The Journal of Computational Science and Engineering.
ISSN: 2583-9055

Comparative Examination of Machine Learning Models for Terrorist Activity Prediction

Olayemi Ariyo[1], M.O Agbaje[2], Akande Oyebola[3] and A.A Izang[4]

[1,2,3,4]Department of Computer Science and Engineering,

Babcock University, Ilisan,Ogun

ariyo0247@pg.babcock.edu.ng[1], agbajem@babcock.edu.ng[2],oyebolaa@babcock.edu.ng[3],
Izanga@babcock.edu.ng[4]

Keyword:
Terrorism, machine learning, prediction, algorithm, GTD

ABSTRACT

Due to terrible events that have recently struck Nigeria and resulted in thousands of lives and significant damage, terrorism has generated a tremendous humanitarian and economic catastrophe. The many terrorist attacks that Nigeria has seen recently include those carried out by Boko-Haram, Fulani/Herdsmen, robberies, intra- and inter-group disputes, and lack of intentionality. Many machine learning techniques, such as Logistic Regression, Random Forest, and Support Vector Machine, have been utilized in order to analyze the dataset and provide forecasts regarding the outcome of specific attacks, the identity of the assault group, and the impact of external variables. To get the most important findings, a thorough comparison of each method is performed. It is necessary to create models that may be utilized to comprehend the actions of these terrorists and prevent or lessen such incidents in the future to stop or curtail their operations in Nigeria.

This study investigates several forms of terrorism forecasting and evaluation utilizing multiple machine learning procedures that take into consideration the performance metrics of the previous work's accuracy measure, with the goal of providing a thorough review for integrating these algorithms in terrorist prediction. Approximately 190,000 terrorist events and occurrences worldwide from 1970 to 2020 are included in the GTD, a well-known database utilized by the authors under examination. The database includes information on the sorts of attacks, including the weapons employed (Global Terrorism Database, 2020). In addition to supporting future research focused at developing these techniques for terrorist prediction analysis with the categories, problems, and prediction systems. It is anticipated that this systematic review will be helpful in introducing these approaches to terrorism researchers. Thirty chosen machine learning papers that forecast terrorist activities, enumerate the relevant knowledge, and emphasize the major limitations found during the study process are the focus of our attention. This increases the effectiveness of crime prevention while guaranteeing safety and security.

Corresponding Author: Email: ariyo0247@pg.babcock.edu.ng[1]

INTRODUCTION

The use of violent and unlawful force to instil fear in a group of people is known as terrorism or terrorist actions. According to Llussá, F., and Tavares, J. (2021), these acts might be politically sponsored or ethnically motivated, based on differences in religion or ideologies. In recent years, terrorism has had a detrimental impact on a variety of industries, groups, countries, and the whole world. The global economy and major stock markets are also affected, as shown by the downward increases in market prices (Song, Y., 2022). Many governments dealing with the issue of terrorism prioritize developing strategies that may most

effectively identify the many elements contributing to terrorism and offer potential means of reducing or eliminating terrorist activity (Uddin, M., et al. 2020). Previous studies have shown that the level of uncertainty and insecurity resulting from terrorist acts has influenced people's decision-making to the extent that many now opt for less adventurous and more cautious paths of action to counteract the feelings of insecurity caused by the terrorist tragedies.

Terrorism seeks to spread fear, anxiety, and concern beyond the influence of a single person to cause instability. There were 1,411 distinct terrorist incidents in 2019 alone, according to the Global Terrorism Database (GTD), which led to 6,362 fatalities and negatively impacting people's quality of life in society (Global Terrorism Database, 2022). For many years, researchers have researched terrorism to comprehend its primary causes, how to carry out counterterrorism operations, and its impacts on society and the economy (Ouassini, N., & Verma, A.K. 2018). However, because to the complexity of terrorism, it is challenging to come up with a workable counterterrorism strategy that would save people's lives. It has been demonstrated that identifying terrorist ideology and forecasting future terrorist actions are crucial and time-consuming tasks. Recently, the many components of terrorism have been studied via the use of machine learning algorithms (Alhamdani, R. et, al. 2018). Law enforcement organizations can utilize these models to anticipate events before they happen and could inflict harm to people, property, or the rule of law. This study offers a thorough review of current developments in the field and offers insight on potential applications of "machine learning" in the anticipation of terrorist strikes.

This study benefits the larger research community by emphasizing the capability of these models and the issues that need to be resolved. Thirty chosen machine learning papers that forecast terrorist activities, enumerate the relevant knowledge, and emphasize the major limitations found during the study process are the focus of our attention. Consequently, the following are this paper's main contributions: First, it presents a compilation of previous research on neighbourhood terrorist attack that used cutting edge machine learning and methods for deep learning. Furthermore, the study described many terrorist assault types and suggested avenues for further investigation to close the current knowledge gaps about terrorist activities and the performance metrics. so logically posing future research goals and/or queries for the scientific community to investigate further.

RELATED LITERATURE ON MACHINE LEARNING MODELS FOR TERRORIST ATTACK PREDICTION

Terrorism may have a devastating effect on a community and greatly harm its citizens. Over the past several decades, a great deal of research has been done on the subject to determine its origins and how to create an efficient counterterrorism system that would lessen the likelihood of terrorist acts. To anticipate some of the elements that may be responsible for a rise in terrorist acts, Agarwal, P. et al. (2019) conducted a comparison investigation of a class of machine learning algorithms using the GTD. These include group dynamics, success rates, and the impact of outside factors. IrfanUddinet M. et., al., (2020) predicted future terrorist using Naïve Bayes, logistic regression, and SVM techniques. Their results show that the five-layer deep neural network is a more successful approach for future terrorist attack prediction.

