scientific reports

Check for updates

OPEN

A big data driven multilevel deep learning framework for predicting terrorist attacks

Ume Kalsooma[1], Sahar Arshad[1], Amerah Albarah[2]✉, Imran Siddiqi[1], Saeed Ullah[3], Abdul Mateen[3] & Farhan Amin[4]✉

In recent years, terrorism has increasingly threatened human security, causing violence, fear, and damage to both the general public and specific targets. These attacks create unrest among individuals and within society. Leveraging the recent advancements in deep machine learning, several intelligent systems have been developed to predict terrorist attacks. However, existing state-of-the-art models are limited, lack support for big data, suffer from accuracy issues, and require extensive modifications. Therefore, to fill this gap, herein, we propose an integrated Big Data deep learning-based predictive model to predict the probability of a terrorist attack. We treat the series of terrorist activities as a sequence modeling problem and propose a big data long short-term memory network. It is a layered model capable of processing large-scale data. Our proposed model can learn from past events and forecast future attacks. The proposed model predicts the likely location of future attacks at the city, country, and regional levels. The experimental study of the proposed model was carried out on the samples in the global terrorism dataset, and promising results are reported on a number of standard evaluation metrics, accuracy, precision, Recall, and F1 score. The obtained results suggest that the proposed model contributes substantially to predicting the probability of an attack at a particular location. The identification of potential locations of an attack allows law enforcement agencies to take suitable preventative measures to combat terrorism effectively.

Keywords Big data, Deep learning, Machine learning

In recent decades, terrorist attacks have continuously struck the global economy and political order. It has become a global menace and is a growing threat to the world today. Formally, the term "Terrorism" refers to the illegal use of power by a non-state actor to cause violence and terror among people, resulting in damage to human lives and properties[1]. In most cases, the objective of terrorist activities is to attain some religious, social, or political goals by attacking innocent people. Terrorism causes unrest and fear among both individuals and the general population[2]. It also causes agitation in society, inhibiting normal life, and also affects the economy of the region being attacked[3]. Unfortunately, technological advancements have also enabled the emergence of new and more sophisticated methods of terrorism[4].

A number of countries around the globe have faced terrorism in some form and, it has become a major challenge for the states and their law enforcement agencies. Statistics show that the number of terrorist attacks has significantly increased after the 9/11 incident and the most affected regions include the Middle East, North Africa, Sub-Saharan Africa, and South Asia[5]. Timely identification of potential attacks and the respective preventive measures are imperative to avoid the incident or, at least, minimize the damage caused by such attacks to individuals and properties. A major challenge in predicting these attacks, their targets, and the groups responsible for such attacks, is the lack of comprehensive historical data[6]. The patterns in terrorist attacks can help in identifying and analysing future terrorist activities and hence efforts can be made to prevent those[7]. Furthermore, well-planned activities and the presence of a number of active terrorist groups make it difficult to identify the attack patterns and forecast the time or location of an attack[8].

The common limitation is the lack of modeling complex spatiotemporal dependencies. These are crucial for accurate location forecasting. For example, studies such as [6], [9], and [10] primarily rely on handcrafted features and

[1]Center of Excellence in Artificial Intelligence & Department of Computer Science, Bahria University, Islamabad, Pakistan. [2]Department of Information Systems, College of Computer and Information Science, King Saud University, Riyadh 11543, Saudi Arabia. [3]Department of Computer Science, FUUAST, Islamabad, Pakistan. [4]School of Computer Science and Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea. ✉email: aalobrah@ksu.edu.sa; farhanamin10@hotmail.com

conventional classifiers without utilizing temporal trends or geographical correlations. In contrast, our proposed model solves these issues by:

- Treating terrorism forecasting as a sequence modeling task using LSTM networks and thus well-suited for learning from historical patterns.
- Incorporating a convolutional layer to extract abstract features before feeding into the recurrent layer, Thus enhances the model's capacity to learn from complex inputs.
- Predicting not only the target region but also the city and country. Thus it enables a more scalable and multi-resolution forecast of possible attack locations.

Briefly, our work proposes a descriptive classification and offers a unified deep-learning architecture for fine-grained and time-aware prediction of terrorist attack hotspots.

Our proposed sequence model is used to predict the location (in terms of city, country, and region) of an attack based on historical terrorism data. For this research, We consider the terrorist activities after the year 2001 as the past studies [11] show that the terrorist incidents from 2002 to 2016 grew by 1,029%. Identifying the possible location of the next attack can facilitate the security forces and law enforcement agencies to take preventive measures beforehand to avoid or, at the least, minimize the impact of an incident.

Inspired by the recent mining attempts[12,13] on the Global Terrorism Data, our research study aims to employ the deep learning and artificial intelligence techniques to design a big data predictive model that can forecast the location of a terrorist attack, based on large data. The proposed modeling relies on the Global Terrorism Database (GTD), an open-access database. Leveraging the recent advancements in deep machine learning, intelligent systems have been developed for medical diagnosis, sentiment analysis, social network analysis, market predictions, transportation systems . We aim to explore the potential of deep learning solutions in predicting the location of terrorist attacks. More specifically, we treat the series of terrorist activities as a sequence modeling problem and employ a long short-term memory network to learn and subsequently forecast the location of the terrorist attack. The key highlights of our research study include the following:

- Herein, we propose an integrated big data multilevel deep learning model for the prediction of terrorist attacks.
- It is a layered model. The first step is Data prepossessing. The second step is data partitioning. The proposed Big Data deep learning algorithm was applied and finally, the terrorists were identified.
- The proposed approach is a bidirectional LSTM model to predict the possible location of an attack in a city, country, and region.
- The experimental study of the system was carried out on the samples in the global terrorism dataset and promising results are reported on a number of standard evaluation metrics. The obtained results suggest that deep learning models can contribute substantially to predicting the probability of an attack at a particular location.

We organize the contents of this paper in the following sections. Section 2 discusses the relevant existing techniques on the subject and similar problems. We next introduce the dataset employed in our study and the proposed methods in Section 3. Section 4 presents the details of our experimental study, the results obtained, and the accompanying discussion. At the end, we conclude the paper with a summary of key findings and outline interesting research directions for future work on this subject.

Related work

Predictive analytics on terrorism-related activities has been investigated with different objectives in the literature. These mainly include identifying the terrorist group responsible for an event, predicting the target and success of an attack, and identifying the location (region) of an attack. We discuss the existing work on each of these in the following sections.

Predicting the impact and target of attack

Among well-known techniques in this category,[2] proposed a model to predict the targets of terrorist attacks along with the weapon(s) used. Random forest was applied on the records in the GTD and accuracy values of 79%, 86%, and 34% are reported for attack type, weapon type, and target type respectively. In[9] a comprehensive analysis of records was carried out using the GTD with the objective to identify the elements that cause an increase in terrorist activities. The dataset was analyzed using different data mining and machine learning techniques including random forest and support vector machine to predict the success of an attack. Likewise, multinomial naïve Bayes and logistic regression were used to predict casualties and the group responsible for an attack. Ensemble learning was employed by[10] to predict the future attack, weapons used in an attack, and the target of an attack.

In [14], the authors proposed a fuzzy rule interpolation system that learns from the experience to make predictions. A bi-directional fuzzy interpolation rule was used to provide assistance for terrorism risk assessment (TRA) that predicts the likelihood of terrorist attacks with minimal dynamic information. The work by[3] aimed to identify the impact of terrorist attacks. Different attributes from GTD were used to identify the impact of an attack. K-means clustering was employed to scrutinize the attack impact and terrorist attacks causing the highest impact are identified. In another study,[15] predicted the success rate of a terrorist attack using different architectures of fully connected neural networks. The proposed model achieved a maximum accuracy of 91%. Likewise,[16] proposed a system that can trigger early warnings of terrorism incidents. The method, referred to by

the authors as the RP-GA-XGBoost algorithm, employed random forest and principal component analysis and has a reported accuracy of 86.33% on GTD.

Predicting the group responsible for an attack

Identifying the terrorist group responsible for an attack has also been investigated in several studies. For instance, [13] proposed a predictive model to identify the perpetrators of terrorist attacks. Random forest, decision tree, and logistic regression were applied to predict the terrorist group as well as the frequency of attacks. In another study, an artificial neural network was employed to identify the group involved in an attack in different regions of Egypt from 1996 to 2017[17]. Likewise, [18] investigated multiple classification techniques including naïve Bayes, ID3, C4.5, nearest neighbor, and support vector machine on the GTD to identify the terrorist group responsible for an attack.

Among other research,[12] proposed a model that aimed to identify the responsible terrorist group and the likelihood of an attack's success using various data mining and machine learning techniques. Similarly,[19] trained several machine learning algorithms, including decision tree, gradient boosting, and random forests, to identify the perpetrators of terrorist attacks. Features like weapon type, target type, type of attack, location, and year of attack were used to identify the group involved in an attack. Experimental evaluation using the GTD demonstrated that the random forest classifier outperformed other models used in the study. Similar studies are carried out in[6] and[20] where the authors compared the performance of different classifiers in identifying the terrorist group. [21] employed the CLope algorithm to extract patterns of historical data from the GTD and predicted the group associated with an attack.

Predicting the region of attack

In addition to predicting the impact and nature of attacks, several studies focused on predictive modeling to identify the geographical region of an attack. Among these studies,[22] proposed a predictive model to identify the region and type of an attack using classifiers such as naïve bayes, artificial neural network, support vector machine, random forest, and J48. A comparative analysis of these methods revealed that random forest outperformed other models. Ensemble learning with nearest neighbor and support vector machine was employed by[23] to predict the continent most susceptible to terrorist attacks. Feature selection was carried out using information gain and Chi-square as well as a combination of the two. A hybrid feature selection reported an accuracy of 97.81% in predicting the danger zones. The study in[24] proposed a real-time terrorist incident data collection system designed to gather all terrorist-related incidents as they occur. A risk projection model was developed using frequency and time factors to predict terrorist attacks. The experimental results showed that the model could successfully predict incidents occurring within a 1.5-mile radius in the subsequent 24 hours. The predictive model in[25] exploited several machine learning algorithms to identify future attacks in terms of target city, attack type, and weapon type. In another work targeting the prediction of the location of an attack, a spatial-temporal recurrent neural network is employed in[26]. Two different datasets, GTD and Gowalla, are employed in the study and promising results are reported in predicting the next possible location of a terrorist attack. A predictive model with decision trees and random forest was employed in[27] to identify the type and location of an attack.[1] carried out a comparative study of conventional machine learning algorithms (logistic regression, support vector machine, naïve Bayes) and deep neural networks. Experiments on the prediction of the type and region of an attack, along with the type of weapon, showed that the deep neural network outperformed the conventional learning methods with an overall accuracy of more than 95.

