International Journal of Scientific Advances
ISSN: 2708-7972
Volume: 6 | Issue: 3 | May – Jun 2025 Available Online: www.ijscia.com
DOI: 10.51542/ijscia.v6i3.29

Analyzing and Predicting of Global Terrorism Attacks Based on Machine Learning

Alor Kuol Chol Mayom, YE Shiren*

School of Computer Science and Artificial Intelligence,
Changzhou University, Changzhou, China, 213164

E-mail: atkuols@gmail.com; yes@cczu.edu.cn

*Corresponding author details: YE Shiren; yes@cczu.edu.cn

ABSTRACT

Terrorism poses a complex and pervasive threat to global security and sustainable development. Over 200,000 terrorist attacks have been documented since 1970, resulting in significant human casualties, extensive property damage, and widespread social unrest. These incidents not only disrupt daily life but also impede economic progress, underscoring the necessity of robust counter-terrorism strategies within the framework of global security governance. Although patterns in terrorist activities may appear random, they are often intentional and systematically organized, reflecting identifiable characteristics that can inform targeted preventive measures. Leveraging open-source datasets such as the Global Terrorism Database (GTD), researchers have constructed analytical and predictive models employing machine learning, clustering, and classification techniques. Various studies have introduced innovative predictive frameworks, including hybrid classifiers, risk assessment models, and deep learning architectures. These advancements contribute to more effective early warning systems and enhanced operational efficiency in counter-terrorism initiatives, with the goal of minimizing human losses and strengthening global security.

Keywords: counter-terrorism machine learning; data analytic; GTD dataset; terrorism classification; feature extraction; risk assessment.

INTRODUCTION

Terrorist attacks typically exhibit high lethality and destructiveness, directly leading to substantial casualties and significant property damage. Furthermore, they impose considerable psychological stress on the affected populations. Overall, these incidents contribute to varying degrees of social instability, disrupting the normal order of work and daily life, and consequently impeding economic development. The analysis and prediction of terrorist attacks facilitate targeted actions against terrorist organizations by providing actionable intelligence for counter-terrorism and preventive operations. This enables authorities to identify emerging or concealed terrorist entities at an early stage, thereby minimizing human and material losses, proactively addressing potential threats, and enhancing the overall security and stability of societal systems.

The patterns of attacks planned and executed by terrorists may appear random at first glance; however, they are typically organized and premeditated actions that are carefully selected and deliberately carried out. Furthermore, attacks conducted by the same terrorist organizations or individuals often exhibit notable similarities in terms of identifiable characteristics. Therefore, there are likely underlying patterns or informal rules that guide the operational behaviors of terrorist groups. By analyzing these characteristic activity patterns, authorities can develop more accurate predictions and in-depth analyses of potential terrorist attack occurrences.

The patterns of attacks planned and carried out by terrorists may appear random at first glance; however, they are typically organized and premeditated actions that are carefully selected and deliberately executed. Furthermore, attacks conducted by the same terrorist organizations or individuals often exhibit consistent characteristics, suggesting the presence of underlying behavioral patterns. These recurring features can be leveraged for the analysis and prediction of future terrorist activities. Ding et al. proposed a novel approach that utilizes widely adopted and robust machine learning techniques to simulate the global risk of terrorist attacks. Their method is based on multi-source data, long-term time series, and geographically distributed datasets, enabling large-scale modeling and risk assessment of terrorism dynamics.

The model demonstrated relatively effective performance in predicting potential locations of terrorist events in 2015. Chuang et al. investigated

the spatial-temporal patterns of terrorist attacks conducted by Al Qaeda (AQ), the Islamic State of Iraq and Syria (ISIS), as well as various local militias and insurgent groups. They applied data-driven, unsupervised k-means clustering to the Global Terrorism Database (GTD) to identify underlying structures in attack patterns.

Petroff et al. proposed a hidden Markov model to generate early warnings for specific types of terrorist attacks. Gohar et al. introduced a novel framework for classifying and predicting terrorist organizations. This framework incorporates four basic classifiers: Naive Bayes (NB), k-nearest neighbor (KNN), Iterative Dichotomous 3 (ID3), and a decision stump (DS).

Tolan et al. employed classification techniques to compare the performance of five fundamental classifiers including Naive Bayes, KNN, and support vector machine (SVM), and utilized the GTD to analyze terrorism trends and terrorist group behaviors. Meng et al. proposed an optimized hybrid classification framework that integrates data collection, preprocessing, hybrid classification, mining, and classifier testing for predicting terrorist attacks.

Bu et al. combined a support vector machine (SVM) with an Intelligent Tuned Harmony Search (ITHS) algorithm to develop the ITHSSVM model for terrorist attack prediction. Li et al. presented a comprehensive analytical framework that integrates social network analysis, wavelet transform, and pattern recognition methods to explore the dynamics of terrorist group behavior and ultimately predict their future attack patterns.

