2022 25th International Conference on Computer and Information Technology (ICCIT)
17-19 December, Cox's Bazar, Bangladesh

Predicting the Success of Suicide Terrorist Attacks using different Machine Learning Algorithms

Md. Junayed Hossain
Computer Science and Engineering
Independent University, Bangladesh
Dhaka, Bangladesh
junayed.ndc16@gmail.com

Sheikh Md. Abdullah
Computer Science and Engineering
Independent University, Bangladesh
Dhaka, Bangladesh
s.m.abdullah013@gmail.com

Mohammad Barkatullah
Computer Science and Engineering
Independent University, Bangladesh
Dhaka, Bangladesh
barkatopu1345@gmail.com

M. Saef Ullah Miah
Faculty of Computing
Universiti Malaysia Pahang
Pekan, Malaysia
md.saefullah@gmail.com

Talha Bin Sarwar
Faculty of Computing
Universiti Malaysia Pahang
Pekan, Malaysia
talhasarwar40@gmail.com

Md Fahad Monir
Computer Science and Engineering
Independent University, Bangladesh
Dhaka, Bangladesh
fahad.monir@iub.edu.bd

2022 25th International Conference on Computer and Information Technology (ICCIT) | 979-8-3503-4602-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCIT57492.2022.10055100

***Abstract*—Extremism has become one of the major threats throughout the world over the past few decades. In the last two decades, there has been a sharp increase in extremism and terrorist attacks. Nowadays, terrorism concerns all nations in terms of national security and is considered one of the most priority research topics. In order to support the national defense system, academics and researchers are analyzing various datasets to determine the reasons behind these attacks, their patterns, and how to predict their success. The main objective of our paper is to predict different types of attacks, such as successful suicide attacks, successful non-suicide attacks, unsuccessful suicide attacks, and unsuccessful non-suicide attacks. For this purpose, various machine learning algorithms, namely Random Forest, K Nearest Neighbor, Decision Tree, LightGBM Boosting, and a feedforward Artificial Neural Network called Multilayer Perceptron (MLP), are used to determine the success of suicide terrorist attacks. With an accuracy rate of 98.4% and an AUC-ROC score of 99.9%, the Random Forest classifier was the most accurate among all other algorithms. This model is more trustworthy than previous work and provides a useful comparison between machine learning methods and an artificial neural network because it is less dependent and has a multiclass target feature.**

***Index Terms*—Terrorism, Suicide Terrorist Attack, Machine Learning, GTD.**

I. Introduction

Terrorism is considered one of the world's biggest problems, affecting and threatening the everyday lives of people around the world. Terrorists are those who carry out violent activities by breaking laws to achieve religious, political, or social goals. Terrorism can be described as an act intended to instill fear and terror in an audience unrelated to the victims. Whether an act is classified as terrorism also depends on whether it is interpreted from a legal, moral, or behavioral perspective [1]. When a terrorist attempts suicide while carrying out an attack, it is referred to as a suicide terrorist attack. Unlike in the past, suicide terrorist attacks are clearly on the rise. According to the Global Terrorism Database (GTD), more than 16,000 terrorist attacks were recorded in 2014, the highest number of attacks in a single year between 1970 and 2017 [2]. However, the impact of a terrorist attack can be mitigated by predicting many things, such as whether or not the attack will be successful. It can also be predicted whether or not the person involved in a terrorist attack will commit suicide. These insights are useful in taking precautionary measures to prevent such attacks.

In present days, with the advancement of technology, it is possible to predict the success rate of a suicide terrorist attack, given a large number of previous data records. For this, Machine Learning (ML) algorithms and Artificial Neural Networks (ANN) can be essential in analyzing these data and combating new terrorist activities through prediction. Since there are various ML and ANN algorithms, it is challenging to choose one. Therefore, four widely used ML algorithms, namely Random Forest [3], Decision Tree [4], LightGBM Boosting [5], K Nearest Neighbor (KNN) [6], and an ANN called Multilayer Perceptron (MLP), are used to detect whether a suicide attack would be successful or not based on only 7 numerical features. Among those four ML algorithms, three algorithms are tree-based, and one algorithm is statistical-based. The reason for choosing a more tree-based algorithm is that it does not require normalization or standardization as a preprocessing of the features and still provides better accuracy than statistical-based algorithms [7]. Since a large amount of data is required as input to build ML or ANN models, the GTD dataset is used, which contains information on approximately 200,000 incidents of domestic and foreign terrorist activity from 1970 to 2017 [2]. The proposed model relies on only 7 of the 18 selected features from the GTD dataset to make this admirably accurate prediction. The nominal data dependency and multi-class classification make this model more effective compared to other methods. The performance evaluation of the implemented ML and ANN algorithms is based on the validation curves and the Area Under the Curve of Receiver Operating Characteristic (AUC-ROC) curves. In addition, the accuracy, precision, recall, and F1-Score are also calculated

