International Journal of Computer Science Trends and Technology (IJCST) – Volume 14 Issue 2, Mar-Apr 2026

RESEARCH ARTICLE OPEN ACCESS

Ensemble Model for Location-Based Terrorism Prediction

Ariyo Olayemi Abimbola*, Maitanmi Stephen.O**, Izang A.A****
Computer Science
Babcock University
Ilisan,Ogun

ABSTRACT

In Nigeria, terrorist attacks by Boko Haram and Fulani militants have become increasingly frequent, yet existing predictive models trained on global datasets failed to capture the country's unique dynamics. Previous studies lacked integration of Geographic Information Systems (GIS), which resulted in imprecise location-based predictions, inaccurate attack predictions, a high rate of false positive alarms, a high rate of false negative alarms, and ineffective separation of "attack" locations from "no-attack" locations. Therefore, there is a need to mitigate against these limitations. Hence, this study developed an ensemble model for location-based terrorism prediction (EMTERROP). EMTERROP was developed using machine learning techniques with GIS integration in five stages: Stage 1 is the Data Collection stage, where data was gathered from the Global Terrorism Database (GTD) with filtered attack records for Nigeria and demographic data from Open Data for Africa. The datasets consist of 5,998 records for Nigeria from 1970 to 2024. Stage 2 involves data integration, where the GTD dataset was integrated with both demographic data and geographic coordinates. Stage 3 is the preprocessing of the dataset. This step was done using standard scalar for normalization; relevant features were selected using Recursive Feature Elimination with Cross Validation (RFECV). Six classifiers (Decision Tree, Random Forest, Gradient Boosting, AdaBoost, LightGBM, and CatBoost) were combined to make the ensemble model. Stage 4 involves model development, where the ensemble model was used to train the dataset. The dataset employed an 80/20 stratified split for training and validation, respectively, with hyperparameter optimization. Stage 5 is Evaluation, where the model performance was evaluated using Accuracy for precise location and inaccurate prediction of attacks, Precision for high false positive alarm, recall for high false negative alarm, and the F1 score to find the optimal balance between Precision and Recall and ROC-AUC for ineffective separation of "attack" locations from "no-attack" locations. Also, geocoding was used in mapping the precise location of attacks in Nigeria. Finally, the developed model was benchmarked with two existing models, which are XGBoost and CNN-LSTM. The evaluation of the EMTERROP shows the following result: Accuracy-98.1%, Precision-97.0%, Recall-98.0%, F1-score-98.0%, and ROC-AUC-98%. Geocoding successfully mapped incidents across Nigerian states, with Borno having the highest concentration of attacks at 70.5%. XGBoost and CNN-LSTM have the following results, respectively: XGBoost with Accuracy-78.90%, Precision-76.30%, Recall-77.80%, F1-score-77.05%, and ROC-AUC-81.20%. CNN-LSTM with Accuracy-72.30%, Precision-70.10%, Recall-71.50%, F1-score-70.80%, and ROC-AUC-75.40%. The study concluded that integrating machine learning with GTD, demographic data and GIS coordinates significantly enhanced the prediction of terrorism. Therefore, it is recommended that security and government agencies adopt EMTERROP for proactive threat assessment.

Keywords — Ensemble learning, Geographic Information System, Global Terrorism Database, Machine learning, Location-based terrorism prediction.

I. INTRODUCTION

Terrorism remains one of the major threats to contemporary society. It has destabilized numerous businesses, social organizations, nations, and the global community in recent years. In Nigeria, terrorist occurrences such as thefts, unintentional acts, attacks by Boko Haram and Fulani militants, as well as intra- and intergroup disputes, have become increasingly frequent. To restrict or minimize these operations, models capable of comprehending terrorist behavior and preventing or reducing the recurrence of such incidents must be developed [1]. The unpredictable nature of attacks, often occurring at unknown times, places, and against unsuspecting individuals demands that law enforcement reevaluate their strategies in light of recent technological advancements [2]. Artificial Intelligence (AI) and machine learning have emerged as transformative tools in this regard. Security agencies can leverage machine learning algorithms to provide accurate estimations, optimize resource allocation, and take proactive measures against terrorism. The success of counterterrorism strategies increasingly depends on precise forecasting powered by AI-driven models. Machine learning can utilize historical data to create and validate predictive models that assess the likelihood of attack success, suicidality, weapon type, timing, and location [3]. These models are capable of learning from large datasets, identifying hidden patterns, and making predictions that enhance the ability of security agencies to anticipate and prevent attacks. Advances in computational technologies have further enabled the development of powerful AI systems capable of handling the complex calculations required for predictive modelling. In this effort, five key characteristics linked to terrorist activities weapon type, region, attack type, suicidality, and likelihood of success will be predicted using machine learning techniques. Although previous studies on terrorism prediction and counterterrorism strategies have offered useful insights, significant gaps remain in the Nigerian context. Key issues include the absence of a distributed database for scalable and reliable dataset storage, the limited integration of GIS

for precise location mapping of terrorist incidents, and the underutilization of demographic and criminal history data that could enhance AI forecasting [4]. These shortcomings reduce the accuracy, adaptability, and long-term effectiveness of predictive counterterrorism systems. Unlike previous studies, this approach not only improves prediction accuracy but also ensures long-term data availability, precise localization of threats, and proactive monitoring of extremist activities. This holistic framework strengthens the ability of the Nigerian military and security services to identify, monitor, and forecast potential terrorist activities, thereby preserving lives and fostering national stability. In order to address those gaps, if AI can be ensemble we can have better predictions. Hence this research intends to develop an Ensemble Terrorism Prediction System.