Hu et al. developed a risk assessment system for terrorist attacks through a quantitative analysis of the GTD. They clustered and ranked terrorist attacks based on the outcomes of terrorist attack rating models. Campedeli et al. proposed the use of temporal meta-graphs and deep learning techniques to forecast future terrorist targets, using real-world attack data from Afghanistan and Iraq between 2001 and 2018. Experimental results indicated that bidirectional LSTM networks outperformed other algorithms in forecasting accuracy

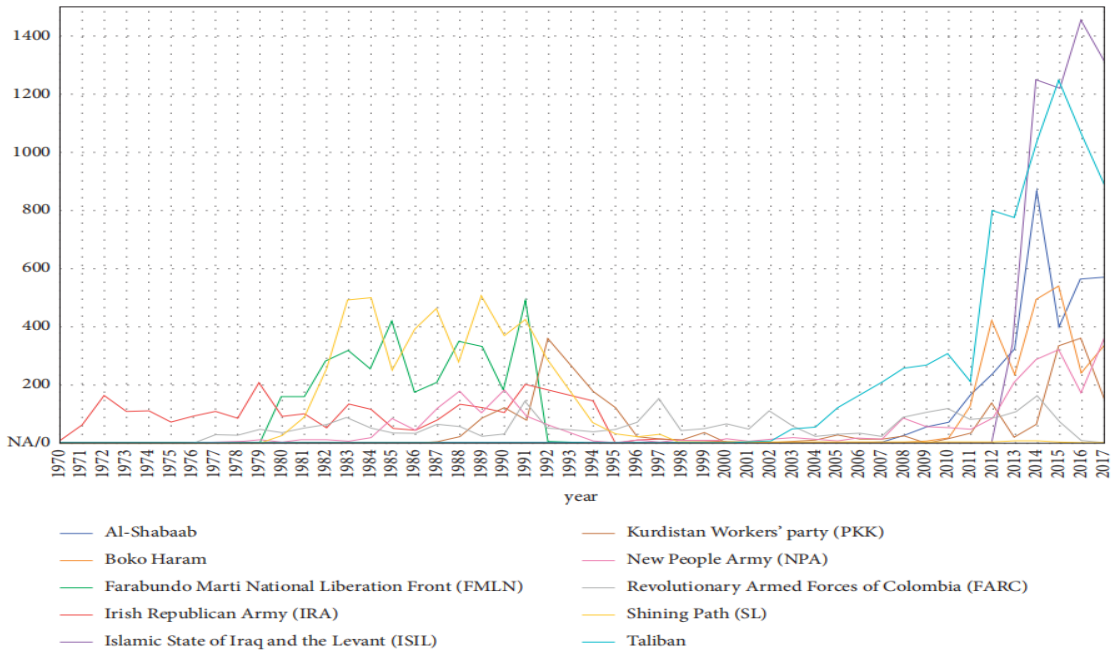


FIGURE 1: The annual distribution of the top 10 terrorist organizations.

Machine learning methods are usually divided into supervised and unsupervised approaches within the Former category, many applications aim at predicting a target variable. The specific method involves establishing a corresponding relationship between the attribute variables and the target variables in the sample dateset, and this mapping relationship is formed by constructing a model from the training dateset. The prediction and evaluation are performed on the testing dateset, and the value of the predicted target variables is then compared with the value of real target variables to derive the prediction accuracy.

For a given terrorist attack, the classification models identify terrorist organizations or individuals in a terrorist attack based on known attribute fields. In the process of supervised machine learning, the existing terrorist event feature data are sent to the classification algorithm model for training and learning. Then, the trained model is used to classify the test or new data to predict candidate terrorist organizations or individuals. Therefore, the prediction of terrorist organizations is a multi-classification problem. The primary purpose of this research is to construct classification models for multi-classification tasks. In this study, we used five supervised machine learning classifiers to predict terrorist organizations responsible for various attacks, in including decision trees, bootstrap aggregating, random forests, extra trees, and super gradient boost.

Decision tree (DT) algorithms can be used as a supervised learning method. By creating a tree model to learn simple decision rules from data features to predict the value of a target variable, the DT model begins the decision from the root node, and the leaf nodes represent a successful guess or correct prediction. There are three major algorithms for creating DTs: ID3, C4.5, and Classification and Regression Tree (CART). ID3 starts from the root node of the tree and uses information gain to select features to build child nodes. C4.5 uses the information gain ratio to select features, which is regarded as an improvement of ID3.

However, these two algorithms cause the problem of over-fitting, which requires pruning. The pruning of the DT removes unnecessary classification features by optimizing the loss function and reducing the overall complexity of the model. CART adopts the Gini index minimization principle to create a tree. It cuts out some sub-trees from the bottom of a fully-grown DT, making the model simpler. We used CART to create decision trees in this study. The following four models are considered ensemble learning, which is a branch of machine learning. The basic unit of these four models is a decision tree.