979-8-3503-4602-2/22/$31.00 ©2022 IEEE

for all these ML models.

The remainder of this study is organized into section two, which provides a summary of relevant work. Section three describes the proposed methodology, and section four analyzes the results of the different ML and ANN algorithms. The entire study is then summarized in section five with additional suggestions for improvement.

II. Related Study

Nowadays, predicting the success rate of suicide attacks is an important area of research due to the increasing threat of terrorism worldwide. However, according to our study, not much research has been published on this topic using ML or ANN. In most cases, researchers use ML or ANN for a binary classification problem. However, a multiclass classification problem that combines the success and suicide of a terrorist attack is a good research area to predict the success rate of such an attack.

In [8], predictions of future terrorist activities are made using deep neural networks. First, the authors develop several models based on traditional machine learning techniques. The result shows that the models cannot make accurate predictions. The authors also create models based on Neural Networks (NN) and Deep Neural Networks (DNN) and find that DNN provides more than 95% accuracy, unlike the traditional ML models. In [9], machine learning algorithms such as Random Forest, Neural NET, and Support Vector Machine are used to simulate the threat of terrorist attacks. With a 96.6% success rate using Random Forest, the model can identify where terrorist attacks might occur. This model correctly predicts 2,037 locations for terrorist attacks. In [10], six supervised machine learning methods (Gaussian Naive Bayes, Linear Discriminant Analysis, k-Nearest Neighbors, Support Vector Machines, Decision Tree, and Logistic Regression) are used to predict the region and country of terrorist attacks. The results show that the Decision Tree provides the highest training accuracy 97.1%in both cases, i.e., predicting the country and region of terrorist attacks, while the Support Vector Machine and Logistic Regression provide the lowest training accuracy of 67%. The results also show that the highest testing accuracy is upto 82%. In [11], the authors propose a system to visualize and predict the number of terrorist attacks by region and attack type using classification models such as Random Forest and Decision Tree. After training the model, the decision tree provides 75.45% accuracy in predicting attacks by region. Also, the accuracy is 79.24% in predicting the types of terrorist attacks. On the other hand, Random Forest is accurate in predicting these things as it achieves 89.54% accuracy in predicting attacks by region. It is also 90.41% accurate in predicting the types of terrorist attacks. Interestingly, in [12], the authors combine the success and suicide of a terrorist attack and show a statistical analysis.

Since no multiclass classification has been done so far, four ML models and an ANN model are used in our study to predict the success of a suicide terrorist attack by using only 7 features. Also, a comparison among all of these models is shown in this research.

III. Methodology

The methodology used in this study is shown in Figure 1. The first step of the procedure is to impute the missing values from the GTD dataset. The Miss Forest algorithm [13] is employed to fill the missing values. After dealing with the missing values, the features ”success” and ”suicide” are merged to form the multiclass target feature named ”Target” for multiclass classification. Since this dataset is imbalanced, it is made balanced using the Synthetic Minority Over-sampling Technique (SMOTE) [14]. Features are then selected using the Feature Selection [15] method to predict the target feature once the importance of each feature is determined. Finally, the machine learning models are set in motion. Each step of the proposed strategy is briefly explained in the following sections.

