frequent item set is: ")
for i in c2:
    if i in freq and freq[i]>=min_support:
        l[1].append(i)
        print(i, freq[i])
        for k in i:
            if k not in x:
                x.append(k)
count=2
while x:
    count=count+1
    c=list(itertools.combinations(x, count))
    check=1
    temp=copy.deepcopy(c)
    for i in c:
        for j in i:
            if j not in l[0]:
                temp.remove(i)
                break
        check=1
        for j in range(2,len(i)):
            if check==0:
                break
            subs=list(itertools.combinations(i,j))
            for k in subs:
                if k not in l[j-1]:
                    temp.remove(i)
                    check=0
                    break
    c=temp
    for j in c:
        for i in records:
            check=1
            for k in j:
                if k not in i:
                    check=0
                    break
            if check==1:
                if j not in freq:
                    freq[j]=1
                else:
                    freq[j]=freq[j]+1
```

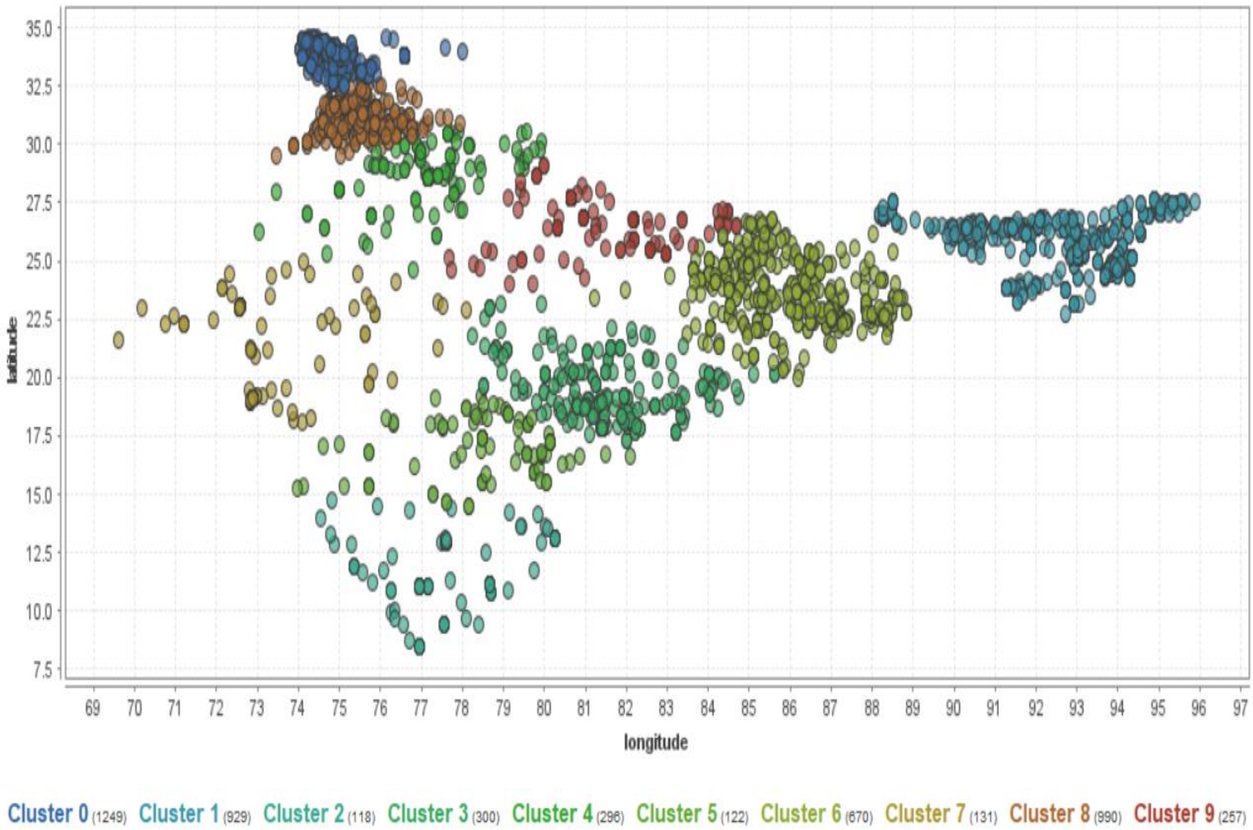
DATA ANALYSIS: -

VISUALISATIONS: -

Effected Cities:



Clustering of Latitudes and Longitudes:



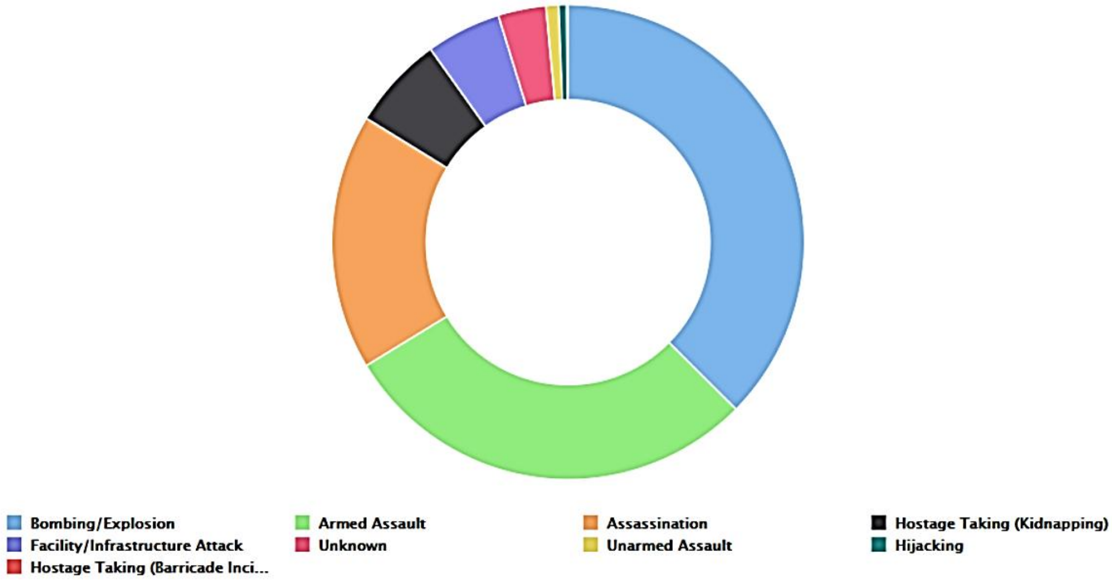
CENTROID TABLE

Cluster	latitude	longitude
Cluster 0	33.876	74.990
Cluster 1	25.801	92.439
Cluster 2	11.902	77.943
Cluster 3	19.368	81.497
Cluster 4	28.618	77.119
Cluster 5	16.947	78.712
Cluster 6	23.620	85.921
Cluster 7	21.016	73.223
Cluster 8	31.189	75.411
Cluster 9	27.184	81.015

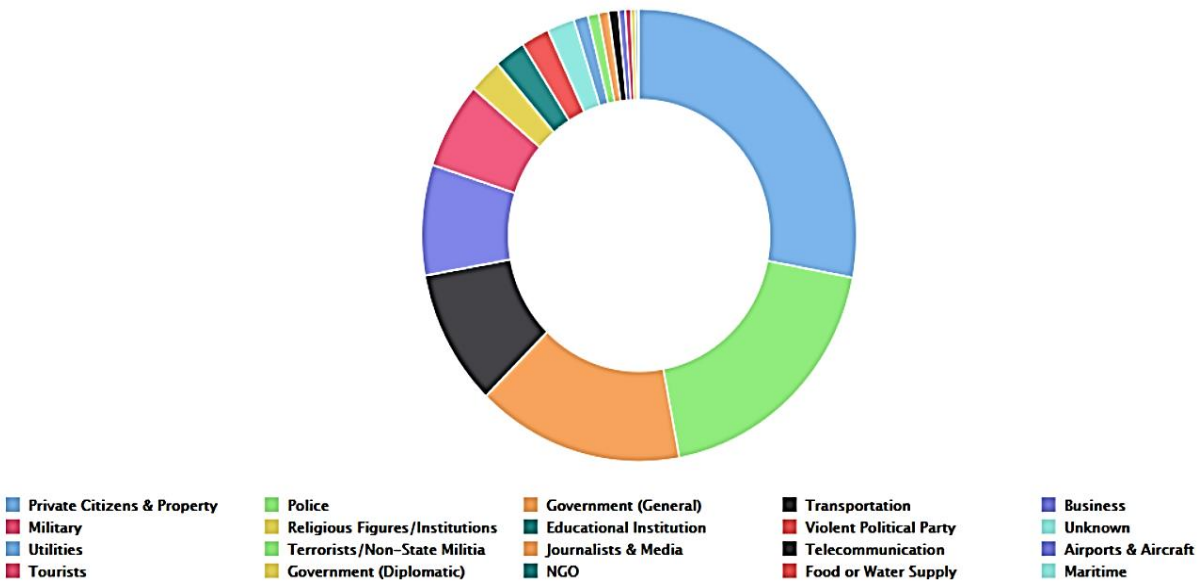
The above table gives the center location of their respective clusters.