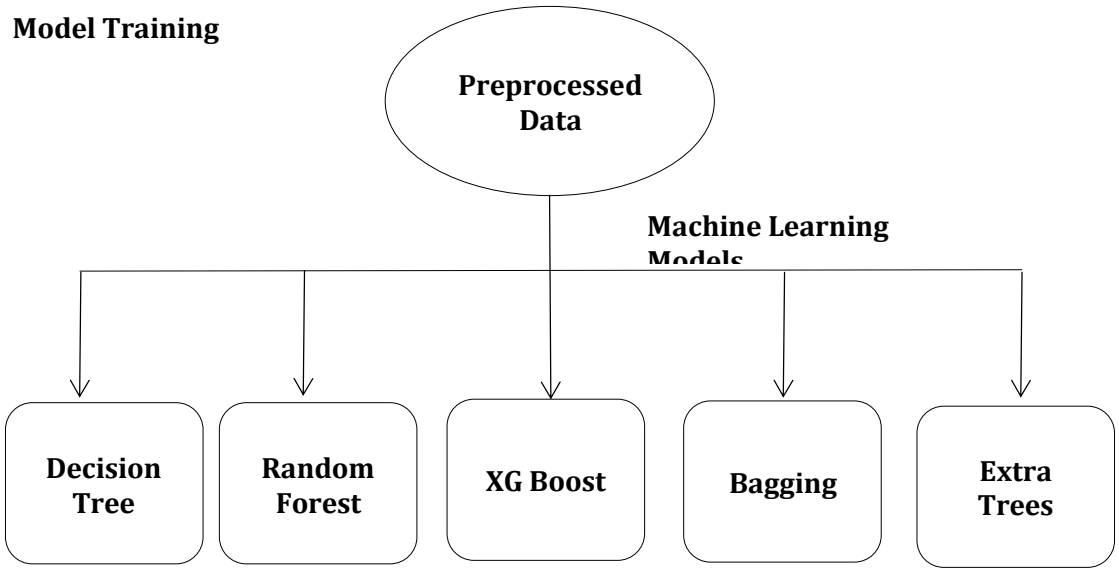
Bootstrap aggregating (Bagging) is a classification algorithm that uses a combination strategy. It first obtains *m* sample sets by extracting the original dataset *m* times with replacement and then uses each sample set to train *m* base classifiers separately. Finally, an integrated classifier was constructed by applying a combination strategy to the base classifiers. Random forest (RF) is an algorithm that integrates multiple DTs through ensemble learning. RF usually uses the mean or mode of the prediction results of each DT in the decision tree set as the final prediction value. The RF in the scikit-learn Python package uses the mean as a predictor.

Compared with a single DT, RF is less likely to be affected by overfitting because each DT of the random forest cannot see the full view of the training set. Each DT only trained a part of the attribute data and did not remember all the noise of the training set.

Extra trees (ET) are also composed of many DTs, such as RF. These decision trees use random features and random thresholds for the node division. ET provides additional randomness, which suppresses overfitting but also increases the bias to some extent. The difference between ET and RF is that RF uses bagging for random sampling, whereas ET uses all samples. RF finds the optimal attributes based on information entropy and the Gini index in a random subset, while ET finds an eigenvalue entirely at random to divide.

The super gradient boost (XGBoost) is also a classification algorithm that integrates multiple decision trees. It pays more attention to the samples that were learned incorrectly in the previous round during training and makes some improvements on Gradient Boosting by introducing second-order derivatives and approximating the loss function with first- and second-order derivatives so that there is more information in the optimization process. In addition, XGBoost adds a regular term to the loss function to weigh the complexity of the model, making it simpler and preventing overfitting. Compared with the RF, there is no dependency relationship between the decision trees in the RF, and they can be parallel. However, XGBoost trees are dependent and must be serialized. This model maximizes the integration speed and efficiency of trees and is a very effective integration algorithm.

Evaluation Metrics. After the machine learning classification model for this problem was designed and constructed, it was necessary to evaluate the performance of a classifier to determine the accuracy of a classifier in predicting the class labels of terrorist organizations.