The authors in[28] present a new approach for the feature section in intrusion detection systems. This approach combines the Cuttlefish Algorithm with a Multilayer Perceptron (MLP) neural network for feature selection in intrusion detection systems (IDS). This approach aims to enhance the detection accuracy and efficiency by reducing the data dimensionality while retaining critical information. The proposed method is evaluated using the KDD Cup 99 dataset, and its performance is compared with existing state-of-the-art feature selection techniques, demonstrating superior classification accuracy. The proposed method offers a promising solution for improving IDS performance by effectively selecting relevant features from high-dimensional datasets[28]. This research investigates the impact of data discretization on the performance of the Naïve Bayes classifier using the KDD Cup 99 dataset. Another research is conducted in[29]. Herein, the authors explore three discretization methods–entropy-based, frequency-based, and frequency square root-based–and evaluate their effectiveness in enhancing classifier performance. The study demonstrates that discretization improves the classifier's accuracy, precision, and recall when compared to using continuous data. Among the methods tested, the entropy-based discretization technique yielded the highest performance across all evaluation metrics. Additionally, discretization reduced the model training time, making it a more efficient approach for large datasets with continuous attributes. The findings suggest that discretization is a valuable preprocessing step for enhancing the effectiveness of the Naïve Bayes algorithm, particularly in handling complex datasets like the KDD Cup.

An overview of notable techniques for predictive modeling of terrorist attacks is presented in Table 1. Common target variables in these studies include the prediction of attack success, target type, responsible terrorist groups, weapons used, and the geographical location of attacks. While a wide range of machine learning techniques have been applied to terrorism prediction, ranging from decision trees and random forests to support vector machines and clustering-based approaches, many of these studies are limited in scope and design. Most existing models treat each terrorist incident in isolation, without accounting for the temporal or sequential nature of events. Furthermore, the use of static features often fails to capture evolving attack patterns over time and across geographic regions. The common limitation is the lack of modeling complex spatio-temporal dependencies. These are crucial for accurate location forecasting. For example, studies such as [6], [9], and [10] primarily rely on handcrafted features and conventional classifiers without utilizing temporal trends or geographical correlations. In contrast, our proposed model solves these issues by using

Predicting the impact and target of attack			
Study	**Dataset**	**Method**	**Remarks**
[14]	Hypothetical data	Fuzzy rule based classification	Terrorist risk assessment is proposed. Dynamic and adaptive fuzzy rule interpolation can be used to improve the reasoning system.
[10]	GTD	Ensemble approach using Random Forest	Future attack, weapons and the target of attack are investigated.
[2]	GTD	Random Forest	Attack, Weapon and Target accuracy values of 79%, 86% & 34% respectively.
[9]	GTD	SVM and Random Forest	Predict the success, casualties, and the group responsible for an attack. Comparative analysis to learn the patterns of attack and clustering algorithms to identify new features.
[3]	GTD	K-means clustering	The impact and hazard level of terrorist attack, that can assist to predict hidden as well as emerging terrorist organizations.
[15]	GTD	Fully connected neural network	Forecasts the success of an attack with an accuracy of 91.17%.
[16]	GTD and Database of terrorist attacks in China	Novel approach named RP-GA-XGBoost	Reports an accuracy of 86.33%.
Predicting the Terrorist Group Responsible for an Attack			
[6]	GTD	Naïve Bayes, ID3, KNN and Decision Tree	Predicts the terrorist group responsible for the attack with an accuracy of 96.4%.
[21]	GTD	Clope Algorithm	Predicts the terrorist group responsible for an attack.
[18]	GTD	Naïve Bayes, KNN, Tree Induction (C4.5), ID3, and Support Vector Machine	SVM reports the highest accuracy of 67%.
[13]	GTD	Random Forest, Decision Tree, and Logistic Regression	Identifies the perpetrator of an attack and the frequency of attacks.
[17]	GTD	Artificial Neural Network	Predicts attacks on different countries using embedded feature selection method with an accuracy of 74.7%.
[12]	GTD	K-nearest neighbor, Random Forest and Naïve Bayes	RF outperforms the other two models with an accuracy of 91.62%.
[19]	GTD	Decision Tree, Gradient Boosting and Random Forest	RF outperforms the other models with an accuracy of 84%.
Predicting the Region of Attack			
[24]	Real-time data	Risk Projection Model	Predicts terrorist attack that may occur in the next 24 hrs with a precision of 96.3%.
[26]	GTD and Gowalla Dataset	Spatio-Temporal Recurrent Neural Network	Predicts the next location of an attack.
[25]	GTD	Multiple classification algorithms	Predicts target city, weapon type, target type and attack type.
[22]	GTD	SVM, ANN, Naïve Bayes, Random Forest, Rep tree and J48	Predicts attack type, attack region and weapon type.
[20]	GTD	K-Nearest Neighbour, Logistic Regression and SVM	Predicts region of an attack and future attacks. SVM outperforms other models.
[1]	GTD	SVM, Logistic Regression, Naïve Bayes and Deep Neural Network	Deep Neural Network outperforms conventional methods with an accuracy of 95%.
[27]	GTD	Decision Tree and Random Forest	Predicts the attack type and the area of an attack.
[23]	GTD	SVM, K-Nearest Neighbour	Ensemble learning with feature selection using a hybrid of Chi-Square and information gain - Accuracy of 97.81%.

Table 1. Comparative Analysis of Literature.

- Treating terrorism forecasting as a sequence modeling task using LSTM networks, which are well-suited for learning from historical patterns.
- Incorporating a convolutional layer to extract abstract features before feeding into the recurrent layer, which enhances the model's capacity to learn from complex inputs.
- Predicting not only the target region but also the city and country, enabling a more scalable and multi-resolution forecast of possible attack locations.

Thus, our work proposes a descriptive classification and offers a unified deep-learning architecture for fine-grained and time-aware prediction of terrorist attack hotspots.

In this research, we propose a sequence modeling to predict the location (in terms of city, country, and region) of an attack based on historical terrorism data. We consider the terrorist activities after the year 2001 as the past studies [11] show that the terrorist incidents from 2002 to 2016 grew by 1,029%. Identifying the possible location of the next attack can facilitate the security forces and law enforcement agencies to take preventive measures beforehand to avoid or, at the least, minimize the impact of an incident.

Critical analysis of existing methods and identified gaps

While the existing body of literature provides a solid foundation for predictive modeling of terrorism-related activities, a closer inspection reveals several recurring limitations that constrain the effectiveness and scalability of these methods. In this section, we critically evaluate the shortcomings of prior work and clarify how our proposed approach specifically addresses these challenges. 1. Lack of Temporal Modeling: A significant portion of earlier studies treats each terrorist incident as an independent observation. Methods such as decision trees, random forests, and support vector machines are often applied on static datasets without capturing the sequence or temporal dependencies between events. This overlooks the natural progression and temporal clustering of attacks, which can carry important predictive signals. For instance, the models proposed in [6,11,12] rely on flat feature vectors, lacking any sequential or historical context. Our contribution explicitly frames the prediction

task as a sequence modeling problem, using long short-term memory (LSTM) networks to learn patterns from chronological event sequences, thus incorporating temporal dynamics directly into the forecasting process. 2. Limited Spatial Resolution Most prior studies focus on predicting the region of an attack–an approach that offers limited actionable insights for law enforcement. Works such as[1,22] report high accuracy, but only at the regional level, which is too coarse for real-time tactical planning. Our model addresses this gap by performing predictions at three levels of geographic granularity: city, country, and region. This multilevel approach enables both strategic and tactical decision-making based on the forecast output. 3. Overreliance on Handcrafted Features Several traditional machine learning approaches in the literature rely heavily on handcrafted features, which may not fully capture the underlying complexity of terrorism patterns. These include static attributes like attack type, target type, and weapon used. Such features can be insufficient in modeling nonlinear, spatio-temporal dependencies that evolve over time. Our approach introduces a 1D convolutional layer prior to the LSTM to extract high-level features from raw sequential input data, thereby enabling the model to learn complex feature representations automatically without manual intervention. 4. Inadequate Generalization and Scalability Many existing models do not scale well with large datasets or fail to generalize across different geographic regions due to class imbalance and overfitting to frequently occurring patterns. Moreover, limited use of regularization and shallow architectures often results in overfitting to specific contexts. In our work, we tackle scalability by using a shallow but expressive architecture, regularized through dropout and batch normalization, and we evaluate the model on a large and diverse dataset (GTD) spanning nearly two decades. This helps ensure both generalization and robustness.

Proposed model

Predicting the location of an attack before it occurs can play a vital role in its prevention[12]. This study proposes a predictive model to identify terrorist attack hotspots. These hotspots are identified at three different scales in terms of geographical spread i.e., city, country, and region. The proposed Model is illustrated in Fig. 1 with further details discussed in the following sections.

Dataset description

- In this research, we use the Global Terrorism Database, an open-source database containing detailed information on terrorist attacks around the world since 1970. The dataset contains information of more than 200,000 incidents. We first carry out a comprehensive analysis of the data to identify the attributes that can support decision-making and predictive modeling. The dataset contains heterogeneous attributes including spatio-temporal information, categorical features, numerical values, and binary features as outlined in the following and summarized in Table 2**Spatio-temporal** attributes include data with time and location information such as year, month, day, latitude, longitude, city, country, and region.
- **Categorical** features include attributes like country, city, region, attack type, target type, target nationality, weapon type, and group name, etc.
- **Numerical** attributes contain numerical values like number of individuals killed or wounded, etc.
- **Binary** attributes in the GTD contain a 0/1 value like political motive, intention to coerce, suicide attack, claimed attack, etc.