CHARTS: -

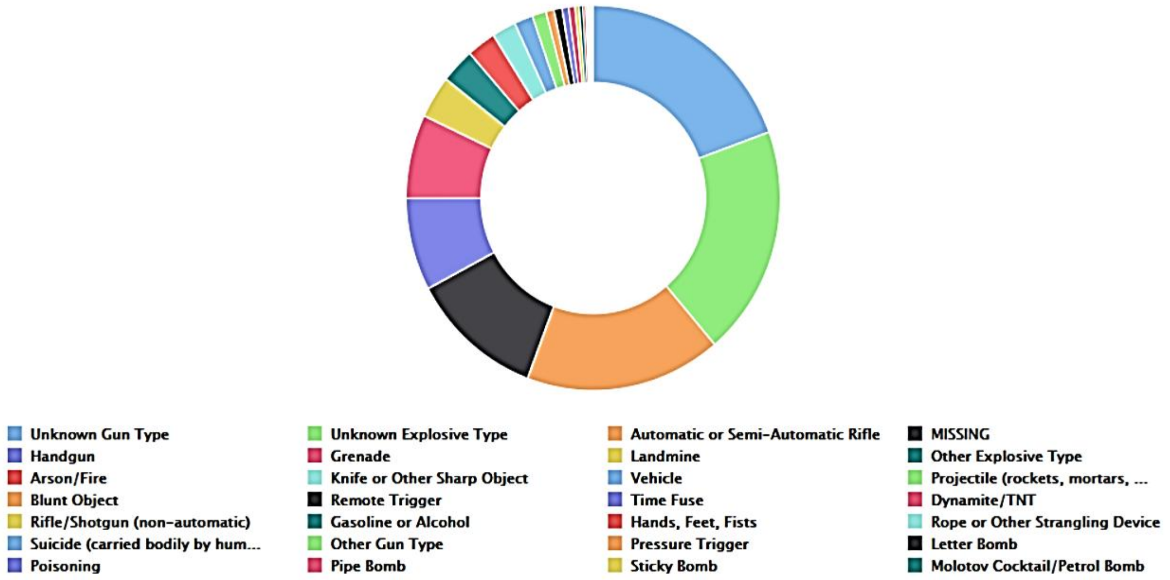
Pie Chart for Attack Type



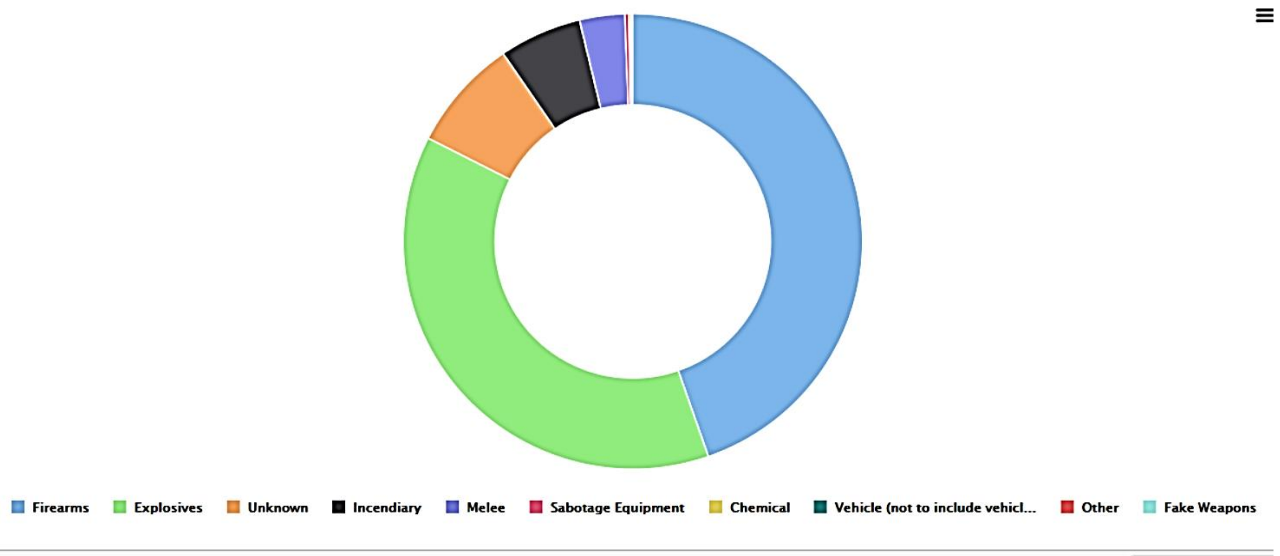
Pie Chart for Target Type



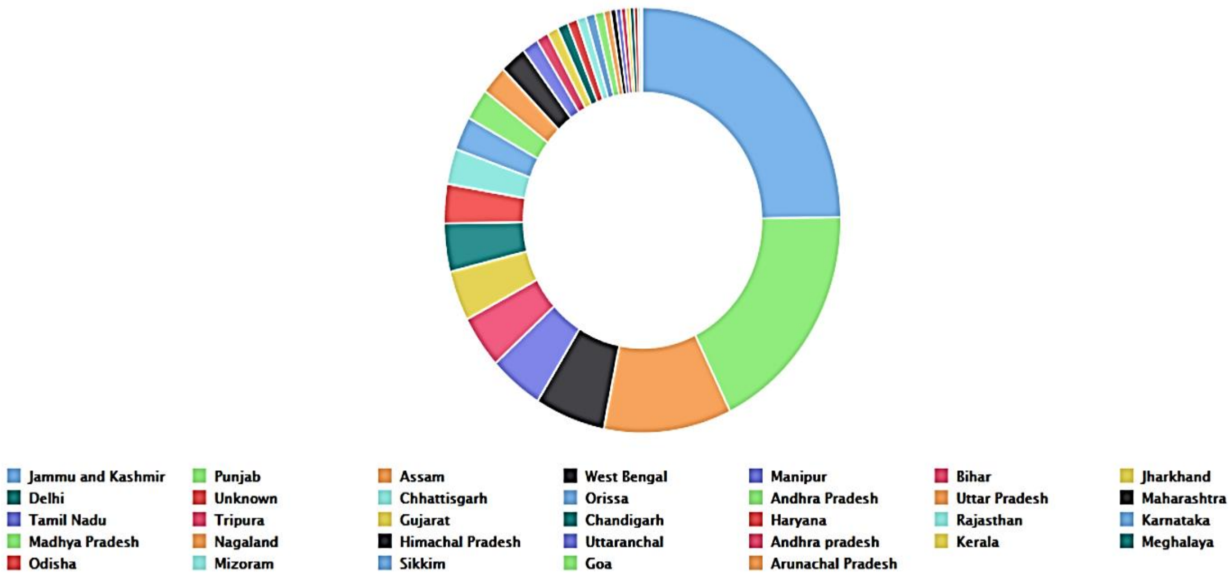
Pie Chart for Weapon Sub-Type



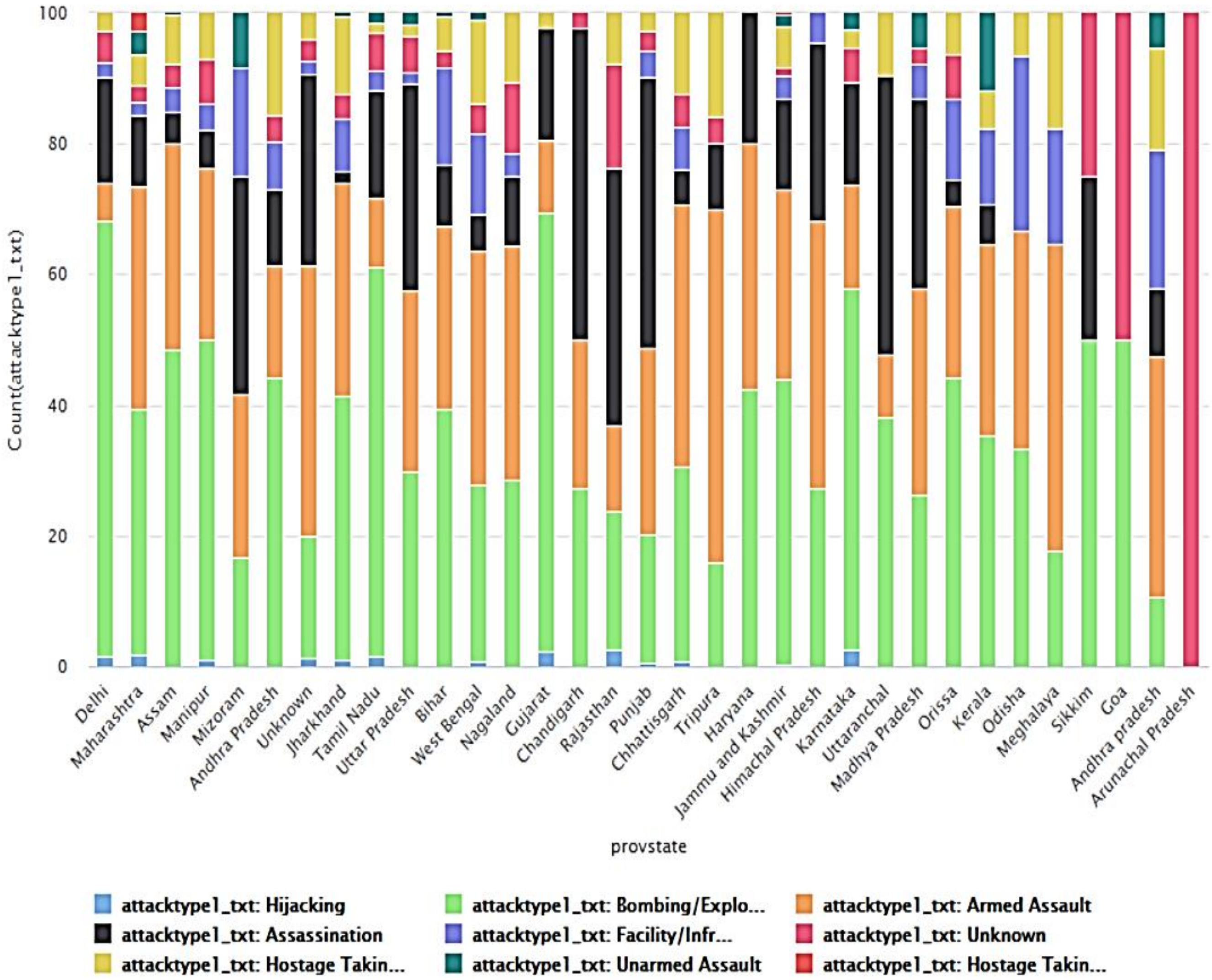
Pie Chart for Weapon Type



Pie Chart for State



Histogram (Stacked) for Attack Type and State



OUTPUT:

('Delhi', 'Bombing/Explosion) 123

('Delhi', 'Armed Assault') 11

('Delhi', 'Assassination') 30

('Bombing/Explosion', 'Maharashtra') 41

('Bombing/Explosion', 'Assam') 256

('Bombing/Explosion', 'Manipur') 110

('Bombing/Explosion', 'Andhra Pradesh') 56

('Bombing/Explosion', 'Unknown') 28

('Bombing/Explosion', 'Jharkhand') 78

('Bombing/Explosion', 'Tamil Nādu') 40

('Bombing/Explosion', 'Uttar Pradesh') 33

('Bombing/Explosion', 'Bihar') 80

('Bombing/Explosion', 'West Bengal') 78

('Bombing/Explosion', 'Gujarat') 31