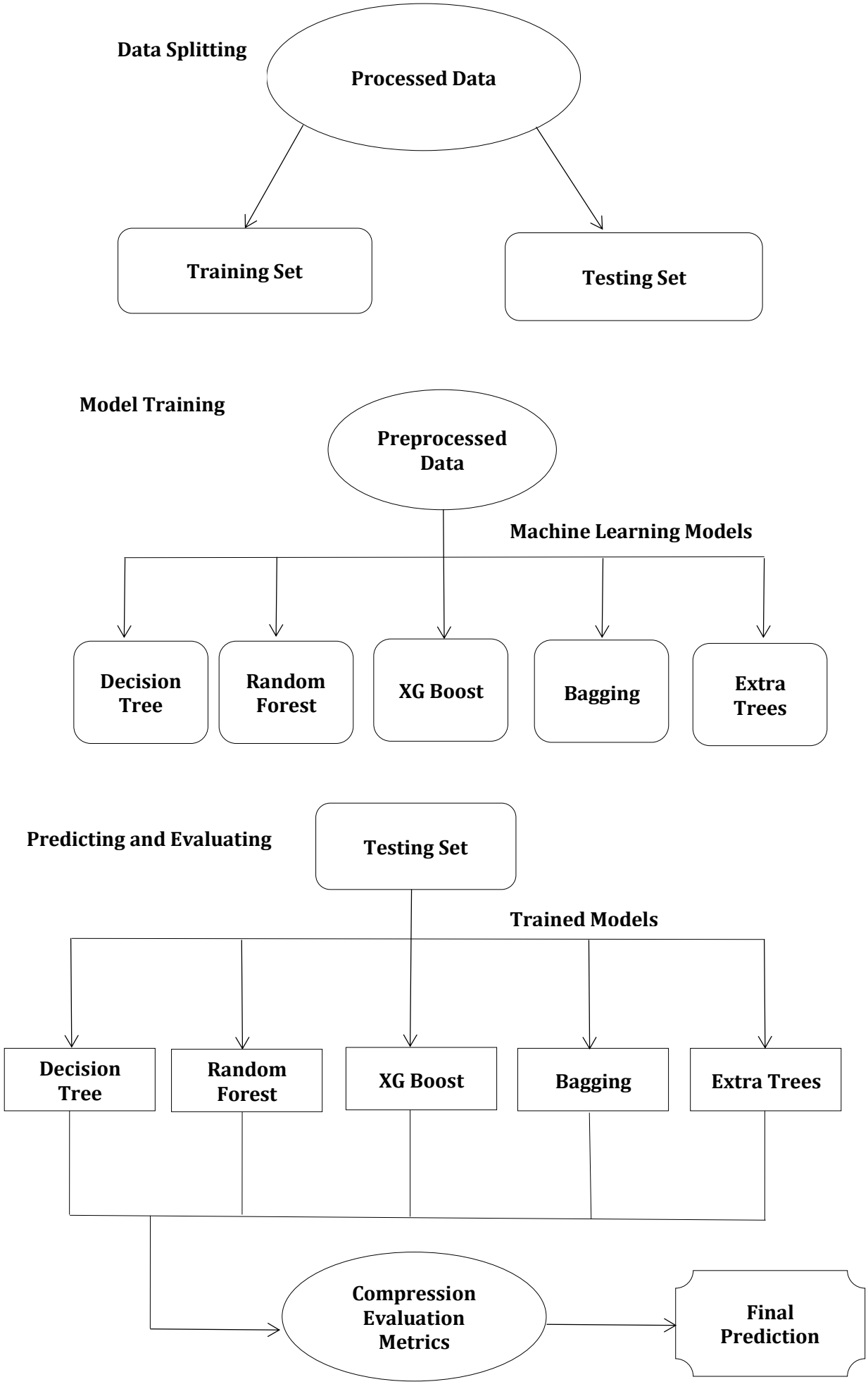


FIGURE 2: The framework for classifying and predicting terrorist organizations.

In machine learning, a multi-class classification problem can usually be converted into multiple binary classification problems. Each binary classification problem classifies a group of target objects into one class (i.e., category) and the remaining target objects into another class. The confusion matrix is an analysis table that summarizes the prediction results and the real results in binary classification and multi-class classification as shown in Table. Based on confusion matrices, four commonly used metrics are generally applied to evaluate the performance of machine learning, including accuracy, precision, recall, and *F*1 scores sufficient to reflect the detail of the assessment results. The *F*1 score is the harmonic mean value of the precision and recall.

TABLE 1: Performance Comparison of Machine Learning Classifiers using Hold-Out and 10-Fold Cross-Validation.

Metrics		Data split verification method			
		Hold-out method	10-fold cross-validation method		
			Mean	Max	Min
Accuracy	Decision trees	0.958647	0.956026	0.964387	0.949943
	Bagging	0.931989	0.933528	0.936764	0.927569
	Random forests	0.968216	0.965974	0.968744	0.962647
	ExtraTrees	0.959501	0.959406	0.962400	0.956011
	XGBoost	**0.971634**	**0.967778**	0.970828	0.963216
Precision	Decision trees	0.928242	0.929096	0.943624	0.918073
	Bagging	0.932152	0.927242	0.938100	0.911614
	Random forests	**0.957727**	**0.955594**	0.963753	0.947774
	ExtraTrees	0.942159	0.941508	0.945737	0.935197
	XGBoost	0.957246	0.952817	0.956800	0.943972
Recall	Decision trees	0.929554	0.931822	0.944081	0.923149
	Bagging	0.858106	0.862504	0.871233	0.854989
	Random forests	0.934140	0.934952	0.941422	0.929029
	ExtraTrees	0.926234	0.928944	0.934792	0.923533
	XGBoost	**0.944904**	**0.942287**	0.950476	0.933696
*F*1 score	Decision trees	0.928603	0.930063	0.943702	0.920590
	Bagging	0.875151	0.875903	0.886239	0.866793
	Random forests	0.942883	0.942658	0.949366	0.935658
	ExtraTrees	0.932798	0.933608	0.937390	0.927087
	XGBoost	**0.950011**	**0.946542**	0.953123	0.937474

TABLE 2: Performance Metrics of Machine Learning Classifiers Across Varying Scales of Terrorist Attacks.