Data limitations and potential biases

Although the Global Terrorism Database (GTD) is one of the most comprehensive publicly available resources for terrorism-related data, it is not without limitations. First, reporting bias is a significant concern–terrorist incidents are more likely to be recorded in regions with better media coverage and institutional transparency. As a result, underreporting may occur in conflict zones or regions with limited press freedom, potentially skewing the data distribution across countries and regions. Second, the labeling of attacks, groups, and motivations is dependent on the interpretation of available sources, which may introduce subjectivity and inconsistency. There may also be a bias toward high-profile or large-scale incidents, while smaller or failed attacks might be excluded. These biases could affect our model's predictions by:

- Overrepresenting frequently reported regions or groups, causing the model to overpredict events in those areas.
- Undermining generalization to less-documented locations or attack types.

While our model aims to generalize across locations and timeframes, we acknowledge these limitations and suggest that future work incorporate data augmentation, additional datasets, or bias correction techniques to improve robustness and fairness in predictive modeling.

Data prepossessing

Effective data preprocessing is crucial for the performance of machine learning models, especially when handling heterogeneous and imbalanced datasets such as the Global Terrorism Database (GTD). Our preprocessing framework consists of data cleaning, transformation, and normalization steps, aligned with established practices in the literature. The preprocessing pipeline includes three key stages: data cleaning, data transformation, and normalization, which are crucial for effective predictive modeling[28] and[29].

- **Data Cleaning:** As a first step in data cleaning, all the attributes having repeated values, once in numerical form and once in textual form, are kept only once. The attributes containing redundant values include country, region, attack type, etc. Furthermore, many attributes also have missing values. We have removed the

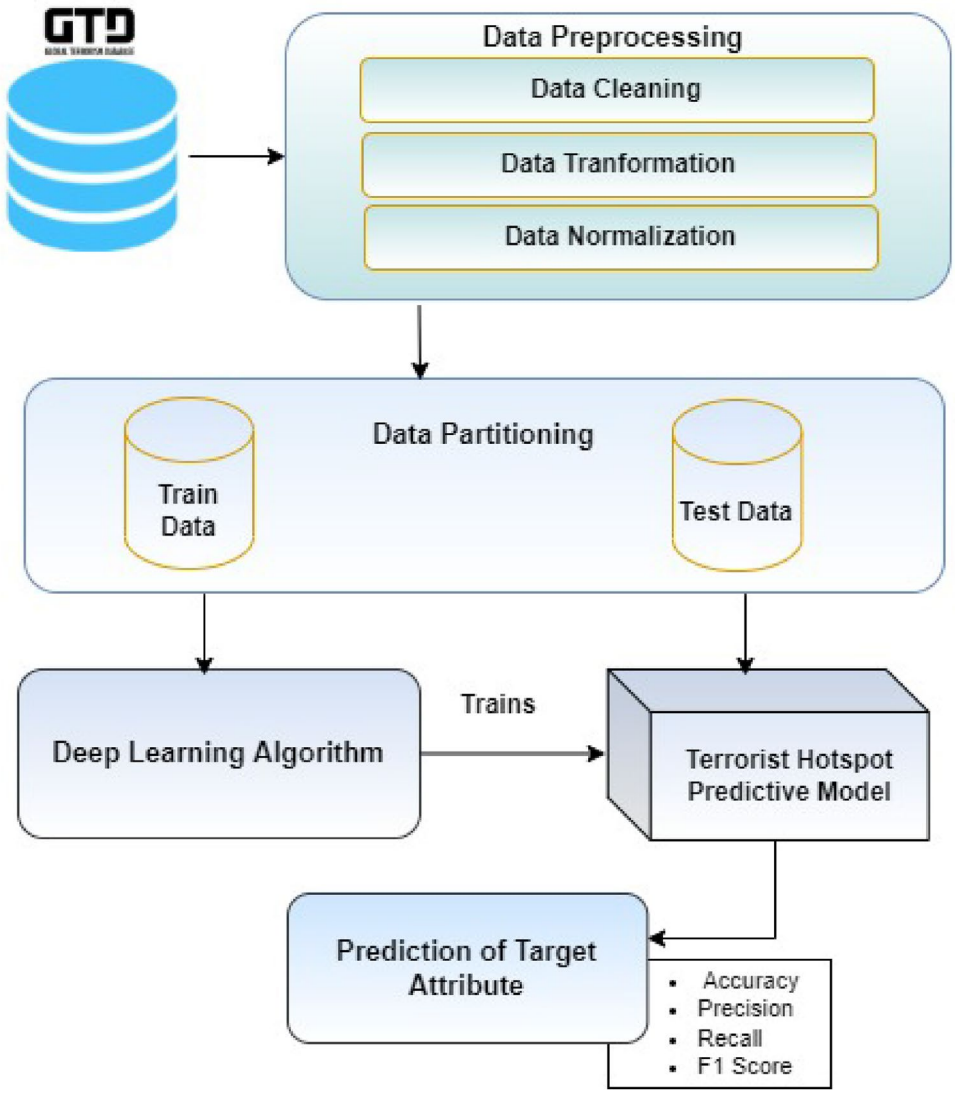


Fig. 1. Proposed model.

Spatio-temporal	Categorical	Numerical	Binary
Year	Attack type	No. of people killed	Extended for 24 hrs
Month	Target type	No. of people wounded	Vicinity of city
Day	Target nationality	Specificity	Political motive
Latitude	Group name	No. of people wounded	Intention to coerce
Longitude	Weapon type	No. of people killed	Non-combatant targets
City		No. of perpetrators wounded	Doubtterr
Country			Multiple
Region			Success
Provstate			Suicide
			Claimed
			Property
			IsHostKid

Table 2. Types of Attributes in the Global Terrorism Database.

attributes with missing values in such a way that those attributes which have less than 20 percent of missing values and are not contained in another attribute are selected while others containing more than 20 percent of missing values are discarded. Missing values in categorical textual attributes are replaced with 'Unknown' and the numerical attributes containing missing values are treated as 'NaN'. We addressed redundancy by removing duplicate attributes and handled missing values by excluding features with more than 20 To enhance data quality, redundant attributes were removed, and features with more than 20

- **Data Transformation:** As discussed previously, the attributes in the GTD contain numerical as well as textual data. In our study, we target a (statistical) machine learning-based predictive model that requires numerical data as input. Consequently, categorical attributes such as region, country, city, group name, attack type, weapon type, and target, which are textual in nature, are converted into numerical representations prior to further processing. Label encoding is employed for this purpose that maps each attribute to the corresponding numerical label. Categorical variables such as region, country, city, group name, attack type, weapon type, and target were converted to numerical form using label encoding. This step facilitates the use of machine learning algorithms that require numerical inputs[1]. Additionally, discretization techniques, which segment continuous data into bins, have been shown to impact predictive accuracy positively and were considered in designing the transformation pipeline[2]. Most machine learning algorithms require numerical input; categorical features such as region, country, city, attack type, and weapon type were encoded numerically using label encoding. Discretization of continuous attributes is known to affect classifier performance, particularly for probabilistic models such as Naive Bayes. Garcia et al. showed that appropriate discretization can enhance prediction accuracy by reducing noise and simplifying the input space[2]. Although our model uses deep learning which can handle continuous inputs, understanding discretization's impact guided our preprocessing choices.
- **Data Normalization:** Data normalization refers to forcing all values within a pre-defined range and is known to accelerate the training of learning algorithms by ensuring speedy convergence (of gradient descent). In our case, once all data is in numerical form, we normalize all attributes in the range [0, 1]. To ensure all features contribute equally and to accelerate model training convergence, numerical features were normalized to a [0,1] range, a standard practice supported by prior studies[1]. These preprocessing steps align with best practices established in the literature for handling heterogeneous and imbalanced datasets in classification problems. To ensure consistent scaling across features and accelerate training convergence, numerical attributes were normalized to the [0,1] range, a standard technique supported by comprehensive reviews in the machine learning literature[3]. This preprocessing pipeline ensures high-quality, standardized input data that facilitates effective learning by the proposed deep learning model.

After pre-processing, we keep a total of 32 attributes for predictive modeling of the location of an attack. These attributes are summarized in Table 3 along with a descriptive explanation of each. The names of the attributes are kept the same as those in the GTD so that readers may establish correspondence between the two.

Exploratory data analysis

To gain deeper insights into the Global Terrorism Database, we conducted an exploratory data analysis using visualization techniques. The analysis focuses on the target attributes, specifically the city, country, and region associated with each attack. This analysis is conducted on the terrorist attacks after 9/11 i.e., from 2001 onward.

- **Most Affected Cities:** After preprocessing, the dataset contains 392 unique cities. As expected, the frequency of attacks varies significantly across different cities. The distribution of frequency of attacks as a function of city for the period 2001 to 2017 is summarized in Fig. 2 where it can be seen that Baghdad, Mogadishu, and Mosul emerged as the three most affected cities during this period.
- **Most Affected Countries:** Terrorism attacks have been reported in many countries around the globe. The pre-processed data in our case contains a total of 134 unique countries that have witnessed terrorism in some form. Figure 3 summarizes the Top-15 most affected countries during the period under study.
- **Most Affected Regions:** In addition to cities and countries, The GTD also categorizes attacks by geographic region. A total of 12 regions are listed in the GTD. These regions include Australasia and Oceania, East Asia, Central Asia, Eastern Europe, Central America and the Caribbean, Middle East and North Africa, South-East Asia, South Asia, North America, South America, Sub-Saharan Africa and Western Europe. The frequency of attacks as a function of these 12 regions (from 2001 to 2017) is summarized in Fig. 4.**Model Training** To address the substantial class imbalance across city, country, and region classes, a weighted categorical cross-entropy loss function was employed during model training. Class weights were calculated as the inverse of the class frequencies, ensuring that minority classes are penalized more heavily during training. This strategy helped improve prediction accuracy, especially for less frequent classes. Label encoding and normalization were also applied during data preprocessing to standardize input features."