The authors, JSPM and Tirwa (2018) categorized, using five machine learning algorithms the dataset weapon used in the attack. It was determined that the type of weapon

used during the operation determines the likelihood of an assault. Rai, H, et., al. (2021) proposed to forecast terrorist attacks, five machine learning strategies have been used to filter the data that is part of an attack target. In this study, AdaBoost, Random Forests, Gaussian Bayesian networks, decision trees, logistic regression, and random forests were tested using data from terrorist events that occurred in 2015 and 2016.

The results of experiments indicate that the Decision Tree method and the Gaussian filter perform well in predicting attacks. A state-of-the-art hybrid classifier for big data-driven terrorist attack prediction was proposed by Meng, X. (2019). A workable approach to forecasting terrorist acts was given, which comprised gathering data, pre-processing, a hybrid classification system for the data, and overall classifier testing. A genetic algorithm is used to optimize the classifier weights to increase the hybrid classifier's prediction accuracy. The results indicate that in terms of forecast accuracy, a hybrid classifier performs better than a single classifier. In a different study, Chatterjee K. and Rai HM. (2021) presented a deep learning framework and CNN-LSTM enabled ensemble strategy for detecting myocardial infarction for the ECG. It was found that this method outperformed the conventional CNN approach. Human loss was revealed to be the most important component in terrorist attack risk by Luo, L., and Chao Q. (2021) using a random forest model. Huamaní E. et al. (2020) used machine learning (ML) to forecast terrorist acts around the globe using the global database on terrorism (GTD). Canhoto, A. (2021) using machine learning (ML) combat terrorism by identifying and stopping money laundering, a crucial tactic in terrorist activities. Hao, M. et al. (2019) sought to determine the spatiotemporal trends of terrorist acts in the Indochina Peninsula employed random forest on the GTD. Directed graphs were used by Mishra, N., et al. (2020) to find network relationships among terrorist operations using the GTD. Extreme Gradient Boosting was used to the GTD by Feng, Y., et al. (2020) to anticipate casualties from terrorist strikes.

RESEARCH METHODOLOGY

Feature selection is necessary because machine learning prediction datasets may contain hundreds of attributes, many of which may not be relevant to the task at hand. A crucial step in gaining additional and preliminary insights into any given dataset is feature selection. Additionally, it can play a significant role in the preparation of data, particularly for machine learning models (König, G., et al., 2021). According to how well the predictive factors describe the target variable, it aids in grading them (Thaseen, I., et al. 2019). Features can be ranked by hand, statistically, or by machine learning. It computes the entropy reduction by dividing the dataset based on a specified random variable value. Preprocessing, feature selection, training, testing, and prediction are all included in this pipeline (Fig. 1). It demonstrates the methodical technique the researchers used to carry out the investigation. For this investigation, the Global Terrorism Database (GTD) was consulted (Global Terrorism Database, 2020). The preprocessed dataset was divided into training and testing subsets.

In the methodology's initial step, 30 pertinent studies that employ machine learning to predict terrorist models are gathered and analyzed; in the second stage, a classification table of each study, the results of several algorithms, the accuracy attained, and a comparison of them are given. Finally, constraints and further research. The publications under review are studies on crime prediction that span the years 2017 through 2023.

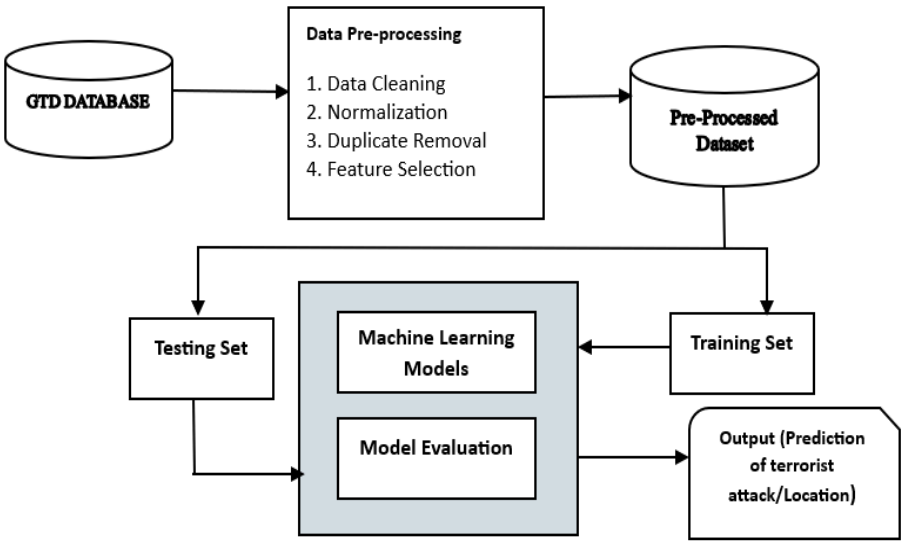

Figure 1. Workflow of Models used for Prediction.

Model Execution:

The models' performance will be assessed using four metrics: accuracy, precision, recall, and F1-score.

The mathematical expressions for the criteria are discussed below:

Precision is (TN+TP)/(TN+TP+FN+FP).
TP/(TP+FP) equals precision.
TP/(TP+FN) is the recall.

F1- Score = 2 x (Precison x Recall)/(Precision+Recall) where the variables TN, TP, FN, and FP, respectively, denote True Negative, True Positive, False Negative, and False Positive in the formulae (Adeosun, M. and Ugbebor, O. 2021).

These were then used to compute the performance requirements; they were located in the confusion matrix. The confusion matrix is a performance indicator used in machine learning classification problems.