('Bombing/Explosion', 'Chandigarh') 12

('Bombing/Explosion', 'Punjab') 179

('Bombing/Explosion', 'Chhattisgarh') 41

('Bombing/Explosion', 'Haryana') 17

('Bombing/Explosion', 'Jammu and Kashmir') 547

('Bombing/Explosion', 'Karnataka') 21

('Bombing/Explosion', 'Madhya Pradesh') 10

('Bombing/Explosion', 'Orissa') 57

('Maharashtra', 'Armed Assault') 37

('Maharashtra', 'Assassination') 12

('Assam', 'Armed Assault') 167

('Assam', 'Assassination') 25

('Assam', 'Facility/Infrastructure Attack') 20

('Assam', 'Unknown') 19

('Assam', 'Hostage Taking (Kidnapping)') 40

('Armed Assault', 'Manipur') 59

('Armed Assault', 'Andhra Pradesh') 28

('Armed Assault', 'Unknown') 62

('Armed Assault', 'Jharkhand') 63

('Armed Assault', 'Uttar Pradesh') 31

('Armed Assault', 'Bihar') 57

('Armed Assault', 'West Bengal') 104

('Armed Assault', 'Nagaland') 10

('Armed Assault', 'Chandigarh') 10

('Armed Assault', 'Punjab') 260