II. RELATED LITERATURE

This study aims to explore a range of machine learning techniques and algorithms for terrorism prediction. It also seeks to provide location-based predictions using geocoding. This section reviews and analyses previous studies relevant to the topic. According to [5] applied five machine learning algorithms to analyse terrorism data from the Global Terrorism Database (GTD). Their study categorized the dataset into three dimensions: type of attack, region of attack, and weapon type used, enabling multi-label classification across different attributes of terrorist incidents. The authors employed standard classification models, although specific algorithm names and performance metrics were not clearly detailed in their report. While their work provides a foundational approach to multi-dimensional classification using terrorism datasets, it lacks integration of spatiotemporal intelligence and does not address how predictive accuracy varies across regions or time. As documented by [6] conducted a study on terrorist incidents in Southeast Asia (1970–2016) using GTD data. They applied five machine learning models, Support Vector Machines (SVM), Artificial Neural Networks (ANN), Naïve Bayes, Random Forest, and Decision Trees, to predict assault type, weapon type, and attack region, achieving over 90% accuracy. While the study showed strong performance, it lacked spatial visualization and deployment capabilities, limiting its utility for situational awareness or field operations. As mentioned by [7] applied K-Nearest Neighbour (k-NN) and Random Forest algorithms to classify and forecast various forms of terrorist acts. Their models achieved a prediction accuracy of up to 88%, demonstrating the effectiveness of ensemble and distance-based classifiers in terrorism-related prediction tasks. However, the study lacked geospatial integration and interpretability mechanisms, and the analysis did not consider socio-political drivers or regional variations in attack patterns. For example, as stated by [8] proposed a machine learning-based system to evaluate and predict terrorism incidents. Using a variety of algorithms including Logistic Regression, Decision Trees, Gaussian Bayesian Networks, AdaBoost, and Random Forest, the study sought to identify high-risk patterns in terrorism-related data. While their approach embraced modern ML techniques, the system lacked spatial modelling which limits its use for on-ground operational decision-making. In another study by as documented by [9] applied ensemble learning algorithms to predict attack types, weapon types, and target types within terrorism data. Their models achieved predictive accuracy ranging between 79% and 86%, highlighting the utility of ensemble approaches for multiclass classification in terrorism analytics. While effective in model performance, the study did not incorporate spatial or temporal dynamics. The absence of interpretability tools or deployment mechanisms also limited its operational value for counterterrorism. Similarly, [10] conducted a comparative study of machine learning models for classifying terrorist incidents in Nigeria. They implemented classifiers such as Random Forest, LightGBM, and SVM, and reported promising performance metrics. Yet, while their analysis focused on classification accuracy, they did not include a deployable model or a distributed architecture for analytics, critical features addressed in the current study through the integration of a web-based platform and a distributed database.

III RESEARCH METHODOLOGY

The approach is a machine-learning pipeline that preprocesses and combines terrorism event data (from the Global Terrorism Database) and supplementary demographic data before training a group of tree-based classifiers to forecast attack occurrences. The process starts by combining demographic and socioeconomic data with terrorism incidences from the open-source GTD, which contains over 181,692 reported assaults from 1970 to 2024. Using NumPy and scikit-learn in Python, data cleaning and feature engineering are carried out, which includes choosing pertinent variables and encoding categorical fields.

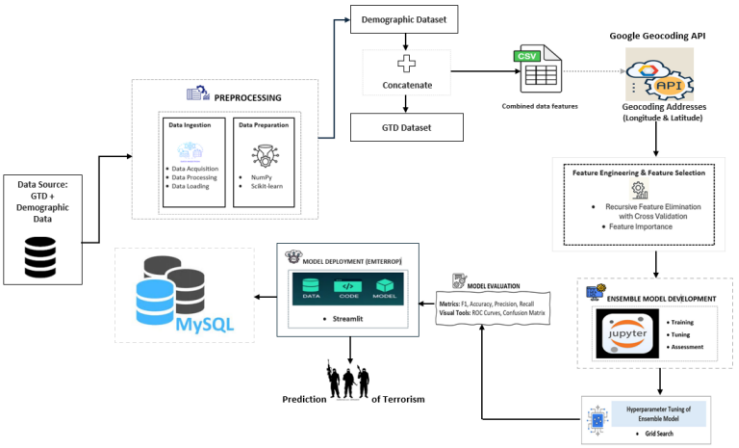

Fig. 1 Proposed Model (Researcher's Model)

For scalability and effective retrieval, geographic addresses were geocoded using the Google Geocoding API to attach latitude/longitude coordinates and then saved in a distributed MySQL database. An ensemble model that includes techniques like Decision Tree, Gradient Boosting, AdaBoost, LightGBM, CatBoost, and Random Forest were trained using a Jupyter environment. Across all evaluation metrics, the ensemble model exhibits the best overall performance and accuracy. The predictive model was developed in Jupyter Notebook, as shown in Figure 1, optimized by hyperparameter tuning using Grid Search, and assessed using metrics like accuracy, precision, recall, F1-score, and ROC-AUC, supported by visual tools like ROC curves and confusion matrices. The model was made available as a live web application using Streamlit, which offers an interactive interface that lets users enter information, make predictions, and see the dangers of terrorism on maps connected to certain geographic locations.

A. Data Sources

The study used the Global Terrorism Database (GTD), maintained by START, as its main data source. The GTD is a public database of terrorist incidents worldwide from 1970 to 2024, containing detailed event-level information such as attack type, target, weapons,

casualties, property damage, and location. For this research, only records related to terrorist attacks in Nigeria were extracted. In addition, demographic data from OpendataforAfrica.org, including indicators such as population, GDP, education, infrastructure, and unemployment, were collected to enrich the dataset. These socioeconomic variables were matched with GTD records by year and country to provide context on the conditions surrounding each attack.

B. Google Maps Geocoding API

Text-based location descriptions were converted into exact latitude and longitude coordinates using Google Maps Geocoding API. The terrorism dataset was then merged with relevant socio-demographic data to form a single enriched dataset (D_GEO) for further analysis. This geocoding process improved GIS-based analysis by enabling accurate mapping and tracking of terrorist incidents across different locations, ensuring that each record was geographically referenced for spatial analysis and response planning.

C. Data Preprocessing

Data preprocessing is a key stage in data analysis and machine learning because it transforms raw, unstructured data into a clean and usable format for analysis and model training. It improves data quality, consistency, and reliability by handling issues such as noise, duplicates, missing values, and inconsistencies. Data ingestion, as the first step in this process, involves collecting and importing data from different sources for further analysis. In this study, the main dataset was the Global Terrorism Database (GTD), which contains detailed records of terrorist incidents worldwide from 1970 to 2024. A subset of 5,998 incidents related to Nigeria was extracted for the research. To strengthen the analysis, additional socioeconomic and demographic data were also collected and merged with the terrorism data. The datasets were downloaded as CSV files, imported into Python using the pandas library, and prepared for cleaning, transformation, and integration. After preprocessing, the dataset was prepared for analysis and model training using Python libraries such as NumPy and Scikit-learn. The cleaned data was converted into a structured, machine-readable format with NumPy arrays for efficient computation. Categorical variables were encoded, numerical features were scaled, and any remaining missing values were imputed. Finally, the data was divided into input features (X) and target labels (y), creating a well-organized foundation for predictive modelling.