MODELS OF TERRORIST PREDICTION USING MACHINE LEARNING

It has been demonstrated that traditional machine learning algorithms can accurately forecast acts of terrorism. To find trends that can be used to anticipate criminal activity, the Global Terrorism Database (GTD has been examined using a range of models, including support vector machines, decision trees, logistic regression, random forests, and others. While complex neural architecture and enormous amounts of data are required for deep learning, conventional "machine learning" Models are easier to analyze and require fewer data. For example, a logistic regression model can be used to predict the likelihood of a specific type of crime occurring based on variables such as the location, time of day, and local demographics (Varun, M., et al., 2023). Identifying the crucial elements that lead to a certain terrorist act is one application for decision tree models. By examining numerous attributes, models such as Random Forests (RF) can be used to predict terrorist attack trends. In addition to these techniques, outlier analysis and anomaly detection in terrorist data can also be performed using traditional machine learning models. Law enforcement organizations can identify possible terrorist activity in Nigeria and take action to stop it by spotting odd trends or outliers in the information.

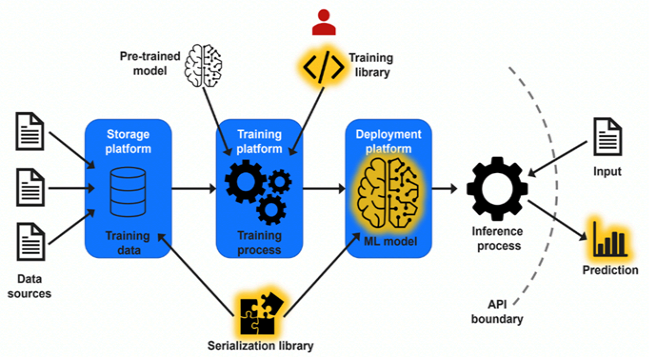

Figure 2. Machine Learning Prediction Process

As shown in figure 2, there are several important phases involved in applying machine learning to anticipate crimes. The next stage is to compile relevant data, such as demographics, weather trends, and crime rates. The next stage is known as data preparation, and it entails preparing the data for usage by cleaning and formatting it. Following data preprocessing, training, and testing data sets are separated in order to build and evaluate models. Feature engineering is the process of selecting important attributes for the model to be trained on, and it occurs after. The data can be exposed to various machine learning techniques for training and prediction once the features have been selected. Several performance indicators are used in the evaluation process to assess the trained models' precision and efficiency in forecasting terrorist activity. The outcomes have the potential to improve making decisions for programs that prevent terrorist and enforce the law.

STAGES OF MACHINE LEARNING:

To efficiently employ ‘machine learning models’ for crime prediction. The obtained dataset must pass through a few steps before the results will be evaluated. To effectively

employ machine learning techniques to make the forecast of crimes, the collected dataset needs to go through a few stages before the results are assessed.

Data Collection:

Data collection refers to the procedure of obtaining and estimating data from multiple, discrete sources. We can comprehend the history of past events by gathering data, which we may then analyze to identify structured patterns. These patterns enable us to build prediction models that identify trends and project future changes using machine learning techniques. Appropriate ways for gathering data are required to build well-functioning techniques. The data ought to contain correct information that is pertinent to the current work (Wang, Z. & Wang, J. 2021).

Preparing the Data:

Preprocessing is the process of converting raw data into a format that can be read by humans. This phase is critical since raw data is insufficient for machine learning to function. Prior to utilizing machine learning algorithms on the data, the data quality should be preserved. Libraries for Python are preconfigured to perform specific tasks. Importing the required libraries is one of the prerequisites for machine learning data pre-processing. The project made use of the following essential Python libraries: DESlib, SKlearn, Statsmodels, Folium, NumPy, Pandas, Matplotlib, Plotly, and Folium (Cruz R. et al., 2020). Python was utilized to import all of the datasets in the.csv file type utilizing the read_csv () method.

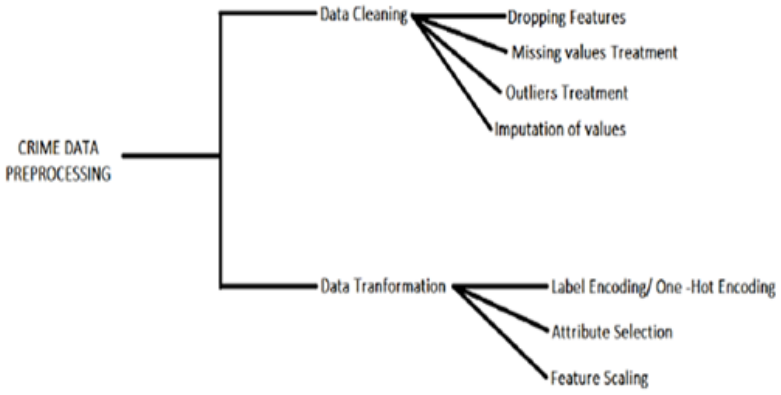

Figure 3. Various Data Pre-processing Activities

Splitting the Dataset:

The supplied dataset is split into two sets using the train-test split, which separates it into train and test sets based on how well each machine learning algorithm works (Brownlee, J. 2020). The initial subset that fits the model is called the training dataset. Rather than being used for training, the second subset—known as the test dataset—is the component that the model uses as input. After then, projections are created and compared to the anticipated values

(Rácz et al., 2021). 80% of the data in the test-train split are usually classified as train data, and 20% are marked as test data. Two opposing circumstances need to be considered when dividing up a dataset: There will be more variance in the parameter computations with less training data. In addition, less testing data will result in a greater disagreement in the implementation statistic.