('Armed Assault', 'Chhattisgarh') 55

('Armed Assault', 'Tripura') 27

('Armed Assault', 'Haryana') 15

('Armed Assault', 'Jammu and Kashmir') 364

('Armed Assault', 'Madhya Pradesh') 12

('Armed Assault', 'Orissa') 34

('Manipur', 'Assassination') 13

('Manipur', 'Unknown') 15

('Manipur', 'Hostage Taking (Kidnapping)') 16

('Assassination', 'Andhra Pradesh') 16

('Assassination', 'Unknown') 44

('Assassination', 'Tamil Nadu') 11

('Assassination', 'Uttar Pradesh') 35

('Assassination', 'Bihar') 19

('Assassination', 'West Bengal') 16

('Assassination', 'Chandigarh') 21

('Assassination', 'Rajasthan') 15

('Assassination', 'Punjab') 375

('Assassination', 'Jammu and Kashmir') 174

('Assassination', 'Madhya Pradesh') 11

('Facility/Infrastructure Attack', 'Andhra Pradesh') 13

('Facility/Infrastructure Attack', 'Jharkhand') 16

('Facility/Infrastructure Attack', 'Bihar') 30

('Facility/Infrastructure Attack', 'West Bengal') 36

('Facility/Infrastructure Attack', 'Punjab') 38

('Facility/Infrastructure Attack', 'Jammu and Kashmir') 45

('Facility/Infrastructure Attack', 'Orissa') 16

('Andhra Pradesh', 'Hostage Taking (Kidnapping)') 22

('Unknown', 'West Bengal') 13

('Unknown', 'Punjab') 26

('Unknown', 'Jammu and Kashmir') 14

('Jharkhand', 'Hostage Taking (Kidnapping)') 23

('Bihar', 'Hostage Taking (Kidnapping)') 11

('West Bengal', 'Hostage Taking (Kidnapping)') 37

('Punjab', 'Hostage Taking (Kidnapping)') 26

('Chhattisgarh', 'Hostage Taking (Kidnapping)') 17

('Hostage Taking (Kidnapping)', 'Jammu and Kashmir') 80

('Jammu and Kashmir', 'Un-Armed Assault') 24

The above output shows the frequency of attack type and state pairing.

From the above data, the government can have customized Anti-Terrorism Squads (ATS) as well as precaution drills to minimize the casualties in respective attack types.