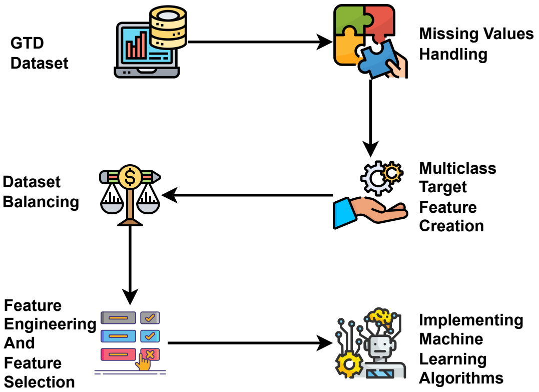
GTD Dataset
Missing Values Handling
Multiclass Target Feature Creation
Dataset Balancing
Feature Engineering And Feature Selection
Implementing Machine Learning Algorithms

Fig. 1. Different Phases of the Methodology Employed in this Study.

A. Dataset Description

Information on terrorist attacks worldwide from 1970 to 2017 is collected using the dataset commonly known as the Global Terrorism Database (GTD) [2]. Unlike many other databases, the GTD presently has almost 200,000 cases with at least 45 variables per occurrence. It also provides systematic data on domestic, transnational, and worldwide terrorist acts during this time. At GTD, everything is shown at each event, including the time and place, the weapons used, the kind of target, the number of victims, and the identified group or person responsible. Among all of these features, 18 of them were chosen. All of the chosen qualities are numeric and have some values that are missing. The Miss Forest algorithm [13] is used to fill in the missing values. An overview of the dataset can be found in Table I.

B. Target Creation

In this dataset, there are two attributes named “success” and “suicide”, which are binary attributes with values of either 1 or 0. Using the binary attributes, a multiclass target feature has been created named “Target” for multiclass classification. The Algorithm 1 describes the procedure of target creation.

TABLE I
OVERVIEW OF THE GTD DATASET

No	Attributes	Types	Information
1	iyear	int64	Year
2	iday	int64	Day (1/2/3.../30)
3	success	int64	1 = ”Yes” The incident was successful. 0 = ”No” The incident was not.
4	attacktype1	int64	This field captures the general method of attack.
5	targtype1	int64	The target type field captures the general type of target.
6	natlty1	float64	This is the nationality of the target that was attacked.
7	weaptype1	int64	Types of weapon are recorded for each inciden
8	kill	float64	This field stores the number of total confirmed fatalities for the incident.
9	extended	int64	1 means duration of an incident extended more than 24 hours 0 means less.
10	country	int64	This field identifies the country or location where the incident occurred.
11	region	int64	This field identifies the region in which the incident occurred.
12	latitude	float64	This field records the latitude of the city in which the event occurred.
13	longitude	float64	This field records the longitude of the city in which the event occurred
14	specificity	float64	This field identifies the geospatial resolution of the latitude and longitude.
15	vicinity	int64	1 = ”Yes” The incident occurred in the immediate vicinity and 0 = ”No”
16	crit1	int64	These variables record which of the inclusion criteria are met.
17	suicide	int64	1 = ”Yes” The incident was a suicide attack. 0 = ”No” This is not
18	nperps	float64	Indicates the total number of terrorists participating in the incident.

Algorithm 1 Target selection using features: “success” and “suicide”

```
if $success$ is 1 and $suicide$ is 1 then
    return 1
else if $success$ is 0 and $suicide$ is 0 then
    return 0
else if $success$ is 1 and $suicide$ is 0 then
    return 2
else if $success$ is 0 and $suicide$ is 1 then
    return 3
```

Here it can be seen that both the success and suicide features return 1 if they contain the binary number 1. This 1 in the target feature indicates that the terrorist attack is successful and the perpetrator attempts to commit suicide. If the suicide is 0 and the success is 1, 2 is returned. And in the target feature, this 2 means that although the terrorist attack is successful, the perpetrator is not able to commit suicide. If success is 0 and suicide is 1, 3 is returned. This 3 in the target feature indicates that although the terrorist attack is unsuccessful, the terrorist manages to commit suicide. However, if both success and suicide contain 0, 0 is returned, indicating that neither the terrorist attack nor the suicide attempt is successful.