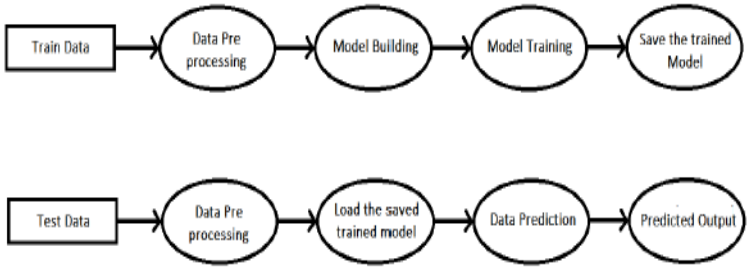

Figure 4. Train and Test Steps

Feature Selection:

Feature selection is a crucial technique in predictive model development because it reduces the number of input variables. This is important because fewer features improve interpretability and expedite training, both of which reduce the spatial requirements of the model (Khaire & Dhanalakshmi, 2022). By picking more significant features and removing redundant and unnecessary characteristics from our dataset, we were able to improve the test data's projected accuracy (Pilnenskiy & Smetannikov, 2020).

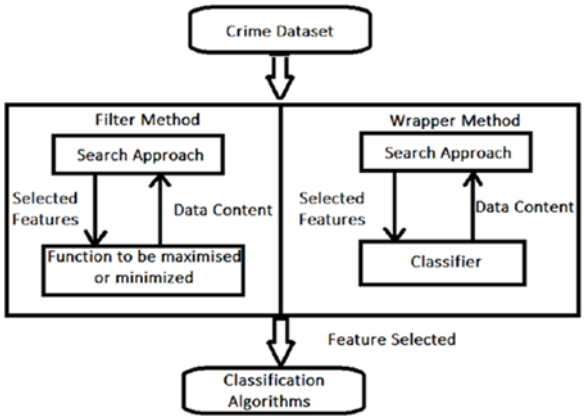

Figure 5. Various Feature Selection Techniques

Evaluating the Performance:

Utilizing metrics to evaluate an algorithm's performance is a fundamental part of any machine learning workflow. To show if progress is being made, these indicators employ a numerical representation. Every machine learning model, no matter how complex or basic linear, needs a quantifiable value to be determined to assess its performance (Yu et al., 2022). The model's performance is monitored and assessed using metrics in both the training and test datasets. In machine learning, every problem is divided into two categories: regression tasks and classification tasks.

CLASSIFICATION OF TERRORIST PREDICTION SYSTEMS:

Typically, there are two categories of machine learning techniques: supervised and unsupervised. Many applications in the former category try to forecast a target variable. With this approach, a mapping connection is created by building a model from the training dataset that corresponds to the attribute variables and the target variables in the sample dataset. The testing dataset is used for both prediction and assessment. To determine the prediction accuracy, the values of the predicted and real target variables are compared. Based on known attribute fields, the classification models identify terrorist groups or individuals involved in a terrorist incident. The classification algorithm model receives the current terrorist event feature data for training and learning during the supervised machine learning process. Subsequently, the test or fresh data is classified using the trained model to forecast potential terrorist groups or individuals.

Table1. An Overview on Machine Learning Models

No	Model	Authors	Features Used	Datasets
1.	DL, KNN and Naive Bayes	Arifin, et al. (2022)	Attack, Bomb, Disinformation, Daesh, ISIS, Al-Qaeda, Murder and Slaughter	Global Terrorism 1973-2022
2.	SVM, DT RF and KNN	Kissi Ghalleb, et. al. (2020)	Location, kind, terrorist organization, or the target.	Databases from GTD Tunisia and ACLED Tunisia.
3.	LR, DT Gaussian Bayesian Network Ada Boost & RF	Gao, et al. (2019)	134 attributes were considered	Global Terrorism Database
4.	SVM, RF and LR	Agarwal, et al. (2019)	Attacktype, nkill, Timestamp	Global Terrorism Database
5.	Extreme Gradient Boosting	Feng, Y. et., al. (2020)	Attack and Kidnapping	Global Terrorism Database

	(XGB)			
6.	Stochastic Gradient Descent (SGD)	Géron, A. (2017).	Suicide, Attack	Global Terrorism Database
7.	SVM and Multinomial Logistic Regression	JSPM, et al. (2018)	Counting features, unigram features, senti-features, polarity of words	Tweets extracted from GTD during the time period 2013- 2016
8.	SVM and Multinomial LR	Kokane, B. et al. (2022)	counting features, unigram features, senti-features, polarity of words	Tweets collected during and before the terrorist attacks in Paris, in November 2015
9.	Aho-Corasick algorithm, KNN and SVM	Sarker, A. et al. (2020)	Terror attack, Severe Terror Attack and Normal Data	Twitter 4j API
10	Jaro-Winkler Levenshteite Needleman-Wunsch Smith-Waterman	Iftene, A. et al. (2017)	retweets, hashtags, links, punctuation marks	Streamed data taken from Twitter
11	Iterative vertex clustering and classification	Benigni, M. et al. (2017)	Following, followers, Mention, Hashtag, among other things	Through the API, 119156 tweets
12	KNN, Naive Bayes and SVM	Garg, P. et al. (2017)	For the study, features such as the quantity of favorites, the number of retweets, and the last retweet time were extracted.	Tweets throughout a 30-day span which contain the hashtags Uri-Attack
13	Deep Neural Network	Zhou, Y. (2017)	Frequency of the hashtag, Twitting time	17K tweets from June 2015 to May 2016, ISIS
14	Deep Convolution Neural Network	El Ali, et al. (2018)	Tweets with hashtags Paris and Beirut	4127489 tweets across 4 languages
15	SVM	Bedjou, K. et al. (2019	Number of posts, Retweets, etc	Corpus of raw 12000 tweets