D. Model Design

EMTERROP was designed as a multilayered framework that ensures a seamless process from data collection and GIS coordinate generation to terrorism prediction. It integrates machine learning with GIS technologies to support location-based risk analysis. The study developed EMTERROP (Ensemble Model for Location-Based Terrorism Prediction), a machine learning system for predicting terrorism risk in Nigeria. The framework followed key phases: integrating GTD, demographic, and geospatial data for 5,998 incidents in a MySQL database; developing multiple base models and combining them through a stacking ensemble; evaluating model performance and the contribution of each data source; and deploying the final model as a Streamlit web application that generates real-time terrorism risk predictions classified as Low, Moderate, or High.

E. Prediction using Ensemble Model (EMTERROP)

A stacked ensemble learning architecture is used by the EMTERROP system to enhance terrorism-risk prediction throughout the 36 states of Nigeria. Six base classifiers—Decision Tree, Gradient Boosting, AdaBoost, LightGBM, CatBoost, and Random Forest—each separately calculate class probabilities in this architecture using input data like demographic, geographic, and contextual variables. Each base model produces a probability P_i (x) for a given input x, which indicates the possibility of an assault. These probabilities are then combined by the ensemble engine using a weighted voting (or averaging) mechanism:

$$P_{\text{ensemble}}(x) = \sum_{i=1}^{n} w_i \;\; P_i(x),),$$

where w_i represents the learned or pre-assigned weight of model i The final predicted class corresponds to the highest aggregated probability. The ensemble design offers several advantages over a single model. By combining classifiers with different strengths, it captures a wider range of patterns in the data. It also reduces variance, lowers the risk of overfitting, and improves performance on unseen data. In addition, the ensemble is more robust to noise, outliers, missing values, and imbalanced data, which are common in terrorism datasets. The final prediction is made by selecting the class with the highest ensemble probability, making EMTERROP more stable, accurate, and reliable for terrorism risk prediction and decision support.

IV. MODEL EVALUATION

The final model was evaluated on test data using standard classification metrics, including accuracy, precision, recall, and F1-score. These measures were derived from the confusion matrix [11], which shows true and false predictions across classes. In multiclass cases, weighted or macro averages were used. The ROC curve and AUC could also be applied to show the balance between true positive and false positive rates. Together, these metrics provide a complete view of model performance, with recall showing how well actual attacks are identified, precision indicating the rate of false alarms, and F1-score balancing both.

F. Accuracy

Accuracy discloses, in general, how the model work and whether a model is being trained properly and correctly. However, it does not give specific details on how it tried to solve the problem. As your primary success, the demerit in using machine learning (ML) accuracy is that, when there is a significant class divide, it fails inadequately [12]. Accuracy may be false for the unbalanced datasets. For evaluating classification models, accuracy is one metric. It has the following definitions formally:

$$Accuracy = \frac{No.\ of\ correct\ predictions}{Total\ no.of\ predictions}$$

G. Precision

When the cost of false positives (FP) is high, then the precision helps. Quantified the proportion of true positives among all predicted positives for each attack type, helping to assess how often the model's predictions were correct when a certain class was flagged [13]. After being assaulted with false alarms, those who detect the results will ignore them when the false positives are too high.

H. Recall

Which is also called recall TPR (true positive rate), is a metric related to the classification model. Captures the model's ability to

correctly identify all actual instances of a particular class, making it especially important for detecting rarer but critical attack categories.

I. F1-Score

This is a measure of a model's accuracy on a dataset. It is used to evaluate binary classification systems, which classify examples into 'positive' or 'negative'. The F1-score is a way of combining the precision and recall of the model, and it is defined as the harmonic mean of the model's precision and recall. The F1-score is commonly used for evaluating information retrieval systems such as search engines, and for many kinds of machine learning models. It is possible to adjust the F-score to give more importance to precision over recall, or vice versa. F1 score uses precision to get the rate of true positive records among the total records classified as positive by machine learning model

J. ROC-AUC

This was used with a one-vs-rest approach to assess how well the models distinguished between different attack categories. The ROC curve shows the relationship between the true positive rate and false positive rate across different thresholds, giving a visual measure of classification performance. The AUC summarizes this performance, with higher values indicating better discrimination between classes. Overall, ROC-AUC helps show how effectively the model separates positive and negative cases and supports threshold-based decision making.

TABLE 1
Cross-Validated Performance Metrics

Performance Metric	Values
Accuracy	0.981
Precision	0.970
Recall	0.980
F1-Score	0.980
AUC	0.98

Table 1 shows that the model performed very well, achieving about 98% accuracy. It also recorded 83% recall, meaning it detected most actual positive cases, and 97% precision, showing that most predicted attacks were correct. The high F1-score of 0.98 indicates a strong balance between precision and recall, while the AUC of 0.98 confirms the model's strong ability to distinguish between positive and negative cases. Overall, these results show that the model is effective, reliable, and suitable for real-world use.

V. MODEL DEPLOYMENT (EMTERROP)

An Ensemble Model was trained using the EMTERROP pipeline, which collects confirmed terrorism incident data and stores it in a cloud-based MySQL database. After training and validation, the top-performing model is selected for deployment. The online interface that hosts the model and displays predictions is built using Streamlit, an open-source Python framework. A remote MySQL database houses all recorded terrorism incidents, ensuring shared data storage and persistence. The Streamlit application connects to this database (e.g. via conn = st.connection('mysql', type='sql')) and supports both data entry and retrieval. New incident reports are added with an INSERT statement:

```
with conn.session as s: s.execute("INSERT INTO incidents (...)
                        VALUES (...);")
                        s.commit()
```

The process ensures that all incident records remain up to date in the cloud database for future training or retrieval. Once the training and validation cycles are complete, the best-performing Ensemble Model was serialized and saved to a file so that the application can load it at runtime. Users can submit data through the interactive interface, and the saved model was loaded to produce predictions via model.predict(...) on the input features. The form also allows users to report new events, which are then stored in MySQL for future access and model retraining. The application also supports historical analysis by retrieving and presenting past incident reports on the user dashboard. Finally, the complete EMTERROP system including database connection configurations, the trained model, and application code were deployed to Streamlit Community Cloud. Users can log in, submit data, receive real-time predictions, and conveniently record new reports through the shareable and interactive web application. (https://terrops.streamlit.app/).