C. Balancing Imbalanced Dataset

Since the fundamental principle of most classification techniques is that the class distribution should be balanced, methodologies for classifying imbalanced datasets cannot produce a good classification with ideal accuracy. [14]. In this case, the two features named “success” and “suicide” are combined to create the target feature called “Target”. There are four classes in this target feature, and they are:

- 1 (Represents success and suicide both)
- 2 (Represents only success)
- 3 (Represents only suicide)
- 0 (Represents none of these success and suicide)

This “Target” feature is imbalanced because there are large differences in the ratio of these four classes. The success cases, which are essentially in class 2, account for about 84.9% of the data in this “Target” feature. Slightly more than 10.45% of the data do not belong to either the success cases or the suicide cases, thus belonging to class 0. These two cases, success and suicide, account for about 3.06% of the dataset classified as class 1, while only the suicide attacks, classified as class 3, account for 1.59% of the dataset.

It is more likely that this model would be overfitted because the dataset is imbalanced. To balance this dataset, instances for the minor category are created using the Random Oversampler method and the Synthetic Minority Oversampling Technique (SMOTE). Figure 2 shows the scenarios of the dataset before and after applying the balancing procedure.

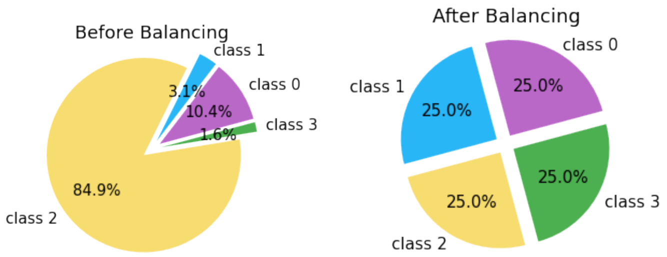

Fig. 2. Overview of the Distribution of Target Data Feature Before and After Performing Balancing Procedure on Dataset.

D. Feature Engineering and Feature Selection

After creating the target feature and balancing the dataset, the feature engineering methodology is applied. The attributes that are correlated to 80% are discarded. This 80% correlation indicates that these features are almost 80% correlated with each other and it is unnecessary to take both of them; instead, one is taken while the other is omitted.

Following the correlation matrix in Figure 3, a feature selection strategy is applied to the selected features. This feature selection approach employs lasso regression by setting 0.05 as the threshold. This Figure 3 shows the correlation coefficients between variables. Each cell in the table represents the relationship between two variables [16]. This correlation matrix illustrates how the features are related to each other. After excluding all correlated features, 7 features (iyear,attacktype1, targtype1, natity1, nkill, country, and latitude) are selected for the machine learning models.

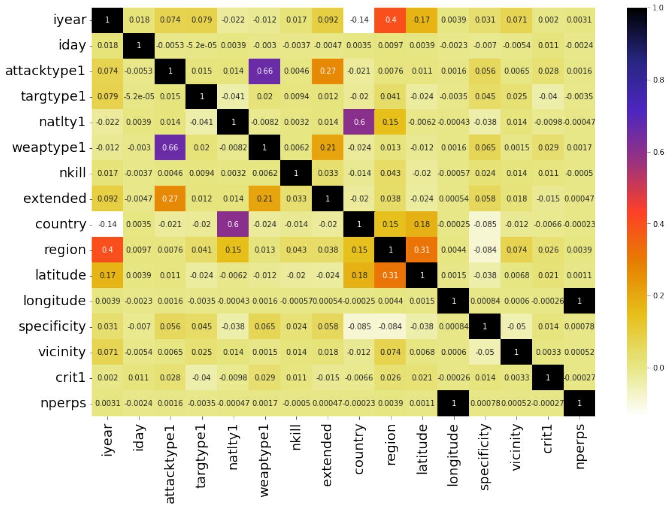

Fig. 3. Correlation Matrix of the Selected Features.

E. Applied Machine Learning and Artificial Neural Network Models

Various ML and ANN models are used to predict the target. The algorithms are trained with 70% of the dataset for training purposes, and the remaining 30% are used for testing. The accuracy of these machine learning algorithms is increased by using K-fold cross-validation (K = 10) and specifying the "random state" for all algorithms to be 42. For the MLP, the architecture is a fully connected network with 2 hidden layers, where the first hidden layer has 12 units and the second layer has 6 units. The architecture is shown in Figure: 4. The accuracy and F1-Score of each machine learning algorithm are also calculated.