Proposed model

In this section, we present the technical details of the predictive model that treats a sequence of events as time-series data. We apply time-series forecasting by analyzing historical data to predict future events[30]. Time-series predictions have been widely used in forecasting applications in finance, medicine, weather, renewable energy and so on[31]. Although hidden Markov models have been traditionally used for time-series modeling, recurrent neural networks (and their variants) have become the preferred approach in recent years. The recurrent connections enhance the capability of neural networks to accurately predict time series data, with more advanced architectures such as LSTM, proving to be more robust and reliable during training[32]. According to[33], while working with time series data, LSTM neurons have the best ability to remember prior values and, consequently, forecast trends. Therefore, in this study, we have employed long short-term memory (LSTM) networks to learn

S. No.	Attribute	Description
1	*iyear*	The year in which incident happened
2	*imonth*	The month in which incident took place
3	*idate*	Date of the month on which incident happened
4	*latitude*	The latitude of the location where the incident took place
5	*longitude*	The longitude of the location of incident
6	*extended*	Yes=1, or No=0, Whether the time of an incident extended to more than 24 hours or not
7	*provstate*	Name of the province or state where the incident happened
8	*specificity*	Identifies the geo-spatial resolution of the latitude and longitude fields
9	*politicalmotive*	Either the motive of attack is political or not
10	*intentiontocoerce*	Either there is an intention to coerce or not
11	$non-combatanttargets$	Whether the incident targets non-combatants
12	*vicinity*	Incident is in the immediate vicinity of the city or not
13	*doubtterr*	Whether there is a certainty that the attack is an act of terrorism or not
14	*nationality*	The nationality of the target
15	*multiple*	if the current incident is connected to some other incidents
16	*success*	The attack achieved its goals or not
17	*suicide*	Yes=1, or No=0, The attack is suicidal or not
18	*claimed*	Did any terrorist group claim the responsibility of an attack?
19	*property*	Any evidence of property damage from a terrorist attack
20	*ishostkid*	Whether the victims were taken hostage or kidnapped
21	*individual*	
22	*nkillus*	Number of confirmed kills
23	*nwound*	Total number of injuries including victims and perpetrators
24	*nwoundus*	Total number injuries including victims and perpetrators
25	*nwoundte*	
26	*city*	The city or town where an attack took place
27	$country\_txt$	The name of the country where the attack took place
28	$region\_txt$	The region of attack
29	$attacktype1\_txt$	The type and method of attack used by perpetrators
30	$targtype1\_txt$	The type of victim or target being attacked
31	$weapontype1\_txt$	The general weapon type used in the attack
32	*gname*	The terrorist group which is responsible for the attack

Table 3. Summary of attributes from the GTD employed in our study.

implicit patterns from the sequence of terrorist incidents and to predict the location-based target variables. LSTMs are enhanced recurrent neural networks that are capable of learning long-term dependencies in making predictions[34] and, are known to outperform the vanilla RNNs.

From the viewpoint of sequence modeling, the input in our case is a sequence of events while location (city, country, or region) represents the target variable, thus allowing the problem to be formulated as a many-to-one mapping. We first define a look-back period $n = 30$ which represents the number of incidents (in chronological order) used to predict the location of the next incident. In other words, to predict the target location of the incident at time $t + 1$, we employ a sequence of n events corresponding to time steps $t_0, t_{-1}, \ldots, t_{n-1}$. The input sequence length was set to 30, representing the most recent 30 terrorist incidents prior to the target prediction point. This value was empirically chosen based on preliminary experiments balancing performance and training efficiency. Smaller window sizes (e.g., 10 or 20) led to lower accuracy, as the model lacked sufficient temporal context, while longer sequences (e.g., 50 or more) showed diminishing returns and increased training complexity. Additionally, a 30-event window aligns with the intuition that recent historical activity within a temporal cluster is more predictive of future incidents, a pattern supported by prior studies in spatio-temporal event forecasting. The process of data sequencing is illustrated in Fig. 5 where a window of length n moves across the dataset and produces the input and output pairs for training the recurrent model(s). As an example, data instances from 1 to 30 make the 1st sequence set, while the location of the next event ($t = 31$) represents the target variable. Next, the incidents numbered 2 to 31 represent the 2nd input sequence, and so on. With a total of 19,538 instances in the (pre-processed) dataset, we produce 19,508 input-output (sequence-target) examples.

Once we have the input sequences and target variables, we train a bi-directional LSTM network to learn the implicit dependencies in the input and to predict the location of the next attack. The proposed CNN-BiLSTM model is particularly suited for terrorism forecasting due to its ability to capture both spatial dependencies and long-term temporal patterns in sequential incident data. The model employed comprises of 1D convolutional, LSTM, and output layers as summarized in the following:

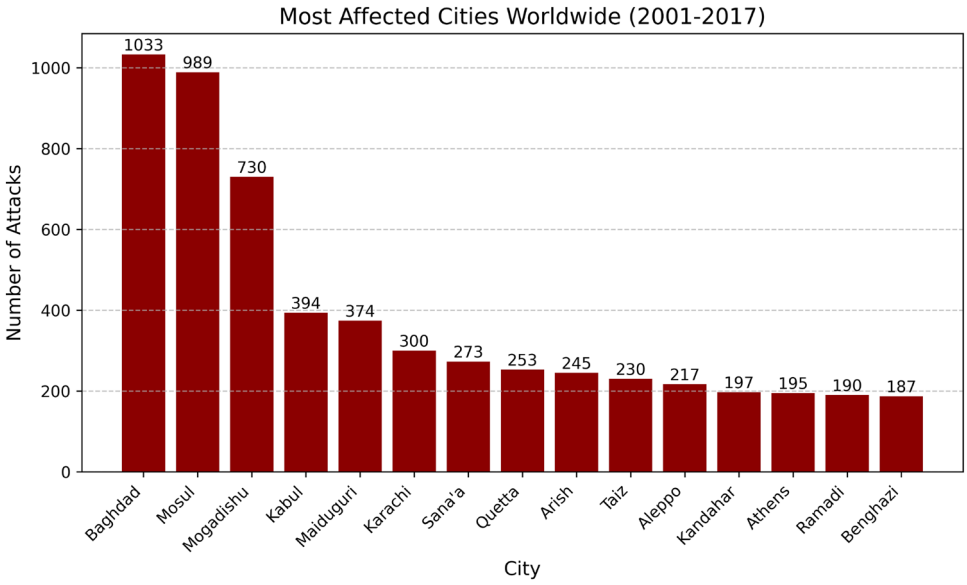


Fig. 2. Most affected cities in 2001–2017 period.

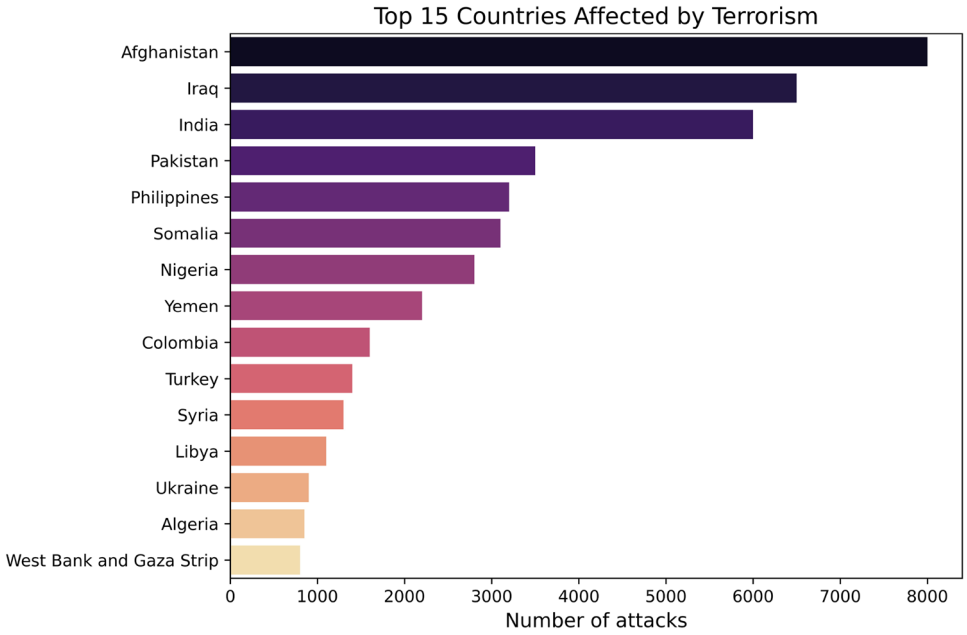


Fig. 3. Most affected countries in 2001–2017 period.

- **1D Convolutional Layer:** The convolutional layer extracts high-level feature representations from the raw input[35]. Instead of directly feeding raw feature sequences to the recurrent layers, a 1D convolutional layer is introduced to enhance feature extraction. A total of 64 1D filters are employed, followed by the ReLU activation function.
- **Bi-directional LSTM Layers:** The convolutional layer is followed by two bi-directional LSTM layers, each with 64 hidden units. Bi-directional layers traverse input sequences in both forward and backward directions, enabling the model to better learn dependencies across the sequence.
- **Fully-Connected Layer:** LSTM layers are followed by a fully connected layer to predict the target variable. The number of neurons in this layer corresponds to the number of unique output class labels based on the target variable (city, country, or region).