K. DISTRIBUTED DATABASE SYSTEM DESIGN

To handle incident reports related to terrorism that users submit using the "Make Report" module, the EMTERROP program integrates a distributed database system. In order to store, retrieve, and process reports for upcoming machine learning activities, this system must guarantee scalable data management, fault tolerance, and high availability

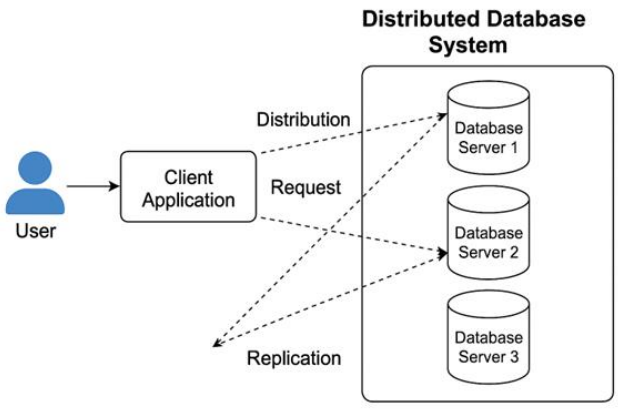

Fig. 2 Distributed Database System (Researcher's Model)

Multiple database servers—Database Server 1, 2, and 3—are part of the distributed database system, which is seen in Figure 3.8. These servers all take part in the distributed processing and storing of submitted data. The Client Application Layer controls communication between the frontend and the backend database cluster and directs information sent by a user who submits a terrorism report using the client-facing interface (created with Streamlit and Python). The architecture facilitates three primary functions:

i) Distribution:

Submitted data was intelligently routed to specific servers based on parameters such as location, type of attack, or timestamp. This helps balance the load and optimize access efficiency.

ii) Request and Retrieval:

When a user or analyst queries past data (e.g., for analytics or training), the client application sends the request to the appropriate

server holding the relevant dataset. This allows for parallel access and low-latency retrieval.

iii) Replication:

To maintain data consistency and redundancy, every report was replicated across the database servers. The replication ensures that even if one server fails; others can provide uninterrupted access to the stored information.

VI. COMPARATIVE ANALYSIS OF ENSEMBLE MODELS FOR TERRORIST ATTACK PREDICTION

The study compared six machine learning classifiers to develop an ensemble model for predicting terrorist attacks. Using a filtered subset of the Global Terrorism Database focused on Nigeria, the final dataset contained 5,998 records, with 4,798 used for training and 1,200 for testing. Eleven predictor variables were selected based on statistical relevance, feature importance, and expert knowledge. The models were developed in Python using Scikit-learn, with Pandas and NumPy for data handling and Matplotlib and Seaborn for visualization. Each classifier's performance was assessed using ROC-AUC, F1 Score, Accuracy, Precision, Recall, and Prediction Time (to measure computational efficiency). With an F1 score of almost 0.98 and a macro-average ROC-AUC of roughly 0.99, the Ensemble Model significantly outperformed all other models in terms of overall performance and demonstrated the ability to distinguish between different assault types.

TABLE 2

Comparative Performance Summary of Classifiers

Model	Accuracy	Precision	Recall	F1 Score	ROC-AUC	Prediction Time (s)
Decision Tree	0.796535	0.792951	0.794610	0.793732	0.70	0.597026
Gradient Boosting	0.657535	0.652900	0.657535	0.650806	0.68	161.774154
AdaBoost	0.326274	0.316926	0.326274	0.312315	0.52	5.031283
LGBM	0.789526	0.785739	0.789526	0.785871	0.70	12.759854
CatBoost	0.797226	0.791548	0.797226	0.792848	0.69	144.531128
Random Forest	0.830545	0.827239	0.830446	0.828213	0.71	15.383599
⭐**Ensemble Model**	**0.980000**	**0.970000**	**0.980000**	**0.980000**	**0.990000**	**18.920000**

Additionally, it demonstrated a high recall rate and good accuracy, especially when it came to anticipating common attack types like bombing/explosion and armed assault. If deployment speed is an issue, other effective models such as CatBoost, LightGBM, and Decision Tree also demonstrated promising outcomes. Although Gradient Boosting delivered reasonable accuracy, its longer training time could limit its practical use. Owing to its excellent balance of accuracy, reliability, and computational efficiency, the Ensemble Model was selected as the primary predictor in the EMTERROP system based on this comparative analysis.

VII. ENSEMBLE MODEL PREDICTION RESULT

In evaluating the predictive capabilities of the system, we first generated predictions using each individual model (Decision Tree, Gradient Boosting, AdaBoost, LightGBM, CatBoost, Random Forest) on a given input (state + date + associated features). For each model, we recorded its output, typically a probability percentage. These individual model results were summarized in table 4. The system computed a combined prediction using the ensemble method: the individual model outputs (probabilities) were aggregated according to pre-defined (or learned) weights to produce the final ensemble probability of a terrorist attack. The final output was then presented as the definitive prediction result for the user. When a user submits a prediction request, the ensemble produces a final probability score indicating the likelihood of a terrorist incident in the selected location and time.

TABLE 3

Predicted Attack Probability Percentage Score for Individual Models

Model	Predicted Attack Probability (%)
Decision Tree	67.2
Gradient Boosting	72.5
AdaBoost	58.3
LightGBM	75.8
CatBoost	77.4
Random Forest	79.1
Ensemble Model	88.6

VIII. COMPARATIVE BENCHMARKING OF EMTERROP WITH PRIOR STUDIES

The EMTERROP framework was benchmarked against relevant studies from the literature review (Trained on Nigeria GTD Subset) based on performance metrics, methodological features, and deployment readiness. The comparison demonstrates EMTERROP's advancements in accuracy, integration, and practical utility.