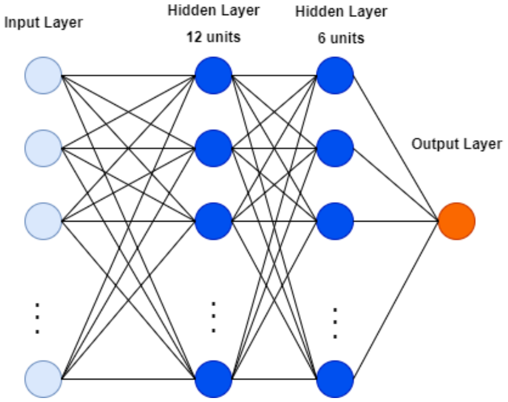

Fig. 4. Architecture of the MLP Model.

IV. Results Analysis

A. Confusion Matrix

A confusion matrix is an MXM matrix used to evaluate the effectiveness of a classification model, where M is the number of target classes [17]. The matrix compares the actual values with the predictions of the machine learning model. This provides a comprehensive picture of how well the classification model is performing and what types of errors it is generating. Figure 5 shows five confusion matrices for five algorithms used in this study.

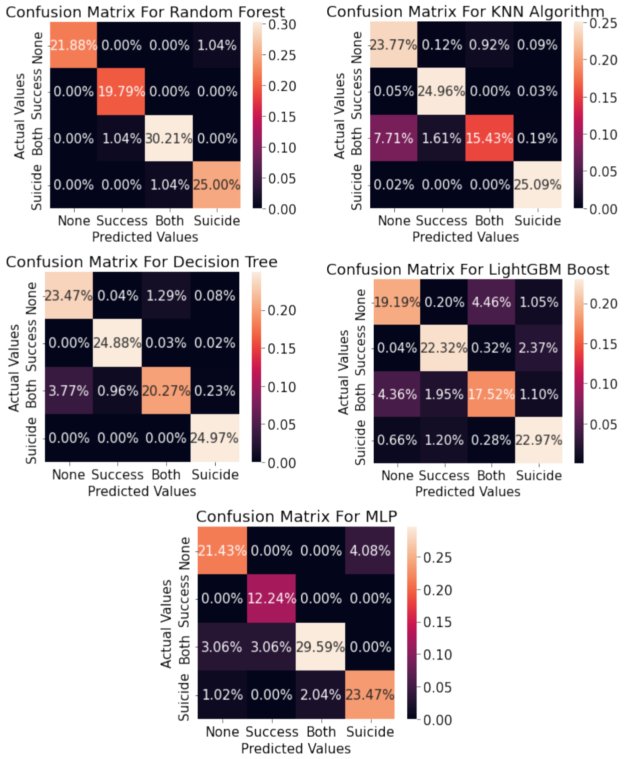

Fig. 5. Confusion Matrix for Different Machine Learning and Artificial Neural Network Algorithms.

According to these confusion matrices, only 3.12% of the data is misclassified by the Random Forest Classifier, while a Decision Tree misclassifies the data by almost 6.42%. Compared to other algorithms, KNN shows very poor performance. In this case, almost 10.71% of the data is misclassified. Interestingly, 13.24% of the data is misclassified by MLP. Here 4.08% of the data is classified as a successful attack, but in fact, there is neither a successful nor a suicide attack.

B. Validation Curves

Using the validation curves, it is found that Random Forest maintains its accuracy for all unknown data to predict the target, as increasing the number of epochs does not affect its accuracy, which is around 93.4%. The Decision Tree performs well when the number of epochs increases. Surprisingly, the validation curve for the KNN remains mostly constant with an accuracy of around 82.3%, but its training accuracy decreases as the number of epochs increases. LightGBM performs consistently, but its training accuracy increases after the 7^{th} epoch. For MLP, it is interesting to note that as the epoch number increases, the validation accuracy also increases. After 11^{th} epoch, it becomes almost constant, with an accuracy of around 84.5%. All these curves are shown in Figure 6.