Summary of data records	Number of terrorist attacks (range)	≥1000	≥500	≥100	≥50	≥5
	Number of terrorist organizations	19	32	122	210	936
	Total number of terrorist attacks	50200	58520	78107	84339	94871
Accuracy	Decision trees	0.982669	0.958647	0.878377	0.854636	0.796164
	Bagging	0.960757	0.931989	0.833312	0.799858	0.740620
	Random forests	0.983068	0.968216	**0.904494**	**0.881195**	**0.835687**
	ExtraTrees	0.979283	0.959501	0.886698	0.860327	0.803225
	XGBoost	**0.983466**	**0.971634**	0.853924	0.791439	0.698567
Precision	Decision trees	0.976950	0.928242	0.787521	0.745648	0.478754
	Bagging	0.945956	0.932152	0.771253	0.685609	0.347113
	Random forests	**0.979232**	**0.957727**	**0.847559**	**0.817384**	**0.520747**
	ExtraTrees	0.973327	0.942159	0.811242	0.761273	0.476816
	XGBoost	0.978406	0.957246	0.752235	0.523490	0.126893
Recall	Decision trees	**0.976073**	0.929554	**0.786034**	0.737920	**0.512161**
	Bagging	0.940090	0.858106	0.605144	0.523339	0.304769
	Random forests	0.974743	0.934140	0.785265	**0.739619**	0.511993
	ExtraTrees	0.970025	0.926234	0.761510	0.708550	0.469377
	XGBoost	0.976059	**0.944904**	0.746525	0.537858	0.138689
*F*1 score	Decision trees	0.976497	0.928603	0.784185	0.736470	0.481310
	Bagging	0.941057	0.875151	0.633059	0.551191	0.305712
	Random forests	0.976587	0.942883	**0.805488**	**0.754597**	**0.502975**
	ExtraTrees	0.971609	0.932798	0.779096	0.723834	0.459432
	XGBoost	**0.977118**	**0.950011**	0.745925	0.523800	0.130349

Accuracy is defined as the ratio of correctly predicted samples to the total number of samples. It is the percentage of terrorist organizations correctly classified in an attack. Precision is the ratio of true positive samples among all samples predicted as positive samples. Recall is the ratio of the number of positive samples predicted to the total number of all positive samples. For specific terrorist organization *i*, precision.

TABLE 3: Precision and Accuracy Category Ratio.

PREDICTION CATEGORY		
Actual Category	**True**	**False**
True	True Positive (TP)	False Negative (FN)
False	False Positive (FP)	True Negative (TN)

METHODOLOGY

Recovery methods

Analysis and modeling prediction of global terrorist attacks were performed in Python 3.6, running on a platform with an Intel Core i7 processor and 24.00 GB DDR RAM.

We utilized the Python libraries pandas-0.25.2, numpy-1.17.2, xgboost-1.0.0, and scikit-learn-0.21.3 For visualization of the analysis results, we used seaborn-0.9.0 and matplotlib- 3.1.1 in Python.

Data Structure Analysis. The data primarily contained the following attributes of information: GTD serial number, date, event description information, time, location, attack description information, weapon information, target information, victim information, casualty information, and action results. There were many fields under each type of information to enrich the data. Each terrorist attack was stored as a record (i.e., a row) of 137 attributes such as country, year, number of deaths and injuries, and use of weapons. Among them, there were 46 attributes with a completeness of more than 70%.

Data Pre-processing. In the dataset, the average number of attacks by all terrorist organizations was 28. However, 3,430 terrorist organizations (91% of all terrorist organizations) launched fewer than 28 terrorist attacks, and 2,600 terrorist organizations (73% of all organizations) launched fewer than five terrorist attacks. These 2,600 terrorist organizations launched 4,038 terrorist attacks, which accounted for only 4% of the identified terrorist attacks (i.e., attacks by identified terrorist organizations). If all terrorist organizations were predicted, too many categories and low sample categories may cause unfavorable training interference noise. Therefore, to make the experiment closer to reality and the trained model more effective, samples with fewer than five terrorist attacks were removed in this study. Some attributes are unrelated to the prediction of terrorist organizations. Training on these attributes would not only increase the required training time but also render the training results unreasonable or impractical; therefore, data pre-processing operations are essential. At this stage, the GTD dataset was processed through data cleaning, feature engineering, and data normalization.

Data Cleaning. Data cleaning aims to reduce the dimensions of the GTD dataset by detecting and deleting irrelevant or redundant attributes and case records. First, attribute fields that contained descriptive text or too many missing values the missing threshold was set to 30%) were removed. Second, missing values in specific attribute fields were filled with the numerical value corresponding to "unknown" according to the data description rules provided by the GTD. Third, some attribute fields were converted into numerical values to facilitate later processing. For example, the "related" attribute field provides the "eventide" of other terrorist attacks related to this terrorist attack in text format, and we convert it to the count of related terrorist attacks. The number of event records after these three steps was reduced to 98,909. Fourth, after deleting the records of terrorist attacks with fewer than five terrorist attacks, we filtered the remaining records of terrorist attacks according to five conditions (i.e., ≥5 times, ≥50 times, ≥100 times, ≥500 times, ≥1000 times). Eventually, the number of records in the experimental dataset was reduced to 94871 after the data-cleaning process.