Initial hyperparameter values, such as sequence length, number of LSTM units, dropout rate, batch size, and learning rate, were chosen based on an ablation study (see Section ??), to provide the best trade-off between model accuracy and computational efficiency. The overall architecture of the network employed in our study is

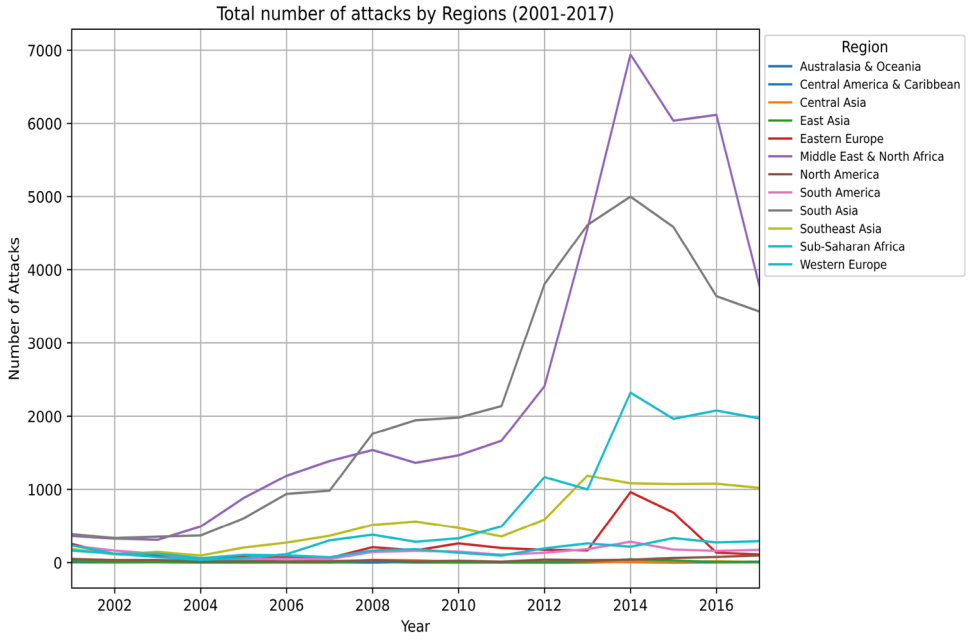


Fig. 4. Frequency of attacks as a function of region.

Event ID	Year	Month	Day	Latitude	.	.	.	Country	Group name
1	2001	1	1	3.800889	.	.	.	Columbia	Paramilitaries
2	2001	1	1	4.5981				Columbia	United Self Defense Units
.	2001	1	1	34.666667				Algeria	Algerian Islamic Extremists
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
30	2001	1	7	25.846914				India	United People's Democratic Solidarity (UPDS)
31	2001	1	9	43.141187				Russia	Chechen Rebels
32	2001	1	9	43.280364				Spain	Basque Fatherland and Freedom (ETA)

Sequence 1 Sequence 2 Sequence 3

Fig. 5. Data Sequencing for model training.

shown in Fig. 6 (where *n* represents the length of a sequence) while Table 4 lists the dimensions of the input/output volumes and number of parameters in each layer. To accelerate training and prevent overfitting, a batch normalization layer follows the 1D convolutional layer, along with two dropout layers using a rate of 0.2. The model is trained for 50 epochs with a batch size of 64 using categorical cross-entropy loss and an 'Adam' optimizer.

Model complexity and scalability analysis

In this section, we perform mathematical modeling. In order, to understand the behavior of our proposed model. at first; Table 4 provides the number of trainable parameters for each layer. A comprehensive evaluation of model scalability requires analyzing computational complexity.The two bi-directional LSTM layers each contain 64 hidden units and process input sequences of length 30 with an input dimension of 64 (from the convolutional

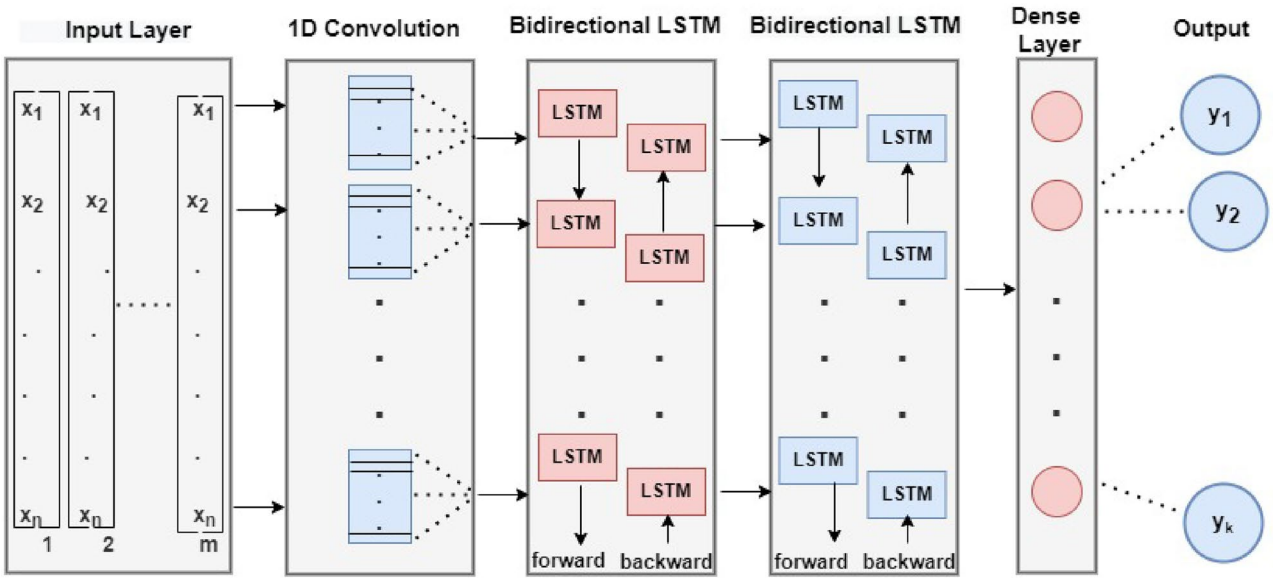


Fig. 6. Architecture of the proposed model.

Layer Type	Output Shape	Parameters	Time Complexity	Space Complexity
Conv1D	(None, 15, 64)	6,016	$O(n(dh+h^2))$	$O(dh+h^2)$
Batch Normalization	(None, 15, 64)	256	$O(n)$	$O(d)$
Dropout	(None, 15, 64)	0	$O(n)$	$O(d)$
Bi-directional LSTM	(None, 15, 128)	66,048	$O(n(dh+h^2))$	$O(dh+h^2+nh)$
Dropout	(None, 15, 128)	0	$O(n)$	$O(d)$
Bi-directional LSTM	(None, 128)	99,816	$O(n(dh+h^2))$	$O(dh+h^2+nh)$
Dropout	(None, 128)	0	$O(n)$	$O(d)$
Dense	(None, 392/134/12)	50,568/17,286/1,548	$O(dh)$	$O(dh)$

Table 4. Layer-wise volumes, parameters, and computational complexities of the employed model.

layer output). The time complexity of each BiLSTM layer is approximately O(T×H×(D+H)) where T=30 is the sequence length and H=64, he number of hidden units, and D=64, the input feature dimension. The proposed BiLSTM process sequences in both forward and backward directions. This involves computing the hidden states for each time step in two LSTM networks, which significantly contributes to the model's computational cost. For each time step, the BiLSTM performs operations based on the supported parameters mentioned in Table 4. The time complexity for processing a sequence of data is

$$O(n(dh+h^2))$$

Where: - n is the sequence length (the number of time steps in the input sequence), - d is the input size, - h is the hidden state size. The term $O(dh)$ accounts for the linear transformation between the input and the hidden state, and h^2 reflects the recurrent connections within LSTM.For the BiLSTM layer, which processes the sequence in both directions (forward and backward), the time complexity is doubled, yielding:

$$O(2+(dh+(h^2))=O(dh+(h^2)$$

Thus, for the entire sequence of length, the total time complexity is

$$O(dh+(h^2)$$

In terms of space complexity, we need to consider both the model parameters and the intermediate states (hidden states) that are computed during both training and inference. Based on the BiLSTM layer, sets of parameters. The total number of parameters for one BiLSTM layer is

$$O(dh + (h^2) + h) = O(dh + (h^2)$$

For the BiLSTM layer (which has two directional LSTMs), the total parameter count is

$$O(2 * dh + (h^2 + h) = Odh + h^2)$$

The total space complexity of the BiLSTM layer is the sum of the parameters, and the intermediate states are given below.

$$O(dh + (h^2)) + nh)$$

Experiments and results

In this section, we have conducted experiments to evaluate the effectiveness of the proposed approach. The 19,508 samples, including input sequences (of length 30) and target location, are split into disjoint training and test sets using the standard 70-30 split. Additionally, 10%

Predicting the city, country, and region of attack

The first series of experiments is carried out to predict the city of the next attack by exploiting the spatio-temporal data in the GTD. To have meaningful inferences, we have selected only those cities that have at least 10 instances in the dataset i.e., the cities in which at least 10 incidents are being reported. Sequence modeling is carried out using bi-directional RNNs, LSTMs, and GRUs, and the corresponding accuracy and loss graphs (during model training with LSTMs) for training and validation datasets are presented in Fig. 7a. On test data, the accuracy values of 67.24%, 77.21%, and 77.33% respectively are achieved for the three models. The values of other metrics are listed in Table 5 where it can be seen that for all metrics, LSTMs and GRUs report comparable results, outperforming the vanilla RNNs. Although our comparison emphasizes accuracy, the proposed model is computationally efficient due to its shallow architecture. It can be trained and deployed on modest hardware, offering scalability potential for large-scale or near-real-time applications.