TABLE 4

Performance and Feature Comparison of EMTERROP with Related Works (Trained on Nigeria GTD Subset)

Study / Model	Dataset Used	Best Model	Original Reported Result	Result on EMTERROP Dataset	GIS Integration	Deployment	Database	Nigeria-Specific
EMTERROP (This Study)	GTD + Demographics	Ensemble (Stacking)	**A**-98.10% **P**-97.0% **R**-98.0% **F1**-98.0% **ROC-AUC**-98.0%	**A-98.10% P-97.0% R-98.0% F1-98.0% ROC-AUC - 98.0%**	Yes	Yes (Web App)	Distributed MySQL	Yes
[90] – Southeast Asia	GTD	SVM/ ANN	**A**-90.00% **P**-89.40% **R**-88.70% **F1**-89.05% **ROC-AUC**-91.20%	**A-68.20% P-65.80% R-66.90% F1-66.35% ROC-AUC-71.60%**	No	No	No	No (Regional)
[103] – Terrorist Org Prediction	GTD	XGBoost	**A**-97.16% **P**-96.80% **R**-96.50% **F1**-96.65% **ROC-AUC**-97.30%	**A-78.90% P-76.30% R-77.80% F1-77.05% ROC-AUC-81.20%**	No	No	No	No (Global)
[145] – CNN-LSTM Hybrid	GTD	CNN-LSTM	**A**-88.00% **P**-87.20% **R**-86.80% **F1**-87.00% **ROC-AUC**-89.50%	**A-72.30% P-70.10% R-71.50% F1-70.80% ROC-AUC-75.40%**	Limited	No	No	No (Global)

Figure 3 compares the performance of different machine-learning models using Accuracy, Precision, Recall, F1 Score, and ROC-AUC. The Ensemble Model achieved the best overall results, outperforming the benchmark models in nearly all evaluation metrics. Its strong

accuracy, F1-score, and balanced precision and recall indicate consistent and reliable classification performance. These results confirm that the Ensemble Model is the most effective and stable option among those tested, supporting its adoption in the EMTERROP system.

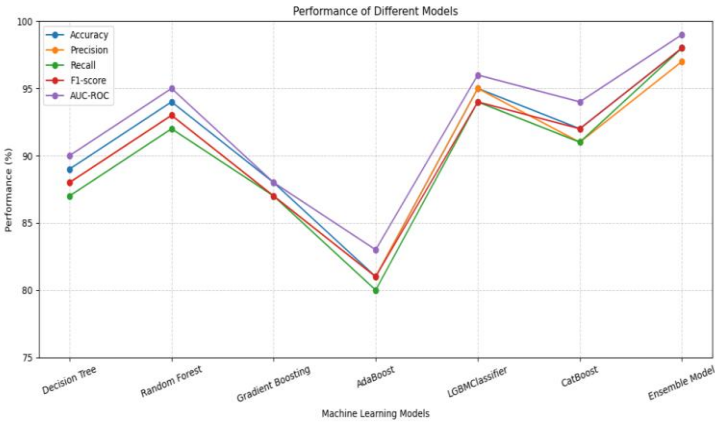

Fig. 3 Ensemble Model Performance Comparison against Benchmark Models using Line chart (Researcher's model)

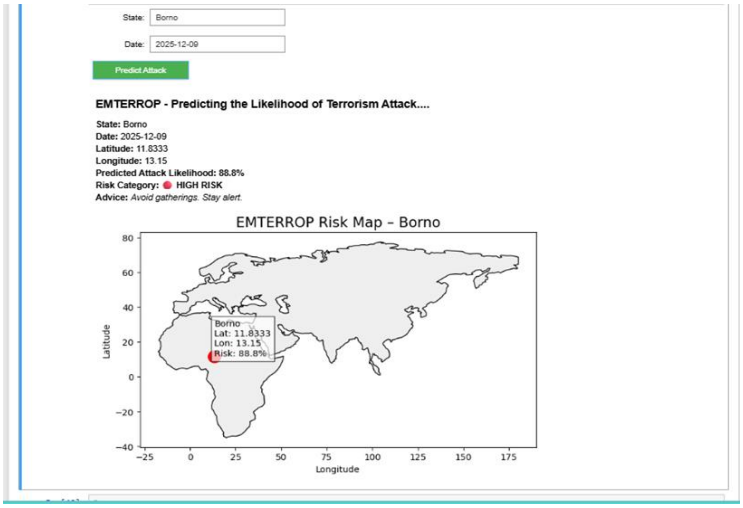

Fig 4. EMTERROP Terrorism Risk Prediction Interface for Borno State

Figure 4 is the EMTERROP risk prediction interface. It displays the selected state, date, latitude, and longitude, then gives the predicted attack likelihood and classifies the area into a risk category. In this example, Borno is classified as high risk, with an attack likelihood of 88.8%. The map below pinpoints the location and helps users see where the prediction applies geographically.

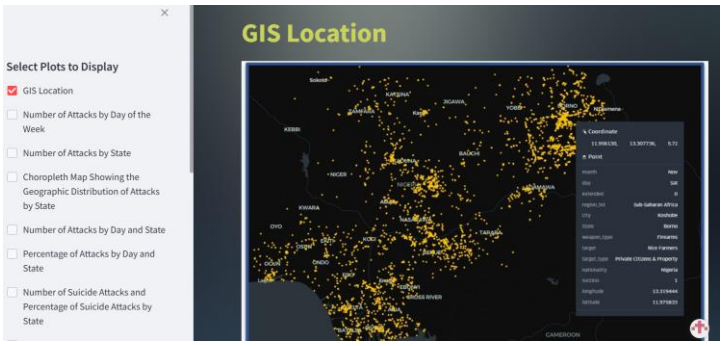

Fig 5. GIS Map Showing the Location Distribution of Terrorist Incidents in Nigeria

The GIS location map in figure 5, which shows the location based distribution of terrorism incidents across Nigeria. The yellow points represent recorded attack locations, while the highlighted point provides detailed geographic information such as coordinates, state, and city. This map helps identify areas with higher concentrations of incidents and supports spatial analysis of terrorism patterns.