Feature Engineering. We tended to retain the objective attributes of terrorist attacks in the GTD and ignored some subjective judgment criteria as well as text-based columns used for interpretation and clearly irrelevant attributes, such as crit1-3, country_txt, region_txt, and eventide. Therefore, 45 potentially relevant attributes were left for analysis. Further selections were then made. First, 34 numerical attributes (int, float) were selected without special processing. Then, the target/victim nationality (natlty1-3) was transformed into an integer numerical type and included. In this way, 37 candidate feature attributes were identified. For these 37 features, it is difficult to determine which should be retained or removed, as the remaining attributes after data cleaning are somewhat correlated. After considering several strategies, we applied the feature selection function (i.e., SelectKBest) in scikit-learn to make the final selection, with only minor adjustments made.

Data Splitting. In machine learning, the sample dataset is usually partitioned into a testing set and a training set in proportion. Because the classification of the target feature attributes in the dataset is usually unevenly distributed, the training and testing sets are divided according to the proportion of the target features in the sample dataset, such that the proportion of the data in each category of the training set and the testing set is consistent with the proportion of the sample dataset, thereby reducing the misleading predictions of the trained models. The following two methods are generally used in data splitting.

Based on the above strategies, to simplify the model and improve prediction accuracy, we selected 36 features for the experiment. These features include: year, month, day, extended, country, region, successful attack, suicide attack, attack type1-3, target type1-3, target subtype1-3, target nationality

(natlty1-3), weapon type1-4, weapon subtype1-4, property, ishostkid, ransom, related, INT_IDEO, INT_LOG, INT_MISC, and INT_ANY. We used the ExtraTrees classifier to build a forest and rank the importance of the 36 feature attributes, as shown in Figure 5. It can be observed that the three most critical attributes for predicting terrorist organizations are the country and region where the terrorist attack occurred, and the target nationality. Thus, the GTD was transformed into a new dataset with a scale of 94,871 × 37 after data reprocessing. Among these, "gname" is the target attribute for prediction, while the remaining 36 attributes serve as the explanatory features.

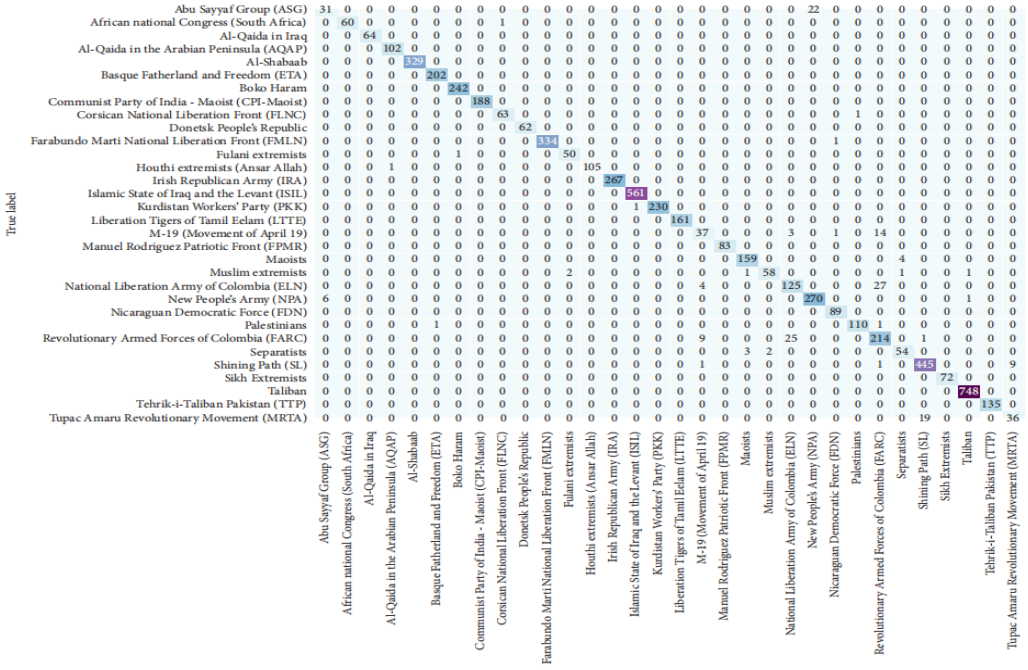


FIGURE 3: Confusion Matrix for Terrorist Organization Prediction.