The next series of experiments is carried out using the same settings but changing the target variable to the country of the next attack. For these experiments, the evolution of accuracy and loss as a function of the number of training epochs (with LSTMs) is presented in Figure 7b while accuracy values of 96.52%, 96.18%, and 97.10% are reported by RNNs, GRUs, and LSTMs respectively. In comparison to the target city, naturally, the results are much more enhanced when predicting the target country. Likewise, when the target variable is changed to the region of attack, high accuracy values of more than 99% are reported by each of the three models. The models also converge relatively quickly in these experiments Fig. 7c). Figure 8 shows an analysis of the obtained results. Herein, it shows the complexity. The most challenging among the three target variables is predicting the city of the next attack. The combination of 1D convolutions with bi-directional LSTMs reports an accuracy of more than 77% on this challenging scenario validating the effectiveness of the proposed modeling scheme in predicting the location of the next attack using past data. For country and region, accuracy values of 97.10% and 99.82%

Ablation studies

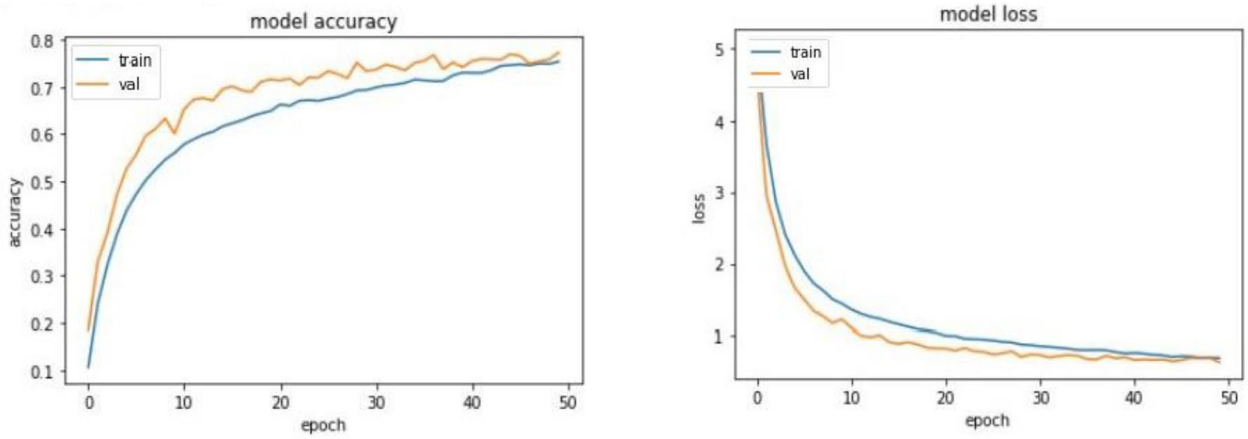
In an attempt to study the evolution of prediction performance as a function of different hyperparameters in the system, we carried out additional experiments. These experiments include all three models and employ the *city* as the target variable. In the first experiment, we study the impact of changing the number of hidden units in the sequence modeling layer (RNN, GRU, or LSTM). The number of hidden units is progressively increased from 32 to 372, and the respective accuracy values for the three models are summarized in Fig. 9a. It can be observed that all three models exhibit more or less similar trends, reporting the highest accuracy values with 64 hidden units. Similarly, we also vary the number of hidden layers in the convolutional as well as the recurrent part of the model. It is observed that in both cases, shallower networks outperform their deeper counterparts. For the recursive layers, the performance starts to drop beyond two hidden layers (Fig. 9b). Likewise, a similar (though less sensitive) trend is observed for the 1D convolutional layers, where a single conv layer reports the highest accuracy values (Fig. 9c).

Finally, we also provide a performance comparison (Table 6) of our method with existing techniques reported in the literature and targeting the prediction of the location of an attack using the GTD dataset. While we consider the identification of location in terms of city, country, and region, most of the studies employ only region as the target variable. It can be seen from the table that the proposed sequence modeling technique reports the highest recognition rate of 99.82% (target variable: region). Furthermore, for more challenging target variables, country and city, our method also reports promising accuracy values of 77.33% and 97.10% respectively, validating the ideas put forward in this study.

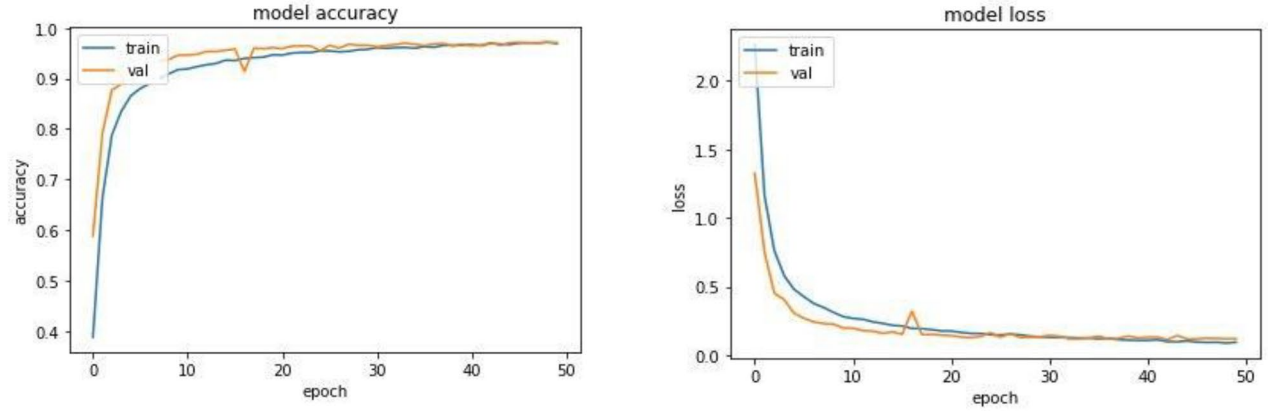
Convergence and sensitivity analysis

In this section, we discuss the convergence and the sensitivity analysis of our proposed model. The details are given below.

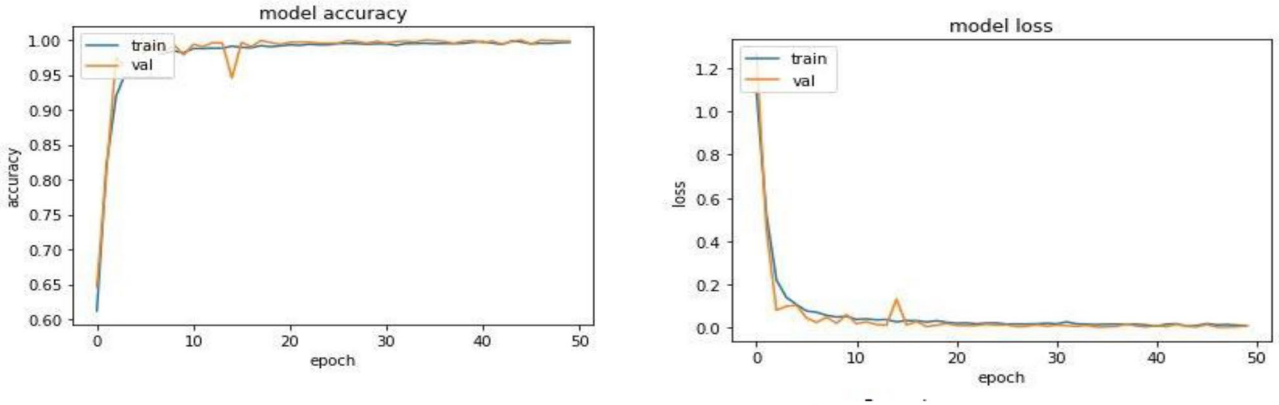
Figure 10 shows the variation in accuracy with different hyperparameter settings. To validate our proposed model. We perform a detailed analysis of learning curves (training and validation loss) with the aim of providing further insights into training dynamics. In this figure, a reader can see the learning curves for training and validation accuracy over 20 epochs. This figure illustrates the progression of accuracy during training and the evolution of the model's performance on the validation set. The training accuracy increases, while the validation



a. Model Accuracy and Loss for City



b. Model Accuracy and Loss for Country



c. Model Accuracy and Loss for Region

Fig. 7. Evaluation of model accuracy and loss for target variables: (**a**) City (**b**) Country (**c**) Region.

accuracy also improves, but at a slightly slower rate, indicating generalization. The learning curves displayed in the graph show the progression of training and validation accuracy over 20 epochs. The training accuracy increases steadily fto providerom 60

Data limitations and bias

Data Limitations and Potential Biases Although the Global Terrorism Database (GTD) is one of the most comprehensive publicly available resources for terrorism-related data, it is not without limitations. First, reporting bias is a significant concern–terrorist incidents are more likely to be recorded in regions with better media coverage and institutional transparency. As a result, underreporting may occur in conflict zones or

	Model	Accuracy	Precision	Recall	F1 Score
City	Bidirectional RNN	67.24%	65.55%	68.43%	64.86%
	Bidirectional GRU	77.21%	72.32%	73.10%	70.33%
	Bidirectional LSTM	**77.33%**	**75.13%**	**76.45%**	**75.78%**
Country	Bidirectional RNN	96.52%	96.40%	96.50%	95.30%
	Bidirectional GRU	96.18%	96.10%	96.18%	95.91%
	Bidirectional LSTM	**97.10%**	**97.04%**	**97.12%**	**96.04%**
Region	Bidirectional RNN	99.32%	99.27%	99.32%	99.29%
	Bidirectional GRU	99.76%	99.01%	99.80%	99.38%
	Bidirectional LSTM	**99.82%**	**99.88%**	**99.84%**	**99.86%**

Table 5. Performance of different models in predicting the location (city, country, region) of the next attack.