For example, in Delhi, there is a large number of bombings so the government can monitor the movement of various bomb components, they can carry out safety drills for bombings to help the public evacuate easily and swiftly, and have a Bomb disposal squad as Rapid Action ATS, increase CCTV coverage. There are also assassinations so they can increase police patrols and VVIP securities as well as a crackdown on illegal assassins. Such steps taken in major terrorist-affected areas will help to dwindle cases to single digits. The above algorithm shows danger areas that should be given priority by the government. The clustering shows the breaking down of ATS commands to the above cluster areas to maintain a decentralized approach for swift decision-making and action. Similar actions can be taken by various affected states to combat terrorism. Similar humanitarian efforts like food, medicines, etc. can be arranged on the above model to provide relief swiftly.

CONCLUSION: -

The conclusion reached is that the Apriori algorithm helped in the pairing of attack type and state which helped in developing a map of the most affected states. The clustering analysis helped in finding of center and forming relevant groups to distribute command and decrease reaction time to prevent fatalities and help humanitarian efforts reach faster.

The centroid table predicts the central location of each command center which can be changed depending on local logistics and support.

EXTENSION OF SCOPE: -

This analysis can be increased in scope by including famines, earthquake-sensitive areas, flood-sensitive areas, cyclone-sensitive areas, etc. The clustering will help in setting up different central command centers to combat them effectively at ground level.

This can also be used for poverty levels, literacy levels, etc. This will help the government to focus on areas that are in more need of government programs and help.

The above model can also be used to predict the location of central super specialty hospitals to provide optimal healthcare to the public.

REFERENCES: -

LITERATURE SURVEY: -

1. Jonas, Jeff, and Jim Harper. *Effective counterterrorism and the limited role of predictive data mining*. Washington, DC: Cato Institute, 2006.
2. H. Mo, X. Meng, J. Li and S. Zhao, "Terrorist event prediction based on revealing data," 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA), 2017, pp. 239-244, DOI: 10.1109/ICBDA.2017.8078815.
3. Ferooz, Faria, et al. "Suicide bomb attack identification and analytics through data mining techniques." *Electronics* 10.19 (2021): 2398.
4. Thuraisingham, Bhavani. "Data mining for counter-terrorism." *Data Mining: Next Generation Challenges and Future Directions* (2004): 157-183.
5. Sachan, Abhishek, and Devshri Roy. "TGPM: Terrorist group prediction model for counter-terrorism." *International Journal of Computer Applications* 44.10 (2012): 49-52.
6. Kumar, V., Mazzara, M., Messina, A., Lee, J. (2020). A Conjoint Application of Data Mining Techniques for Analysis of Global Terrorist Attacks. In: Ciancarini, P., Mazzara, M., Messina, A., Sillitti, A., Succi, G. (eds) Proceedings of 6th International Conference in Software Engineering for Defence Applications. SEDA 2018. Advances in Intelligent Systems and Computing, vol 925. Springer, Cham. https://doi.org/10.1007/978-3-030-14687-0_13
7. DeRosa, Mary. *Data mining and data analysis for counterterrorism*. Washington, DC: CSIS Press, 2004.
8. Guzik, Keith. "Discrimination by Design: predictive data mining as security practice in the United States war on terrorism." *Surveillance & Society* 7.1 (2009): 3-20.
9. I. Rizwan, A. Masrah, A. M. Aida, H. Payam, and K. Nasim, "An experimental study of classification algorithms for crime prediction," Indian Journal of Science and Technology, vol.6, March 2013
10. Bell, David, et al. "Exploring future challenges for big data in the humanitarian domain." *Journal of Business Research* 131 (2021): 453-468.

SIMILARITY INDEX: -

It was done on the **TURNITIN** software with help of the Lab instructor.

1% Similarity Index without Literature Survey.

AFTER-TERRORISM REHABILITATION and HUMANITARIAN EFFORTS

ORIGINALITY REPORT

1 %	1 %	1 %	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	deepblue.lib.umich.edu Internet Source	1 %
2	lists.mplayerhq.hu Internet Source	1 %

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		

A 30% Similarity Index was found after including Literature Survey.

AFTER-TERRORISM REHABILITATION and HUMANITARIAN EFFORTS

ORIGINALITY REPORT

30%	30%	0%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.tandfonline.com Internet Source	30%

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		