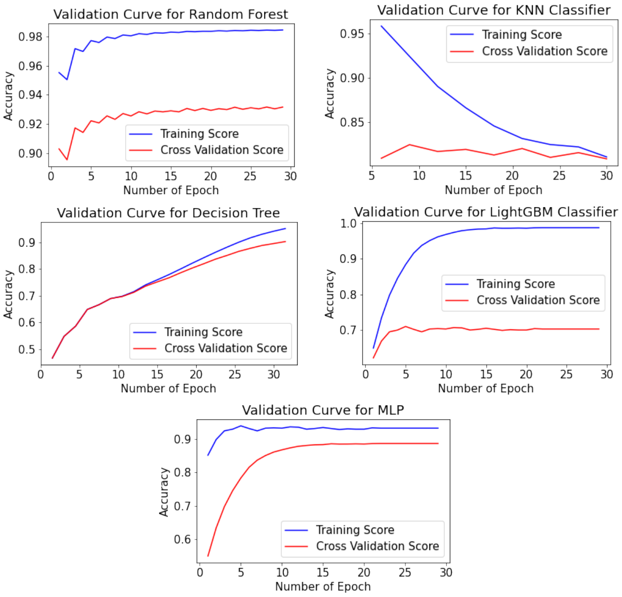

Fig. 6. Validation Curves for Different Machine Learning and Artificial Neural Network Algorithms.

C. AUC-ROC Curve

One of the most used evaluation metrics for binary classification issues is the Area Under the Curve of Receiver Operating Characteristic (AUC-ROC). A ROC curve is a graph that shows how well a classification model performs across all categorization levels [18]. The classification accuracy is enhanced by lowering the classification threshold. Plotting the True Positive Rate (TPR) and False Positive Rate (FPR) as a function of the ROC curve shows TPR on the y-axis and FPR on the x-axis. The area under the ROC curve in two dimensions is quantified by AUC. The accuracy of the model's prediction increases with increasing AUC-ROC score. All ROC curves for the different machine learning methods used in this study are shown in Figure 7. To represent the ROC curve, four separate graphs are plotted for a single algorithm with respect to the other classes, since the ROC curve reflects only the binary classification.

The Random Forest algorithm outperforms the other algorithms by correctly identifying the majority of samples and achieving an AUC-ROC score of approximately 98.93%. The classes represented as only suicide and none or both success and suicide are mostly correctly classified by the KNN and Decision Tree algorithms. However, these two algorithms misclassify the success cases of a terrorist attack, and the scores of AUC-ROC are 96.1% and 96.4%, respectively. The performance of LightGBM algorithms is quite good in this study. It can perform accurate classification when the target feature contains only success and both success and suicide cases. The AUC-ROC score for LightGBM Boosting is 93.67%. Finally, the MLP does not perform very well in this study. Its AUC-ROC score is around 89.23%, and it can better distinguish the classes containing only success cases.

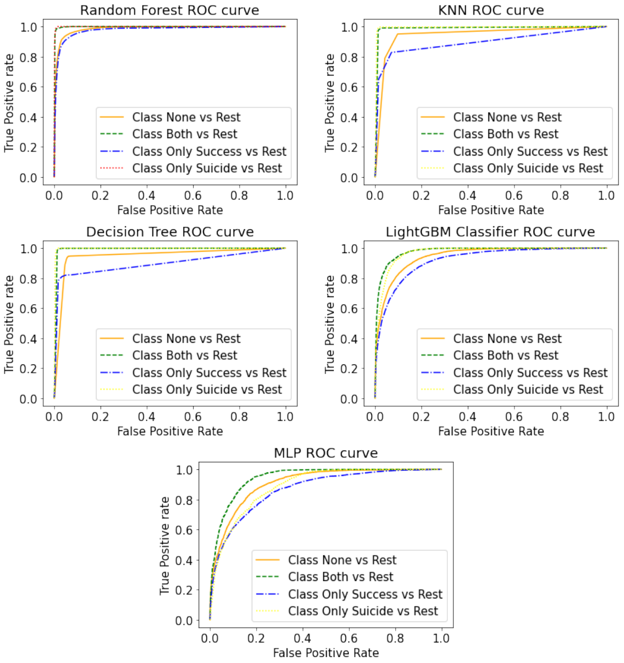

Fig. 7. ROC curves for Different Machine Learning and Artificial Neural Network Algorithms.