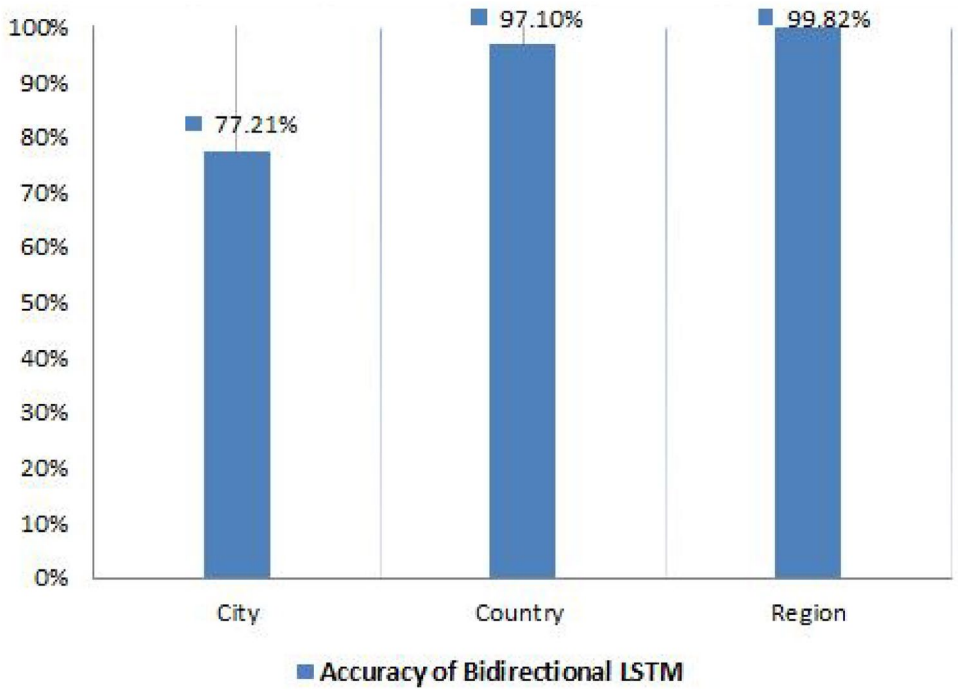


Fig. 8. Accuracy values (1D Conv+ BiLSTM) for the three target variables: city, country and region.

regions with limited press freedom, potentially skewing the data distribution across countries and regions. Second, the labeling of attacks, groups, and motivations is dependent on the interpretation of available sources, which may introduce subjectivity and inconsistency. There may also be a bias toward high-profile or large-scale incidents, while smaller or failed attacks might be excluded. These biases could affect our model's predictions by: – Overrepresenting frequently reported regions or groups, causing the model to overpredict events in those areas. – Undermining generalization to less-documented locations or attack types. While our model aims to generalize across locations and timeframes, we acknowledge these limitations and suggest that future work incorporate data augmentation, additional datasets, or bias correction techniques to improve robustness and fairness in predictive modeling.

Evaluation metrics for imbalanced data

Data Limitations: Given the inherent class imbalance in terrorism-related datasets–where the occurrence of attacks is relatively rare compared to non-events–it is crucial to employ evaluation metrics that go beyond overall accuracy. In addition to accuracy and F1-score, we report the Area Under the Receiver Operating Characteristic Curve (AUC-ROC), which measures the trade-off between true positive and false positive rates across different thresholds. A higher AUC indicates better model discrimination, particularly important for imbalanced classification. We also include Precision, Recall, and Precision-Recall (PR) curves, which are especially informative when the positive class (e.g., occurrence of an attack) is rare. These metrics emphasize the model's ability to correctly identify positive cases without being overwhelmed by the majority class.

The following metrics were used to assess model performance:

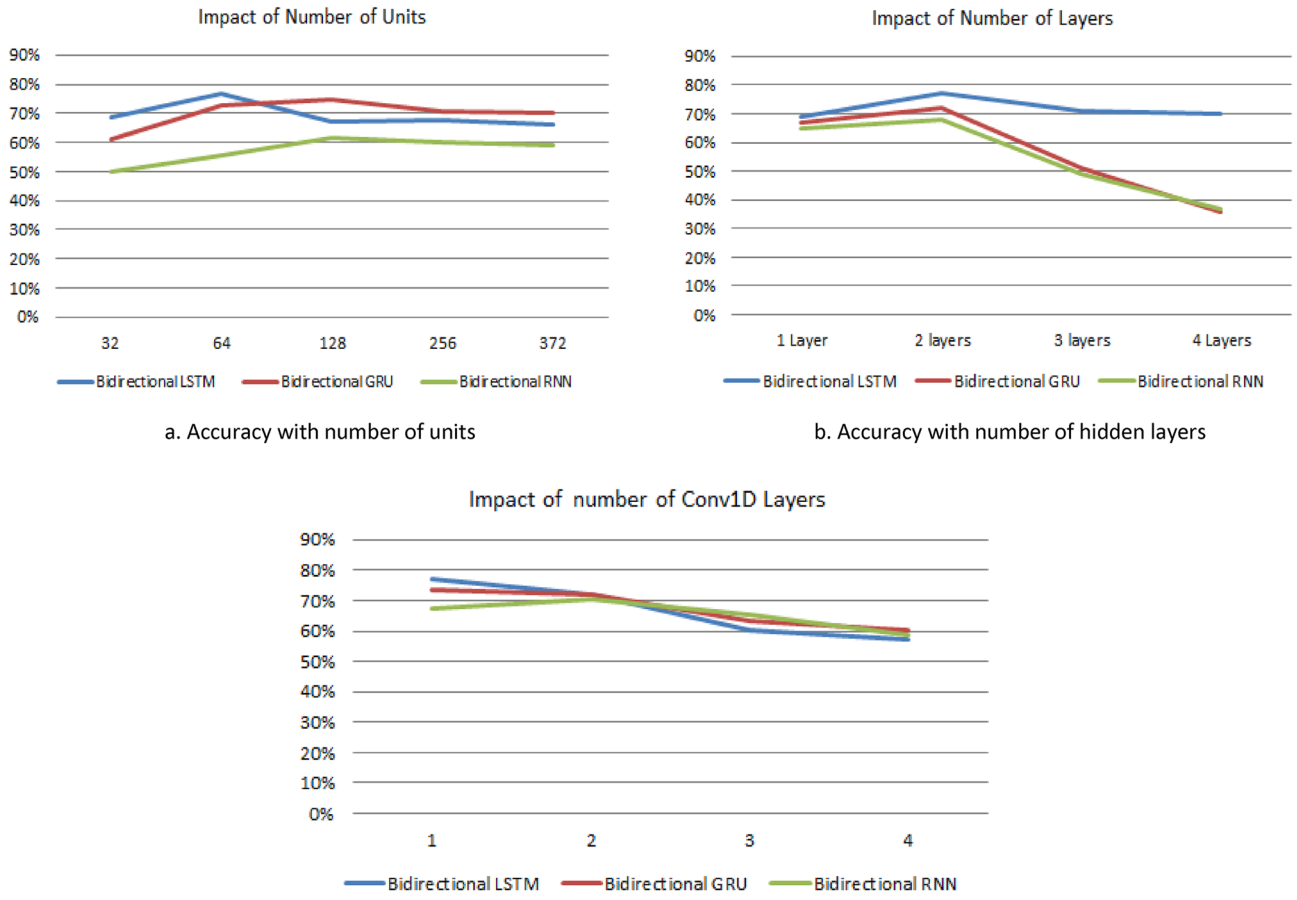


Fig. 9. The evolution of predictive performance for the target variable city as a function of different hyperparameters: (**a**) Number of hidden units in the LSTM (**b**) Number of recurrent layers (**c**) Number of convolutional layers.

Study	Method	Findings	Accuracy
Proposed Model	**Bi-directional LSTM**	**Region**	**99.82%**
		Country	**97.10%**
		City	**77.33%**
[23]	SVM, K-Nearest Neighbor	Region	97.81%
[1]	Deep Neural Network	Region	95%
[24]	Risk Projection Model	Region	96.3%
[17]	Artificial Neural Network	Country	74.7%
[26]	Spatio-Temporal RNN	Region	67.12%

Table 6. Comparison of our predictive model with state of art models.

- Accuracy: Overall correctness of predictions.
- Precision: Proportion of predicted positive cases that are actually positive.
- Recall (Sensitivity): Proportion of actual positive cases correctly identified.
- F1-Score: Harmonic mean of precision and recall.
- AUC-ROC: Measures the model's ability to distinguish between classes.
- AUC-PR: Especially informative under class imbalance.

These metrics collectively provide a more balanced and nuanced evaluation of the model's predictive performance. Where relevant, threshold selection can also be adjusted using ROC or PR analysis to prioritize recall or precision, depending on operational needs.

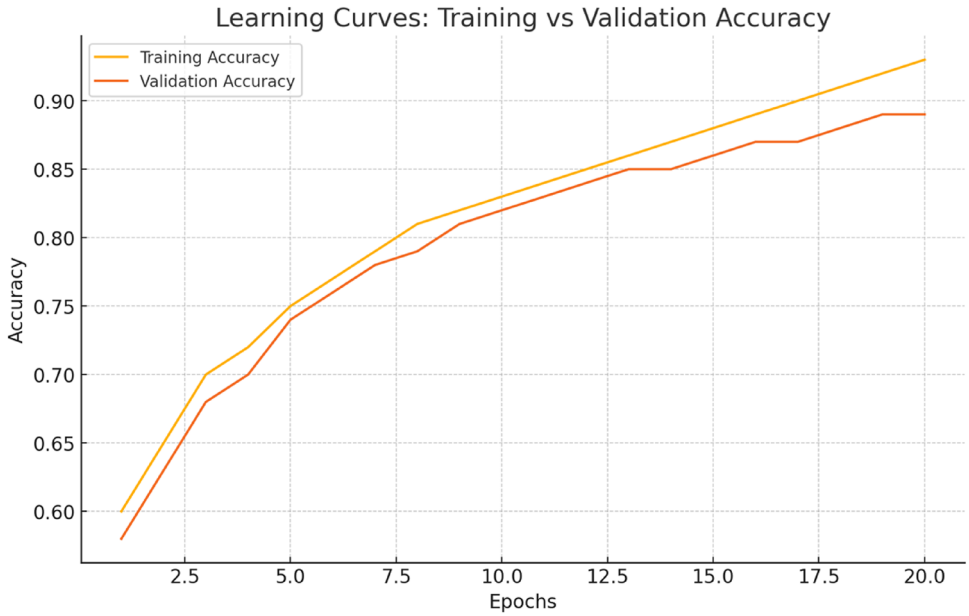


Fig. 10. Learning curves: training vs validation accuracy.

Model interpretability

Given the sensitive nature of terrorism prediction, it is critical not only to develop accurate models but also to ensure their predictions are interpretable and transparent. To better understand the internal decision-making of our model, we explored its behavior using post-hoc interpretability methods.