IX. IMPLEMENTATION OF THE EMTERROP

A predictive and analytical tool called the Ensemble Model for Terrorism Prediction (EMTERROP) system was created to establish the probability of terrorist attacks in particular areas. Its major purpose was to enhance proactive counterterrorism tactics by identifying potential high-risk areas before attacks occur. EMTERROP offers a comprehensive platform for studying data connected to terrorism by combining location-based monitoring, citizen reporting systems, and ensemble models. In order to produce predicted insights that help security agencies make prompt and well-informed judgments, the system analyzes both historical and current data. The Make a Report function, which allows users to submit incident reports straight into the system, is a crucial part of the architecture. All submitted data are stored in a centralized database, ensuring efficient data management, retrieval, and analysis. This centralized storage was specifically designed to address the scarcity of terrorism-related datasets tailored to Nigeria, thereby creating a valuable repository for research and policy development. The EMTERROP system comprises interconnected context. See below each module: The home page as seen in figure 6 displays several buttons, including Prediction, Visualization, make a Report, About, and Login, each designed to perform a specific function aimed at proactively managing and preventing terrorism.

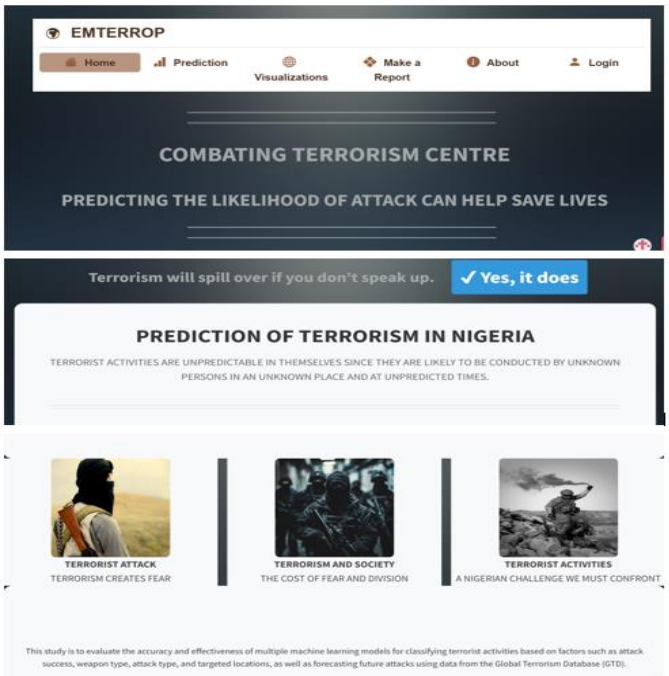

Fig 6. EMTERROP Home Page

The Login Page provides a simple interface for user authentication, requiring a username and password. It features a welcome message introducing the application as a terrorism prediction tool and emphasizes the need to log in to submit a report.

The design includes a password visibility toggle and a straightforward layout with a Login button as shown in Figure 7.

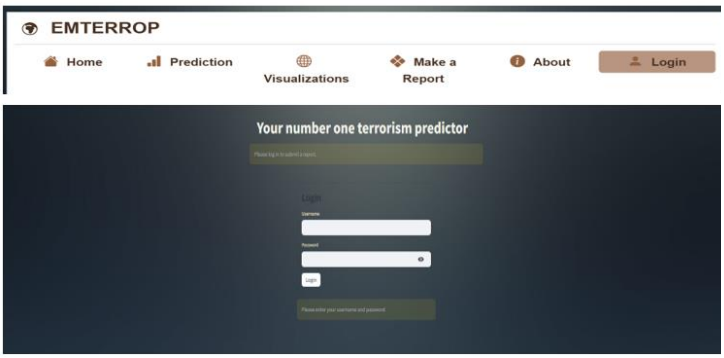

Fig 7. EMTERROP Login Page

The model predicts a low probability of 45.68% for a terrorist attack. Along with the prediction, it provides a recommendation to proceed with daily activities while remaining vigilant and being informed through credible news and security updates, as illustrated in Figure 8. This highlights how EMTERROP delivers actionable insights, even in low-risk scenarios, to promote safety and awareness.

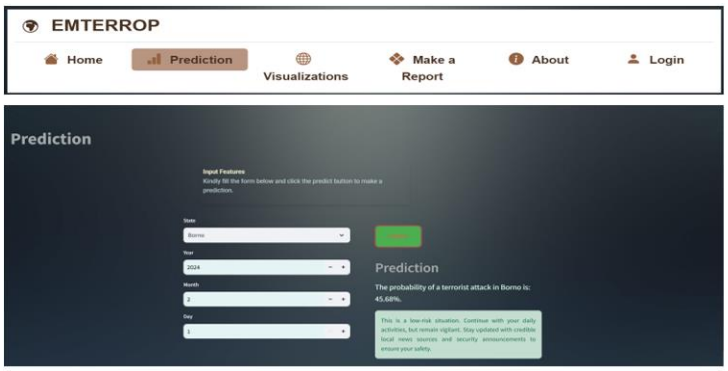

Fig 8. EMTERROP Prediction Page - Low Risk

The risk level is significant when users input specific features such as state, year, month, and day to predict the likelihood of a terrorist attack. For the given inputs (Anambra, 2024, May 7), the prediction shows a high probability of 65.38% for a terrorist attack. This result is accompanied by a warning message urging security agencies to implement immediate and rigorous measures to mitigate the risk as seen in Figure 9, underscoring the tool's critical role in proactive security planning.