16	Naive Bayes, SVM, Logistic Regression	Alsaedi, et al. (2017)	Stop words and stemming	collection of a tweet sent in August 2011
17	ML Classifiers such as Naive Bayes, KNN, SVM, and XGBoost classifiers and ANN	Kant, G., et., al. (2023)	Classify Twitter posts that have been geocoded into categories based on their Location	Twitter
18	Hybrid DL platform based on models for long-term memory (LSTM) and convolutional neural networks (CNN)	Saidi, F., and Trabelsi, Z. (2022)	Determine the traits of future terrorist operations	GTD
19	Spatial technology, machine learning, and remote sensing	Cil, A. et., al. (2021)	Predicts the presence or absence of Europe's terrorism on a previously unstudied geographic scale	GTD ACLED ICEWS
20	ML models used for topic modeling and text classification to determine the attacker's motivation for the attacks.	Bridgelall, R. (2022)	Aims of the attacks are identified in six categories: Protest, retaliate, intimidate, weaken, force, and despise	GTD
21	Five machine learning classifiers prediction models	Pan, X. (2021)	Predicting terrorist organizations with the highest attack frequency	GTD
22	ML and NLP with textual features	Abdalsalam, M., et., al (2021)	Classification and predication of attack types	GTD
23	Ensemble ML model which combines SVM	Olabanjo, O. et., al (2021)	Identification of terrorist-prone continents	GTD

	and KNN			
24	DNN and ML models (LR, SVM, and NB)	Uddin, M. et., al. (2020)	Forecasting terrorist activity, such as the possibility that suicide strikes would be successful, the kind of weapon to be used, the attack's location, and its nature	GTD
25	Predictive analysis makes use of the RF-based ML-based model XG Boost.	Feng, Y., et., al. (2020)	Assess if terrorist attacks will cause innocent people to die.	Terrorist attacks in China and the GTD
26	GCN model using multi-layered deep neural network (NNGCN). A deep neural network with several layers	Feng, Y., et., al. (2020)	To research terrorist attack categorization and early warning systems	Cornell, Texas, Washington, Wiki, terror attacks
27	Quantitative research and the K-means clustering technique	Hu. X., et., al. (2019)	Models of risk assessment for locating dormant or emerging terrorist groups and networks of terrorist groups' affiliations.	GTD
28	Ontology-based knowledge graphs were created utilizing linkages and verbs based on violence, like "attack," "killed," and so on, between entities, like locations, persons, and organizations.	Srinivasa, K., et., al. (2019)	putting together a framework to create a knowledge base with criminal entities and their connections	Online news sources

29	The C4.5 categorization methodology applied to analyze terrorism	Saiya, N., and Scime, A. (2019)	The investigation shows how classification trees could help us understand terrorism better and perhaps help politicians avert more attacks.	GTD
30	KNN, NBB, SVM ID3, and C4.5	Tolan, G. and Soliman, O. (2017)	Date, attack type, attack weapon, target type, etc.	The National Consortium for the Study and Response to Terrorism's Global Terrorism Database

Figure 6. An Overview on Machine Learning Models Used in Terrorist Prediction Research.

CATEGORIZED TERRORISM ANALYSIS TYPES:

The results of different attacks differ significantly, with armed attacks and hijackings resulting in the highest number of casualties. Apart from detonation and explosion, GTD has recorded the subsequent categories of assaults: assassination, assaults with weapons, kidnappings, two types of hostage-taking, attacks on infrastructure and facilities, and unarmed attacks. Differentiating these tactics from bomb assaults is crucial. All eight species fall into one of three categories: hybrids, antihuman bodies, or anti-material things. Under GTD, armed assault attacks seek to use guns or other deadly equipment to murder or injure victims (Luo, L., and Qi, C. 2022). Additional targeted human assaults include assassinations and hostage-taking (of two types). Unlike the previous category, hijacking is an attack on a physical object, with the primary goal being to seize control of the target facility's vehicles and infrastructure. Assassination, assault with a weapon, bombing or explosion, hostage taking (Barricade Incident), kidnapping, attack on a facility or infrastructure, assault without a weapon, and unknown are the eight primary categories of terrorist operations recognized by the GTD. Regarding the attack, the following details are relevant:

- Assassination: An act done with the intention of killing a prominent figure or celebrity.
- Armed Assault: This is any attack in which the primary objective is to cause harm or death to a target using a weapon, such as a gun, knife, or incendiary device.
- Bombing/Exposure: An attack when the principal agent is a material that degrades rapidly and releases a pressure wave that damages the immediate vicinity.
- Hijacking: An attack on a person's right to freedom when the perpetrator pushes the victim against his will and without a valid reason; alternatively, an act in which the perpetrator carries out covert objectives, like pressuring the state or other authority to free prisoners or accomplish a different political objective.
- Hostage Taking (Barricade Incident): When someone arrests or detains another person and threatens to kill, harm, or imprison him in order to coerce a third party—a state, an intergovernmental organization, a natural or legal person, or a group of people—to perform a specific act as an explicit or implicit condition of releasing the hostage, that person is guilty of

taking hostage.

- Hostage taking, also known as kidnapping: an act when the primary objective is to seize control of hostages in return for compromises or to halt regular activities. The primary objective of a facility/infrastructure attack is to do harm to non-human entities, such as houses, schools, places of worship, and other vital infrastructure facilities.
- Unarmed Assault: An attack in which the principal intent is to kill or seriously hurt another person using a weapon other than a firearm, explosive, incendiary, or sharp object (such as a knife).

Table 2. Categorized Terrorist Types

General Category	Analysis type	Freq.
Assassination	kill	6
Armed Assault	Weapons, gun, knife	7
Bombing/Exposure	Attack, bomb	3
Hijacking	Kidnapping	3
Hostage Taking	terrorist activities	7
Unarmed Assault	Protest, retaliate, intimidate, weaken, force, and despise	10

Figure 7. Categorized Terrorist Types in the Reviewed Articles

DISCUSSION AND FUTURE WORK

In this section, the performance of the machine model under review is examined. Table 3 summarizes the metric of each model and compares in terms of average train, test accuracy, average recall, and F1-score. It was noted that hybrid Deep Learning model achieved the highest rating report values across all scales. The categorization test report demonstrates that learning models such as Hybrid Deep Learning, DNN, ANN and Naïve Bayes performed better than others. The performance of LGBM, Random Forest, SVM is closely similar to XGB which gave an average of 70%. Models like Logistics regression, Gaussian NB, Quadratic Discriminal Analysis produced similar results of 70%. Because every model is unique and has different qualities when it comes to learning and training, there will be a relative variation in the time required to develop the model.