The AUC-ROC scores obtained in the experiment are shown in Table II.

TABLE II
AUC-ROC SCORES ACHIEVED FROM THE EXPERIMENT.

Algorithm	AUC-ROC(%)
Random Forest	98.93
KNN	96.1
Decision Tree	96.4
LightGBM Boosting	93.67.7
MLP	89.23

D. Accuracy, Precision, Recall and F1-score

In addition to the AUC-ROC curve, accuracy, precision, recall, and F1-Score are well-known evaluation metrics commonly used to measure the performance of the employed models. These metrics are widely used in various ML and ANN. applications [7], [19], [20]. Four machine learning models are used to predict the target attribute, among which Random Forest outperforms all with 98.39% accuracy. Decision Tree also performs well with 97.54% accuracy. The remaining algorithms also perform well with reasonable accuracy, except MLP. Since the target has multiple defining features, it is easier for traditional machine learning algorithms to accurately classify unknown data than for the MLP model. Figure 8 shows the comparative analysis of accuracy, precision, recall, and F1-Score of all algorithms used in this study. From the comparative analysis, Random Forest is the winner among the algorithms used, while KNN and Decision Tree also perform very well in predicting the target class with accuracy above 95% in this dataset. Table III shows the performance comparison with the best accuracy of the existing models and the best accuracy of this study.

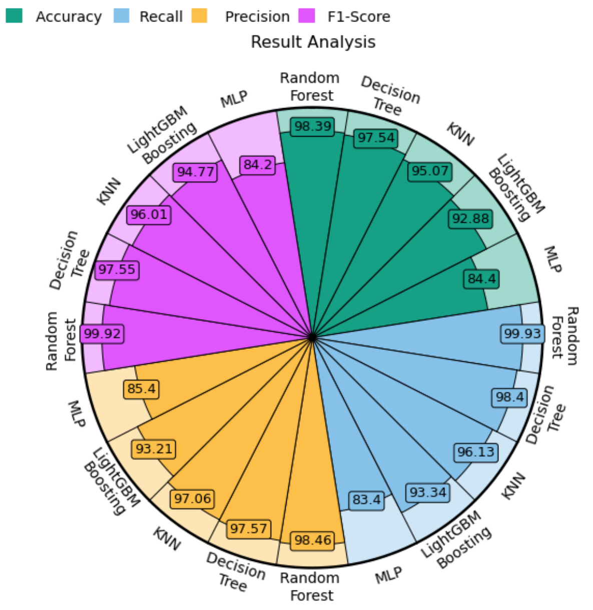

Fig. 8. Result of Different Machine Learning and ANN Algorithms.

TABLE III
COMPARATIVE ANALYSIS WITH THE EXISTING WORKS.

Study	Approach		Highest Accuracy
	Algorithm	Classification	
Uddin et al. [8]	ANN and ML	Binary class	DNN: 95.11%
Ding et al. [9]	ML	Binary class	Random Forest: 96.61%
Singh et al. [10]	ML	Binary class	Decision Tree: 97.12%
Huaman [11]	ML	Binary class	Random Forest: 89.52%
This study	ANN and ML	Multiclass	Random Forest: 98.42%

V. Conclusions and Future work

Terrorism is a global problem that damages a country's security and reputation, as well as the confidence and lives of its citizens. Terrorism changes citizens' perceptions of real life. However, terrorism can be contained if its underlying factors can be identified. These factors can be easily identified with modern technologies such as machine learning. To determine the success of a suicide terrorist attack, several machine learning and ANN models have been developed. The results of this study show that Random Forest has the highest accuracy of 98.39% compared to the other four algorithms. The results of this study can be used to improve future defense against terrorist attacks. In the future, other types of terrorism and their factors (e.g., the success rate of a terrorist attack related to the type of weapon used) can be studied using different machine learning or ANN algorithms, which will help reduce terrorism and improve security.

References

[1] C. L. Ruby, "The definition of terrorism," *Analyses of social issues and public policy*, vol. 2, no. 1, pp. 9–14, 2002.

[2] G. LaFree and L. Dugan, "Introducing the global terrorism database," *Terrorism and political violence*, vol. 19, no. 2, pp. 181–204, 2007.