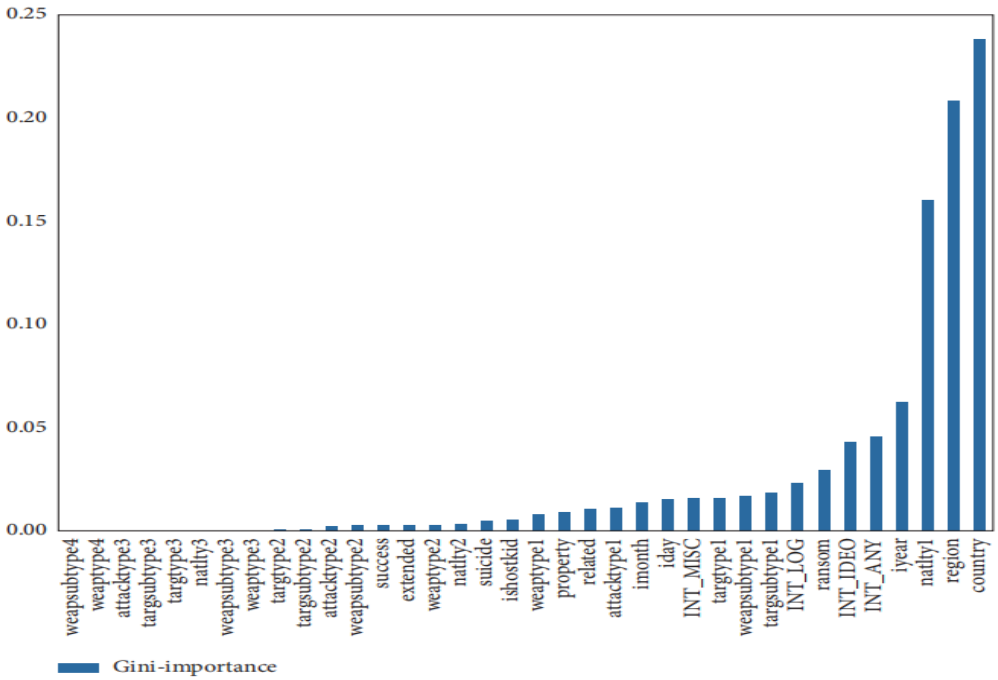


FIGURE 4: Feature Importance Ranking for Terrorism Attack Prediction.

This chart visualizes the Gini-importance ranking of 36 feature attributes used in a machine learning model for predicting terrorism attacks. The x-axis displays the names of these features, while the y-axis represents their corresponding Gini-importance score, a measure of how much each feature contributes to the model's ability to reduce impurity (and thus improve prediction accuracy). The features are arranged in ascending order of importance, revealing a clear trend where a small subset of features exhibits significantly higher importance than the rest. Notably, "country," "region," "nality1"

(nationality 1), and "iyear" (incident year) appear to be the most influential predictors, suggesting that geographical context, the primary nationality involved, and the year of the attack play a crucial role in the model's predictions. Conversely, many weapon and target subtype features show very low importance, indicating they have a minimal impact on the model's decision-making process. This analysis highlights the key drivers in the dataset that the machine learning model relies on for forecasting terrorist events.

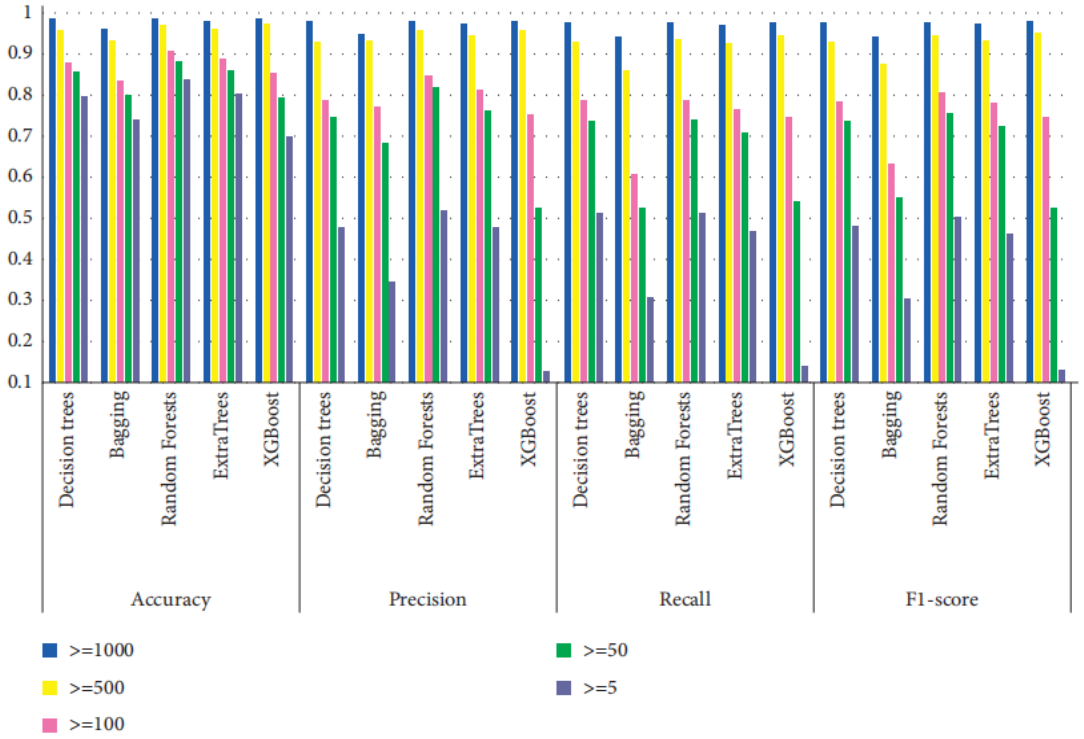


FIGURE 5: Performance Comparison of Machine Learning Classifiers Across Different Attack Frequency Ranges.