The algorithm with the lowest performance results was AdaBoost. When comparing the performance of all the models, AdaBoost has the lowest value (63%), closely followed by Linear SVC (69%). Hybrid Deep learning outperformed all other models with a value of 99.4%. The models exhibit good performance, classifying assaults according to important criteria, and have an average accuracy of more than 78%. The lack of standard datasets is evident from the above survey. Various studies carried out have used different datasets, thus making direct comparisons difficult. Datasets collected for the threatening, detection and prediction of the terrorist attack were different depending on the study conducted. On the basis of the data collected various types of features were extracted for classification.

The future research will strive to improve the model's performance further by

implementing hybrid method of combining models to achieve high performance results and adding new features using feature engineering. In addition, more research will need to focus on finding the most important traits and eliminate the rest, which should increase the model's accuracy. The machine learning model, which can track text messages delivered for ransom and forecast future terrorist acts based on the names of target groups, may be optimized and made less complex by employing feature-reduction techniques.

Table 3. Accuracy and Performance of Comparison of Machine Model

Algorithm	Train accuracy	Test accuracy	Average Re-call	Average F1-score
LGBM	81.0	81.0	79.0	78.0
Random Forest	81.0	80.0	79.0	78.0
SVC	80.0	80.0	79.0	75.0
XGB	80.0	79.0	78.0	78.0
Extra Trees	80.0	79.0	77.0	77.0
Bagging	79.0	78.0	77.0	77.0
K Neighbors	78.0	78.0	77.0	75.0
Linear SVC	77.0	76.0	76.0	69.0
Linear Discriminant Analysis	77.0	76.0	73.0	72.0
DNN	94.6	94.8	94.8	94.8
SVM	78.8	78.3	78.2	78.2
Logistic Regression	76.0	74.0	74.0	70.0
Gaussian NB	74.0	74.0	74.0	70.0
Quadratic Discriminant Analysis	74.0	73.0	72.0	70.0
Decision Tree	72.0	70.0	72.0	72.0
Extra Tree	67.0	67.0	67.0	66.0
AdaBoost	63.0	61.0	63.0	63.0
Naïve Bayes	81.3	80.9	80.8	88.7
CNN	80.0	81.0	82.0	83.0
LSTM	77.0	74.0	74.0	74.0
ANN	88.1	87.3	88.0	88.0
K-Means	77.0	73.0	77.1	73.0
Hybrid DL	99.1	99.3	99.4	99.4

Figure 8. Accuracy and Performance of Comparison of Machine Model Used in the Reviewed Articles

LIMITATION FROM THE REVIEW:

Machine Learning models need help with disparity and perform poorly. Larger training datasets are needed to counter this. The more features there are, the more optimization opportunities there are. Furthermore, the model gets more complicated as the number of characteristics rises. Various studies carried out have used different datasets, thus making direct comparisons difficult. Datasets collected for the assault, detection and prediction of the terrorist attack were different depending on the study conducted. Based on the data collected, various types of features were extracted for classification. The vast number of categories on the dataset also potentially hinders the machine learning models' performance.

CONCLUSION:

Machine learning improves the defense against biological, physical, and electronic threats by increasing the difficulty of simultaneously locating the attacker and improving target identification accuracy. One of the reasons for instability in nations all around the world is terrorist strikes. We will be able to carry out more thorough inquiries if we have a clear knowledge of how this incident happened. This study reviews current developments in the field and sheds light on possible uses of ‘machine learning’ in the anticipation of terrorist attack using various datasets.

This study highlights the potential of these models and areas that require improvement, which benefits the broader research community. The four primary performance measures that were utilized to evaluate performance metrics were accuracy, precision, recall, and the F1-score. After thirty machine learning models were counted and compared, the results demonstrated that merging several models and integrating text characteristics with other features considerably enhanced the predicted performance for terrorist attack types.

This will provide a solid foundation and point of reference for cooperative counterterrorism operations in Nigeria, improve government vigilance and emergency management capabilities in preventing terrorist attacks, and improve understanding of terrorism.

REFERENCES

1. Rana, O., Burnap, P., and Alsaedi, N. (2017). “Can we foresee a riot? Using Twitter for disruptive event detection”, ACM Transactions on Internet Technology (TOIT), vol. 17, no. 2, pp. 1–26, 2017.
2. Abdalsalam, M., Li, C., Dahou, A., Noor, S. (2021). "A study of how textual features affect the GTD dataset's ability to predict terrorist attacks”. Engineering Letters, 29(2).
3. Chandra, S., Sharma, M., and P. Agarwal (2019). "Comparison of machine learning techniques for terrorist attack prediction." The Twelfth International Conference on Contemporary Computing (IC3),

2019 (pp. 1–7). IEE Explore (www.ieee.org).