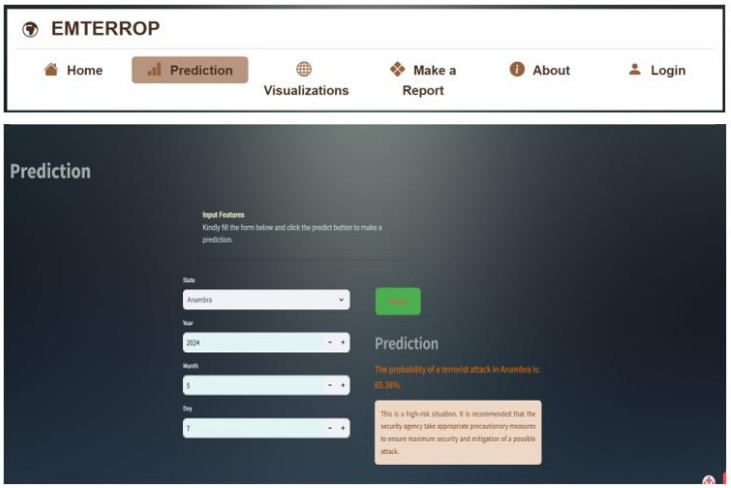

Fig 9. EMTERROP Prediction Page - High Risk

The "Make a Report" page as shown in Figure 10 enables users to report details of terrorist incidents through a structured form. It allows users to input information such as the location, weapon type, casualties, attack specifics, and their contact details. The form features interactive dropdown menus and input fields, facilitating the collection of data for analysis, prediction, and documentation purposes. This report is stored in the central database for later retrieval.

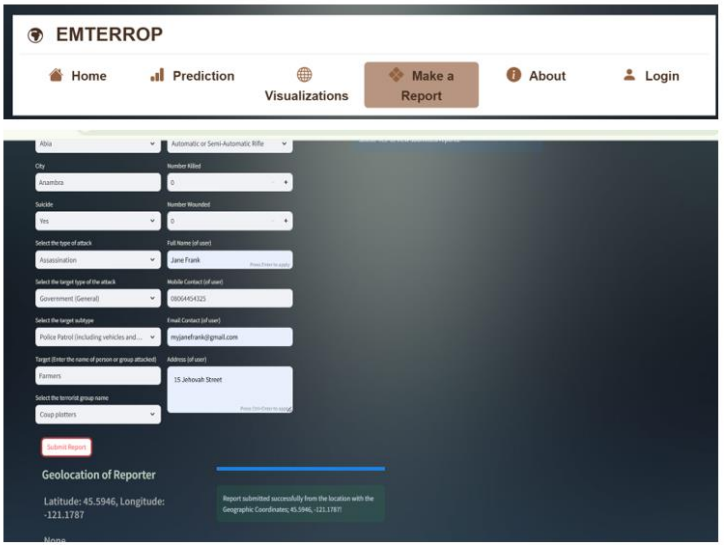

Fig 10. EMTERROP Make a Report Page

The Submitted Reports section features a table summarizing user-submitted details of terrorist incidents, including information such as location, attack type, and target etc. Designed as a historical data review tool, it is likely tied to the "Show submitted reports?" option for toggling visibility as shown in Figure 11. This section was incorporated to address the lack of terrorism data specifically tailored to Nigeria for this research. It also serves as a storage solution for future retrieval and inference.

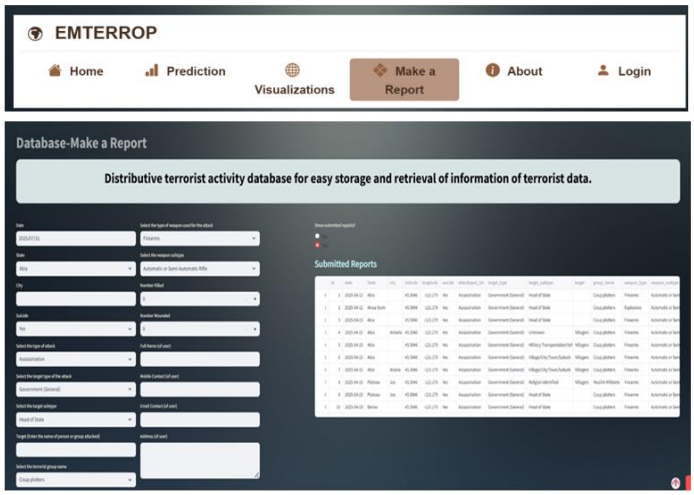

Fig 11. EMTERROP Submitted Report Page on the Distributive Database

X. DISCUSSION AND FUTURE WORK

The results above provide a thorough assessment of the EMTERROP predictive framework's effectiveness in classifying terrorism incidents in Nigeria compared against a variety of benchmark machine-learning models. Using a stratified 80/20 split, the dataset was divided into training and testing sets, and the hyperparameter set with the highest cross-validated F1 score was identified via GridSearchCV. The Ensemble Model outperformed all individual classifiers: it achieved an accuracy of 98.1%, with similarly strong precision, recall, and F1-score values (Precision ≈ 97.0%, Recall ≈ 98.0%, F1-score ≈ 98.0%) and recorded a prediction time of approximately 18 seconds on the same hardware. Because EMTERROP combines multiple learners and leverages their complementary strengths, it successfully captures complex, non-linear patterns in high-dimensional feature space, mitigates overfitting, and produces stable, reliable predictions. The preprocessing pipeline begins with data collection and cleaning, then numerical features are normalized using StandardScaler or MinMaxScaler and categorical variables are encoded using LabelEncoder or OneHotEncoder. Feature selection was performed using Recursive Feature Elimination with Cross-Validation (RFECV) to retain only the most predictive features. The system was implemented in Python with a MySQL backend database and a Streamlit frontend, enabling users to enter new incidents, retrieve historical data, and generate predictions, thereby establishing EMTERROP as a practical, scalable solution for real-time terrorism risk assessment across Nigeria.

To further advance the EMTERROP framework for terrorism prediction in Nigeria, future studies should consider expanding the dataset to include more recent and diverse incident records from various regions and socio-economic backgrounds, which would enhance the model's generalizability and robustness. Incorporating additional data sources, such as real-time intelligence feeds, social media analytics, and qualitative insights from security experts, could provide a more comprehensive understanding of terrorism dynamics. Future developments could involve integrating IoT and exploring Deep learning and AI techniques and integrating temporal or sequential data may further improve predictive accuracy and adaptability to evolving threats. Field validation and pilot deployments in collaboration with security agencies are also recommended to assess the system's practical effectiveness and facilitate its integration into operational workflows. Finally, ongoing updates and refinements based on user feedback and emerging trends will help ensure the continued relevance and impact of the predictive framework.