[3] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, oct 2001. [Online]. Available: https://link.springer.com/article/10.1023/A:1010933404324

[4] J. R. Quinlan, "Induction of decision trees," *Machine learning*, vol. 1, no. 1, pp. 81–106, 1986.

[5] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, "Lightgbm: A highly efficient gradient boosting decision tree," *Advances in neural information processing systems*, vol. 30, pp. 3146–3154, 2017.

[6] E. Fix and J. L. Hodges, "Discriminatory analysis. nonparametric discrimination: Consistency properties," *International Statistical Review/Revue Internationale de Statistique*, vol. 57, no. 3, pp. 238–247, 1989.

[7] S. S. Islam, M. S. Haque, M. S. U. Miah, T. B. Sarwar, and R. Nugraha, "Application of machine learning algorithms to predict the thyroid disease risk: an experimental comparative study," *PeerJ Computer Science*, vol. 8, p. e898, 2022.

[8] M. I. Uddin, N. Zada, F. Aziz, Y. Saeed, A. Zeb, S. A. Ali Shah, M. A. Al-Khasawneh, and M. Mahmoud, "Prediction of future terrorist activities using deep neural networks," *Complexity*, vol. 2020, 2020.

[9] F. Ding, Q. Ge, D. Jiang, J. Fu, and M. Hao, "Understanding the dynamics of terrorism events with multiple-discipline datasets and machine learning approach," *PloS one*, vol. 12, no. 6, p. e0179057, 2017.

[10] K. Singh, A. S. Chaudhary, and P. Kaur, "A machine learning approach for enhancing defence against global terrorism," in *2019 Twelfth International Conference on Contemporary Computing (IC3)*. IEEE, 2019, pp. 1–5.

[11] E. L. Huamaní, A. M. Alicia, and A. Roman-Gonzalez, "Machine learning techniques to visualize and predict terrorist attacks worldwide using the global terrorism database," *Machine Learning*, vol. 11, no. 4, 2020.

[12] C. Santifort-Jordan and T. Sandler, "An empirical study of suicide terrorism: A global analysis," *Southern Economic Journal*, vol. 80, no. 4, pp. 981–1001, 2014.

[13] D. J. Stekhoven and P. Bühlmann, "Missforest—non-parametric missing value imputation for mixed-type data," *Bioinformatics*, vol. 28, no. 1, pp. 112–118, 2012.

[14] K. Li, W. Zhang, Q. Lu, and X. Fang, "An improved smote imbalanced data classification method based on support degree," in *2014 International Conference on Identification, Information and Knowledge in the Internet of Things*. IEEE, 2014, pp. 34–38.

[15] A. Jović, K. Brkić, and N. Bogunović, "A review of feature selection methods with applications," in *2015 38th international convention on information and communication technology, electronics and microelectronics (MIPRO)*. Ieee, 2015, pp. 1200–1205.

[16] H. F. Kaiser and K. Dickman, "Sample and population score matrices and sample correlation matrices from an arbitrary population correlation matrix," *Psychometrika*, vol. 27, no. 2, pp. 179–182, 1962.

[17] M. Khaled, A. Bin, M. Hossain, S. Rahman, J. Ferdaus *et al.*, "Multiclass classification for gvhd prognosis prior to allogeneic stem cell transplantation," in *Australasian Joint Conference on Artificial Intelligence*. Springer, 2022, pp. 487–500.

[18] Z. H. Hoo, J. Candlish, and D. Teare, "What is an roc curve?" pp. 357–359, 2017.

[19] S. Ahsan, S. T. Nawaz, T. B. Sarwar, M. S. U. MIAH, and A. Bhowmik, "A machine learning approach for bengali handwritten vowel character recognition," *IAES International Journal of Artificial Intelligence*, vol. 11, no. 3, 2022.

[20] N. Alfaz, T. B. Sarwar, A. Das, and N. M. Noor, "A densely interconnected convolutional neural network-based approach to identify covid-19 from chest x-ray images," in *Proceedings of the 11th International Conference on Robotics, Vision, Signal Processing and Power Applications*. Springer, 2022, pp. 419–425.