The chart above presents a comparative analysis of five machine learning classifiers – Decision Trees, Bagging, Random Forests, ExtraTrees, and XGBoost – across four key performance metrics: Accuracy, Precision, Recall, and F1-score. The performance of each algorithm is evaluated across five distinct ranges of terrorist attack frequency within the dataset: ≥1000, ≥500, ≥100, ≥50, and ≥5 incidents. Each group of bars represents a specific evaluation metric, with individual bars within each group indicating the performance of a particular classifier for a given attack frequency range, color-coded for easy identification. The y-axis quantifies the metric values, ranging from 0.1 to 1.0, allowing for a direct visual comparison of the classifiers' effectiveness in handling datasets with varying levels of event prevalence. The figure highlights the strengths and weaknesses of each algorithm under different data conditions, providing insights into their suitability for predicting terrorist activities based on the frequency of past events.

CONCLUSIONS

This study employs ensemble machine learning techniques to develop multiclass classification models for predicting the perpetrators of terrorist attacks, utilizing data from the Global Terrorism Database (GTD). Initially, a frequency analysis of terrorist organization attacks was conducted, profiling 32 high-activity organizations with over 500 incidents. Subsequently, a feature selection strategy identified 36 relevant attributes, which were used to train five classifiers: Decision Tree, Bagging, Random Forest, Extra Trees, and XGBoost. Model performance and stability were assessed via hold-out validation and 10-fold cross-validation.

The models were designed to predict the 32 profiled high-frequency terrorist organizations. Experimental results demonstrated strong performance and stability across all models, with XGBoost and Random Forest achieving peak prediction accuracies of 97.15% and 97.03%, respectively. A confusion matrix was used to visualize and analyze the XGBoost model's predictions. The methodology is extensible to a wider range of terrorist organizations.

Performance analysis revealed that Random Forest consistently performed well across various classification counts, while XGBoost excelled in scenarios with fewer classes (e.g., dozens), showing comparable performance to Random Forest. The predictive models offer a macroscopic view of global terrorist attack perpetrators, identify key contributing factors, and provide decision support for counter-terrorism efforts.

Future work will focus on enhancing model performance and accuracy through algorithmic improvements and dataset refinement. However, the

inherent sparsity and dynamic nature of terrorist attacks pose challenges to large-scale monitoring and prediction, even with advancements in machine learning.

REFERENCES

[1] J. M. Poland, Understanding Terrorism: Groups, Strategies, and Responses, Prentice-Hall, Englewood Cliffs, 1988.

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

[3] 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, Article ID e0179057, 2017.

[4] Y.-L. Chuang, N. Ben-Asher, and M. R. D'Orsogna, "Local alliances and rivalries shape near-repeat terror activity of alQaeda, ISIS, and insurgents," Proceedings of the National Academy of Sciences, vol. 116, no. 42, pp. 20898–20903, 2019.

[5] V. B. Petroff, J. H. Bond, D. H. Bond, and D. H. Bond, "Using hidden Markov models to predict terror before it hits (again)," in Handbook of Computational Approaches to Counterpartrorism, pp. 163–180, Springer, New York, NY, USA, 2013.

[6] F. Gohar, W. H. Butt, and U. Qamar, "Terrorist group prediction using data classification," in Proceedings of the International Conference on Artificial Intelligence and Pattern Recognition, pp. 199–208, Kuala Lumpur, Malaysia, 2014.

[7] G. M. Tolan, O. S. Soliman, and O. S. Soliman, "An experimental study of classification algorithms for terrorism prediction," International Journal of Knowledge EngineeringIACSIT, vol. 1, no. 2, pp. 107–112, 2015.

[8] X. Meng, L. Nie, and J. Song, "Big data-based prediction of terrorist attacks," Computers & Electrical Engineering, vol. 77, pp. 120–127, 2019.

[9] B. Bu, Z. Pi, and L. Wang, "Support vector machine for classification of terrorist attacks based on intelligent tuned harmony search," Ekoloji, vol. 28, no. 107, pp. 153–164, 2019.

[10] Z. Li, D. Sun, B. Li, Z. Li, and A. Li, "Terrorist group behavior prediction by wavelet transform-based pattern recognition," Discrete Dynamics in Nature and Society, vol. 2018, Article ID 5676712, 2018.

[11] X. Hu, F. Lai, G. Chen, R. Zou, and Q. Feng, "Quantitative research on global terrorist attacks and terrorist attack classification," Sustainability, vol. 11, no. 5, p. 1487, 2019.

[12] G. M. Campedelli, M. Bartulovic, and K. M. Carley, "Learning future terrorist targets through temporal meta-graphs," Scientific Reports, vol. 11, no. 1, pp. 8533–8615, 2021.

[13] G. M. Campedelli, On Meta-Networks, Deep Learning, Time and Jihadism, Universit`a Cattolica del Sacro Cuore, XXXII ciclo, a.a. 2018/19,Milanohttp://hdl.handle.net/10280/70552.

[14] G. M. Campedelli, I. Cruickshank, and K. M. Carley, "A complex networks approach to find latent clusters of terrorist groups," Applied Network Science, vol. 4, no. 1, pp. 1–22, 2019.

[15] B. A. Desmarais and S. J. Cranmer, "Forecasting the locational dynamics of transnational terrorism: a network analytic approach," Security Informatics, vol. 2, no. 1, pp. 1–12, 2013.

[16] W. Guo, K. Gleditsch, and A. Wilson, "Retool AI to forecast and limit wars," Nature, vol. 562, no. 7727, pp. 331–333, 2018.