XI. LIMITATION FROM THE REVIEW

Despite the advancements made by the study in terrorism prediction and classification using the EMTERROP framework, several limitations should be acknowledged. The research relied primarily on historical data from the Global Terrorism Database, which may not capture the most recent trends or emerging tactics in terrorism, potentially affecting the model's adaptability to evolving threats. The geographic and socio-economic features used, while comprehensive, may not fully represent all contextual factors influencing terrorism incidents across Nigeria. Additionally, the system's performance was evaluated using retrospective data and cross-validation, without real-time field testing or operational deployment, which limits the assessment of its practical effectiveness in live counterterrorism scenarios. The computational requirements for training ensemble models may pose challenges for implementation in resource-constrained environments. Finally, the absence of certain data types, such as real-time intelligence feeds or qualitative insights from security experts, may restrict the model's predictive scope and accuracy.

XII. RECOMMENDATIONS AND CONTRIBUTION TO KNOWLEDGE

To further improve the effectiveness and reach of the EMTERROP predictive framework for terrorism prediction in Nigeria, it is recommended that future research expand the dataset to include more recent and diverse incident records, as well as additional socio-economic and environmental variables. Integrating real-time data sources and collaborating with security agencies could enhance the system's responsiveness and practical value. Efforts should also be made to validate the framework in operational settings, ensuring its adaptability and reliability in real-world counterterrorism scenarios. Developing a robust system that has user-friendly interfaces and training modules for end-users, for security personnel, this would facilitate broader adoption. Exploring the integration of advanced ensemble methods and incorporating temporal data could further boost predictive accuracy and support more proactive decision-making in terrorism prevention and response. The research recorded significant contributions to the field of terrorism analytics in Nigeria by developing the EMTERROP predictive framework, which integrates machine learning with GIS intelligence for proactive terrorism prediction and classification. By leveraging a refined, Nigeria-specific subset of the Global Terrorism Database and incorporating both geographic and socio-economic features, the study addresses the limitations of previous models that lacked local relevance and spatial data integration. The highlighting of multiple ensemble classifiers, with the Ensemble Model achieving robust performance, sets a new standard for predictive accuracy in this context. Additionally, the creation of a scalable, distributed database system for terrorism incident storage and retrieval enhances the practical utility of the framework. The work provided a foundation for future research in data-driven security solutions and supported more informed, evidence-based decision-making for counterterrorism efforts in Nigeria.

XIII. CONCLUSION

The research successfully developed and validated the EMTERROP predictive framework for terrorism prediction in Nigeria, integrating machine learning techniques with GIS intelligence to address critical gaps in previous studies. Utilizing a refined subset of the Global Terrorism Database and incorporating both geographic and socio-economic features, the study considered multiple ensemble classifiers with accuracy of 98.1%, a precision of 97.0%, a recall of 98.0%, an F1-score of 98.0%, and a ROC-AUC of 0.98. These results clearly demonstrate the model's robust ability to distinguish between attack and non-attack instances, making it highly suitable for counterterrorism applications. The system's architecture, built with Python, Streamlit, and MySQL, supports scalable data storage, efficient retrieval, and GIS-enhanced decision support, enabling users to input new incidents, access historical data, and obtain actionable predictions. By addressing the lack of Nigeria-specific predictive systems, integrating GIS data, and providing a scalable terrorism database, this research advances the field of terrorism analytics and offers a practical tool for anticipating and mitigating terrorist attacks. The EMTERROP framework's strong performance and adaptability position it as a valuable resource for security agencies, with potential for further enhancement through expanded datasets and additional predictive features.

REFERENCES

[1] A. O. Olufemi, M. Adeosun, and P. O. Tayo, "Prediction of terrorist activities in Nigeria using machine learning models, Innovations, no. 71, 2022. [Online]. Available: https://www.researchgate.net/publication/366090665"

[2] K. McKendrick "Artificial intelligence prediction and counterterrorism. London: The Royal Institute of International Affairs-Chatham House, 2019"

[3] H. Abdullah, S. Dabeeruddin, S. Jadran, and Z. Ameema, "Intelligent Automation of Crime Prediction using Data Mining, in Proceedings of the 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE), 2022. DOI: 10.1109/ISIE51582.2022.9831620"

[4] K. Idhoko and J. Ojaiko, "Integration of Geographic Information Systems (GIS) and Spatial Data Mining Techniques in Fight against Boko Haram Terrorist in Nigeria, International Journal of Science and Research (IJSR), vol. 3, pp. 1-8, 2014"

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

[6] M. Junaedi, A. Fachrurozi, M. R. Kusumayudha, and W. Gata, "Analysis of the Classification of Terrorist Attacks in Indonesia," JITE, vol. 4, no. 1, Jul. 2020. DOI: 10.31289/jite.v4i1.3788.

[7] H. Mo, X. Meng, J. Li, and S. Zhao, "Terrorist event prediction based on revealing data, in Proceedings of the IEEE 2nd International Conference on Big Data Analysis (ICBDA), Beijing, China, 2017, pp. 239–244"

[8] S. Saha, H. Aladi, A. Kurian, and A. Basu, "Future Terrorist Attack Prediction Using Machine Learning Techniques," 2019.

[9] J. K. Ndambuki, "An Algorithm for Identification of Terror Events and Hotspots Using K-means and Discriminant Analysis," Strathmore University Repository, 2021. [Online]. Available: https://su-plus.strathmore.edu/handle/11071/10943. [Accessed: Jun. 29, 2025].

[10] I. E. Bello, "Space Technology and Geospatial Intelligence for National Security in Africa," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/376987314. [Accessed: Jun. 29, 2025].

[11] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825-2830, Oct. 2018. [Online]. Available:

[12] J. Erbani, P.-E. Portier, E. Egyed-Zsigmond, and D. Nurbakova, "Confusion Matrices: A Unified Theory," *IEEE Access*, vol. 12, pp. 181372–181419, 2024, doi: 10.1109/ACCESS.2024.3507199

[13] D. Krstinić, A. Kuzmanić Skelin, I. Slapničar, and M. Braović, "Multi-Label Confusion Tensor," *IEEE Access*, vol. 12, pp. 9860–9870, 2024, doi: 10.1109/ACCESS.2024.3353050