4. Ugbebor, O. and Adeosun, M. (2021). "An empirical evaluation of jump diffusion models, symmetric and asymmetric, for the Nigerian stock market indices" African Scientific. 12: e00733. (www.elsevier.com)
5. Agarwal, P., Sharma, M. and Chandra, S. (2019). "Assessment of machine learning techniques in terrorist attack forecasting," at the twelfth international conference on contemporary computing (IC3), 2019. 2019 IEEE, pp. 1–7.
6. Alhamdani, R., Sattar, I., and Abdullah, M. (2018). "Deep learning-based recommender system for worldwide terrorist database," International Journal of Machine Learning and Computing, vol. 8, pp. 571–576, 2018.
7. Arifin, V. Jallow, F. Lubis, A. Bahaweres, R. and Rofiq, A. (2022). "Predicting terrorists' terms with a deep learning model to plan attacks in real time twitter tweet from rapid miner," in 2022 10th International Conference on Cyber and IT Service Management (CITSM). IEEE, 2022, pp. 1–6.
8. Bedjou, K. Azouaou, F. and Aloui, A. (2019). "Detection of terrorist threats on twitter using svm," in Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, 2019, pp. 1–5.
9. Bridgelall, R. (2022). "Using natural language processing to categorize the desires stated by terrorists" Social Sciences, 11(1), 23.
10. Benigni, M. Joseph, K. and Carley, K. (2017). "Online extremism and the communities that sustain it: Detecting the and supporting community on twitter," PloS one, vol. 12, no. 12, p. e0181405, 2017.
11. Brownlee, J. (2020). "Machine Learning Algorithms: Train-Test Split Evaluation. In the Mastery of Machine Learning"
12. Cil, A. E., Yildiz, K., Buldu, A. (2021). "Detection of ddos attacks with feed forward based deep neural network model". Expert Systems with Applications, 169, 114520
13. Cruz, R., Hafemann, L., Sabourin, R., & Cavalcanti, G. (2020). DESlib is a dynamic Python library for ensemble selection. Machine Learning Research Journal, 21.
14. Chatterjee K. and Rai HM. (2021). "Hybrid ensemble technique and CNN-LSTM deep learning model for automatic detection of myocardial infarction using big electrocardiogram data." Applied Intelligence 2021(2).
15. Canhoto, A. (2021). "Using machine learning from an affordances perspective to combat money laundering and terrorism financing globally." Business Research Journal 131: 441–52. CrossRef.
16. El A. Ali, Stratmann, T., Park, S. Sch¨oning, J. Heuten, W. and Boll, S. (2018). "Measuring, understanding, and classifying news media sympathy on twitter after crisis events," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1–13.
17. Yin, Y., Li, Z., Hu, Z., Wang, D., and Feng, Y. (2020). "A terrorist attack casualty prediction technique based on XGBoost." Complex & Intelligent Systems, 6(3), 721–740.
18. Garg, Ph. Ranga, V. and Garg, H. (2017). "Sentiment analysis of the uri terror attack using twitter," in Proceedings of the 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 17–20.
19. Gao, Y., Wang, X., Chen, Q., Yang, Q., Yang, K.- and Fang, T. (2019). "Suspects prediction towards terrorist attacks based on machine learning," in 2019 5th International Conference on Big Data and Information Analytics (BigDIA). IEEE, 2019, pp. 126–131.
20. Géron, A. (2017). "Hands-on Machine Learning with TensorFlow and Scikit-Learn: Ideas, Resources,

and Methods to Create Intelligent Systems," 2nd ed. Sebastopol: O'Reilly Media, p. 856.

21. Hu, X., Lai, F., Chen, G., Zou, R., Feng, Q. (2019). "Quantitative research on global terrorist attacks and terrorist attack classification. Sustainability", 11(5), 1487.
22. Huamaní, E. Alva M. and Avid R. (2020). "Using the Global Terrorism Database, Machine Learning Techniques to Visualize and Predict Terrorist Attacks Worldwide." 11: 562–570 in the International Journal of Advanced Computer Science and Applications. [CrossRef].
23. Hao, M., Dong J., Fangyu D., Jingying F. and Shuai C. (2019). "Using GIS and the Random Forest Method to Simulate Spatial-Temporal Patterns of Terrorism Incidents on the Indochina Peninsula" Geo-Information Journal of ISPRS International 8: 133. [CrossRef].
24. Iftene, A. Dudu, M. and Miron, A (2017). "Scalable system for opinion mining on twitter data. dynamic visualization for data related to refugees' crisis and to terrorist attacks," 2017.
25. IrfanUddin, M., NazirZada, F., YousafSaeed, A., SyedAtif A., Shah,Mahmoud A. Khasawneh, and Marwan M., (2020). "Prediction of Future Terrorist Activities Usin g Deep Neural Networks," HindawiComplexit 2020: 1-16. (www.hindawi.com)
26. JSPM W. and Tirwa, K. (2018). "Machine learning-based predictive modeling of terrorist attacks" Int. J. Pure Appl. Math, vol. 119, pp. 49–61, 2018.
27. JSPM, W. and Tirwa, K. (2018). "Predictive modeling of terrorist attacks using machine learning". Int. J. Pure Appl. Math. 119:49-61. (www.ijpam.eu)
28. K¨onig, G., Molnar, C., Bischl, B. and Grosse-Wentrup, M. (2021). "Data processing for prediction relative feature importance, in 2020 25th International Conference on Pattern Recognition" (ICPR), pp. 9318–9325.
29. Khaire, U. M., & Dhanalakshmi, R. (2022). "Reviewing the stability of the feature selection algorithm". In King Saud University's Journal of Computer and Information Sciences (Vol. 34, Issue 4). [10.1016/j.jksuci.2019.06.012] is the DOI link.
30. Kokane M., Saurav S., Bhairu, V., Kshitij C., and Kanojiya, B. (2022). "Detecting online spread of terrorism on twitter using machine learning," International Journal of Engineering Research Technology (IJERT), vol. 11, 2022.
31. Kissi A. G. and Ben A. (2020) "Machine learning-based terrorist act prediction: Tunisia case study," in 17th International Multi-Conference on Systems, Signals Devices (SSD), 2020, pp. 398–403, 2020.
32. Kant, G., Weisser, C., Kneib, T., Säfken, B. (2023). "Topic model—Machine learning classifier integrations on geocoded twitter data". In: Biomedical and other applications of soft computing, pp. 105–120. Springer.
33. Llussá, F. and Tavares, J. (2021). "Which fear at what price? Regarding the financial fallout from terrorist attacks". Letters on Economics,110: 52-55. (www.elsevier.com)
34. Luo, L. and Chao Q. (2021). "An analysis of the crucial indicators impacting the risk of terrorist attacks": A predictive perspective. Safety Science 144: 105442. [CrossRef]
35. Luo, L., and Qi, C. (2022). "The tendency of terrorist organizations to explosive attacks: An institutional theory
36. Perspective". Frontiers in Psychology, 13, 747967.
37. Shrabanee S., Debabrata S., and Mishra, N. 2020). "A Cloud-Based Intelligent Framework for Examination of Terrorism-Related Activities." New Directions in Management and Decision Science. The latest developments in computing and intelligent systems. By Andrew W. H. Ip, Madjid Tavana,

Vipul Jain, and Srikanta Patnaik, editors. Volume 1005, pages 225–35, Singapore: Springer.

38. Meng, X, Nie, L, and Song J. (2019). "Predicting terrorist attacks using big data." Computers Electr Eng 2019; 77:120–7.
39. Ouassini, N., & Verma, A.K. (2018). "Demographic Conditions or Socioeconomic Inequality: A Micro-level Examination of Terrorism in Jharkhand" Victim Justice and Victimology Journal, 1, 63–84.
40. Olabanjo, O. A., Aribisala, B. S., Mazzara, M., Wusu, A. S. (2021). "An ensemble machine learning model for the prediction of danger zones: Towards a global counterterrorism." Soft Computing Letters, 3, 100020.
41. Pan, X. (2021). "Quantitative analysis and prediction of global terrorist attacks based on machine learning. Scientific Programming", 2021, 1–15.
42. Pilnenskiy, N., & Smetannikov, I. (2020). "Among the Python data analysis tools are feature selection algorithms. Future Internet," 12(3). 10.3390/fi120305 can be found here.
43.
44. Héberger, K., Bajusz, D., and Rácz, A. (2021). "Effects of train/test split ratios and dataset size on multiclass QSAR/QSPR classification. Molecular Structures and Dynamics", 10.3390/molecules 26041111.
45. Rai, H, Chatterjee K, and Dashkevich S. (2021). "Using a novel hybrid unetresnext-50 deep CNN model, automatic and accurate abnormality detection from brain MRI images is achieved": Biomed Signal Processing Control 2021; 66:102477.
46. Sarker, A. Chakraborty, P. Sha, S., Khatun, M., Hasan, M. and Banerjee, K. (2020). "Improvised technique for analyzing data and detecting terrorist attack using machine learning approach based on twitter data," Journal of Computer and Communications, vol. 8, no. 7, pp. 50–62, 2020.
47. Saiya, N., and Scime, A. (2019). "Comparing classification trees to discern patterns of terrorism". Social Science Quarterly, 100(4), 1420–1444.
48. Srinivasa, K., Thilagam, P. S. (2019). "Crime base: Towards building a knowledge base for crime entities and their relationships from online newspapers. Information Processing & Management", 56(6), 102059.
49. Sarker, A. Chakraborty, P. Sha, S., Khatun, M., Hasan, M. and Banerjee, K. (2020). Yang, Y., Song, Y., Chen, B., and Hou, N. (2022). "Oil prices and terrorist attacks: An analysis of time-varying causal relationships" 246: [www.elsevier.com] 123340–12350.
50. Saidi, F., and Trabelsi, Z. (2022). "A hybrid deep learning-based framework for modeling and predicting future terrorist activities." Egyptian Informatics Journal, 23(3), 437–446.
51. Tolan, G. and Soliman, O. (2017). "An experimental study of classification algorithms for terrorism prediction," International Journal of Knowledge Engineering-IACSIT, vol. 1, no. 2, pp. 107–112.
52. Thaseen, I., Kumar, C. and Ahmad, A. (2019). "Using an ensemble of classifiers and chi-square feature selection to create an integrated intrusion detection model," Arab. J. Sci. Eng. 44 (2019) 3357–3368.
53. Zeb, A., Saeed, Y., Aziz, F., Zada, N., Uddin, M. I., et al. (2020). "Deep neural network prediction of future terrorist activities." 2020(17) Intricacy, 1–16.
54. Uddin, M., Zada, N., Aziz, F., Saeed, Y., Zeb, A., Ali Shah, S. & Mahmoud, M. (2020). "Prediction of future terrorist activities using deep neural networks": 1-16 (www.hindawi.comy).
55. Varun, M., Lavanya E., Piyush, V., and Nirmalya, R. (2023). "A Systematic Review and Future Prospects of Crime Prediction Using ML and DL". ID for Digital Object 10.1109/ACCESS.2023.3286344.

56. Wang, Z. & Wang, J. (2021). “Utilizing Machine Learning for Resource Management and Public Security Information”. Science and Technology, 2021. 10.1155/2021/4734187 is the URL to use.
57. Chen, R., Lai, K. K., Yu, L., and Zhou, R. (2022). "One-Hot Encoding or Imputation for Preprocessing Missing Data for Credit Classification?"58(2) Finance and Trade in Emerging Markets.10,1080/1540496X.2020.1825935, since it may be found on the internet.
58. Zhou, Y. (2017). "Assault detection and network analysis of pro-ISIS fanboys using Twitter data," in 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA). IEEE, 2017, pp. 386–390.
59. National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2020). Global Terrorism Database [Data file]. Retrieved from https://www.start.umd.edu/gtd