We applied SHAP (SHapley Additive Explanations) to estimate the contribution of each input feature (e.g., number of incidents, fatalities, attack types) toward the model's output. This allowed us to rank features by their importance and identify those most strongly associated with an increased likelihood of predicted attacks. For instance, spikes in coordinated attacks or fatality counts in recent days often had higher SHAP values, indicating a strong influence on the model's predictions. In addition, for the temporal component, we used saliency maps on the Conv1D-LSTM architecture to visualize which time steps within the 30-day input window were most influential. These visualizations revealed that the model tended to focus more on recent activity patterns (e.g., the last 7–10 days), suggesting short-term escalation signals played a key role in prediction. These interpretability tools not only help validate the model's logic but also provide decision-makers with greater transparency. Such insights are valuable in identifying whether a model's prediction aligns with known threat patterns or requires further human review.

Future work may explore integrating explainability directly into the model architecture or applying counterfactual explanations to better understand "what-if" scenarios in operational settings.

"Given the sensitive nature of terrorism prediction, it is critical not only to develop accurate models but also to ensure their predictions are interpretable and transparent. To better understand the internal decision-making of our model, we explored its behavior using post-hoc interpretability methods.We applied SHAP (SHapley Additive exPlanations) to estimate the contribution of each input feature (e.g., number of incidents, fatalities, attack types) toward the model's output. SHAP values represent the average marginal contribution of a feature across all possible combinations of features, providing a unified measure of feature importance for each prediction. Features such as fatality counts, attack types classified as 'bombing/explosion,' and coordinated multiple attacks consistently showed higher SHAP values, indicating stronger influence on the model's output. These findings align with prior work by Lundberg et al.[1], demonstrating SHAP's effectiveness in interpreting complex sequence models for temporal event prediction. Figure X presents the SHAP summary plot, which visualizes the distribution of SHAP values across all samples for the top features. The plot highlights how each feature impacts the prediction magnitude and direction, with color coding indicating feature value magnitude. Table X summarizes example mean absolute SHAP values for key features, illustrating their relative importance in representative model predictions: Feature Mean Absolute SHAP Value Interpretation Fatality Count 0.45 High fatalities strongly increase risk Bombing/Explosion (Attack Type) 0.38 Bombing attacks have significant impact Coordinated Multiple Attacks 0.32 Multiple attacks in short succession Number of Incidents 0.28 Frequency of attacks influences output Hostage Taking 0.15 Lesser influence compared to fatalitie In addition, for the temporal component, we used saliency maps on the Conv1D-LSTM architecture to visualize which time steps within the 30-day input window were most influential. These visualizations revealed that the model tended to focus more on recent activity patterns (e.g., the last 7–10 days), suggesting short-term escalation signals played a key role in prediction. These interpretability tools not only help validate the model's logic but also provide decision-makers with greater transparency. Such insights are valuable in identifying whether a model's prediction aligns with known threat patterns or requires further human review. Future work may explore integrating explainability

directly into the model architecture or applying counterfactual explanations to better understand "what-if" scenarios in operational settings."

Comparative analysis and practical considerations

In addition to accuracy-based comparisons, we evaluated our proposed Conv1D-LSTM model against traditional machine learning baselines (e.g., Random Forests, Logistic Regression) and simpler neural architectures (e.g., standalone LSTM or CNN models) across several practical dimensions:

Model Accuracy AUC-ROC Inference Time (ms/sample) Training Time (mins) Parameter Count Scalability Logistic Regression 69.4 Random Forest 72.1 LSTM Only 74.8 Conv1D Only 73.6 Conv1D-LSTM (Ours) 76.5

- Computational Efficiency: Our Conv1D-LSTM model offers a good balance of performance and speed. While not as lightweight as Logistic Regression, it provides significantly better predictive capability while maintaining reasonable inference times (2ms per sample), making it viable for near real-time use.
- Training Overhead: Training time is moderate (12 minutes on a mid-tier GPU) and scalable across datasets of similar size, making periodic retraining practical.
- Scalability: The model supports batch inference and can be deployed efficiently using standard deep learning frameworks (e.g., TensorFlow, PyTorch). Its architecture is well-suited for integration with modern event monitoring pipelines.
- Deployment Considerations: The model has a relatively low memory footprint and supports fast inference, which is critical for continuous monitoring systems. Furthermore, its performance gains justify the moderate increase in computational complexity over traditional models.

These practical considerations reinforce the viability of our approach in real-world applications, where decision latency, model refresh cycles, and hardware limitations must be taken into account.

Conclusion

In recent years, the tasks of predicting and combating terrorism have gained considerable importance. In addition to conventional methods, utilizing the recent advancements in deep (machine) learning, predictive analytics can substantially aid the security forces and intelligence agencies in taking preventive measures beforehand. In this context, the proposed study targeted the problem of predicting the location of the next terrorist attack using large data. we considered a series of terrorist incidents as time-series data and formulated the task of predicting the location of the next attack as a sequence modeling problem. The predictive model comprises 1D convolutions followed by bi-directional LSTM layers which strive to learn the implicit patterns in the sequence of incidents and forecast the city, country, and region of the next incident. The experimental study of the system was carried out on the global terrorism dataset and promising results are reported on a number of standard evaluation metrics. The obtained results suggest that deep learning models can contribute substantially to predicting the probability of an attack at a particular location.

There are several interesting research directions that can be explored as an extension of the current study. To enable comparison with previous studies, our evaluation focused on commonly used metrics such as accuracy, precision, recall, and F1 score. However, we recognize the limitations of these metrics in the presence of class imbalance. In our ongoing research, we plan to incorporate additional metrics such as AUC-ROC and precision-recall curves to provide a more thorough assessment of model performance, especially for underrepresented classes.

Given the sensitive nature of terrorist attack prediction, model interpretability is critical for real-world deployment and decision-making. While the proposed model focuses on predictive performance, it currently operates as a black-box, providing little transparency into which features or past events drive specific predictions. This can be a significant limitation in practical scenarios, where law enforcement or policy analysts require explanations for model outputs to ensure trust, accountability, and effective action.To address this, future work will explore incorporating interpretable deep learning techniques, such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations), which can help quantify the influence of specific inputs (e.g., location, time, weapon type) on the model's decision. In addition, attention mechanisms or feature importance analysis could be integrated into the model architecture to enhance transparency and provide decision support information. Furthermore, data sets such as the GTD typically represent a terrorist organization as a single unified entity rather than as a network of interconnected groups. Only a few studies, such[36] and[37], have attempted to explore the structure of terrorist networks and identify strong links among groups and subsubgroups.se aspects require further in-depth investigation, where modern machine learning approaches may prove particularly effective.[38] investigated the relationships between terrorist groups between 1987 and 2005 and concluded that more than one-third of the groups have at least one cooperative relationship, and about 10 percent of the groups have at least one adversarial relationship. This area of research has been addressed in only a limited number of studies, such as data from global social networks on terrorist groups [39], and warrants further investigation.In addition, our current Conv1D-BiLSTM model operates as a many-to-one sequence predictor without autoregressive feedback from previous predictions. Future research could explore autoregressive architectures and incorporate attention mechanisms such as Transformers, which have shown success in modeling long-range dependencies and providing enhanced interpretability. Evaluating these approaches may further improve prediction accuracy and model transparency in terrorist attack forecasting.

Data availability

The authors confirm that the data supporting the findings of this study are available within the article.

Received: 26 September 2024; Accepted: 19 June 2025
Published online: 02 July 2025

References

1. Uddin, M. I. et al. Prediction of future terrorist activities using deep neural networks. In *Complexity* (2020).
2. Aladi, H. B. et al. International Conference On Smart Technologies For Smart Nation (SmartTechCon). *IEEE.***2017**, 1010–1017 (2017).
3. Xueli, H. et al. Quantitative research on global terrorist attacks and terrorist attack classification. *Sustainability* **11**(5), 1487 (2019).
4. Halim, Z. et al. Utilizing 3D joints data extracted through depth camera to train classifiers for identifying suicide bomber. *Expert Syst. Appl.* **179**, 115081 (2021).
5. Global Terrorism Database. https://www.start.umd.edu/gtd/search/Results.aspx?search=GTD &sa.x=39 &sa.y=7. Accessed: 202 0-01-15.
6. Faryal, G. et al. Terrorist group prediction using data classification. In *Work. MultiRelational Data Min. MRDM2003 10* 199–208 (2014).
7. Tutun, S., Khasawneh, M. T. & Zhuang, J. New framework that uses patterns and relations to understand terrorist behaviors. *Expert Syst. Appl.* **78**, 358–375 (2017).
8. Zakaria, M., Jun, W. & Ahmed, H. Effect of terrorism on economic growth in Pakistan: An empirical analysis. *Econ. Res.-Ekonomska istra ž ivanja* **32**(1), 1794–1812 (2019).
9. Agarwal, P., Sharma, M. & Chandra, S. Comparison of machine learning approaches in the prediction of terrorist attacks. In *2019 Twelfth International Conference on Contemporary Computing (IC3)* 1–7 (IEEE, 2019).
10. Snehanshu, S. & Abu, S. Future terrorist attack prediction using machine learning techniques (National Institute of Science Technology and Development Studies, 2017).
11. Magen, A. Fighting terrorism: The democracy advantage. *J. Democr.* **29**(1), 111–125 (2018).
12. Alsaedi, A. S., Almobarak, A. S. & Alharbi, S. T. Mining the global terrorism dataset using machine learning algorithms. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* 1–7 (IEEE, 2019).
13. Chaurasia, S., Warikoo, V. & Khan, S. Global Terrorism Predictive—Analysis. In *Advances in Computer Communication and Computational Sciences* 77–85 (Springer, 2019).
14. Jin, S., Ge, J. & Peng, J. Terrorism risk assessment using hierarchical bidirectional fuzzy rule interpolation. In *2016 IEEE 15th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC)* 403–410 (IEEE, 2016).
15. Trisha, J. Predicting success of global terrorist (2019).
16. Feng, Y. et al. An XGBoost-based casuality prediction method for terrorist attacks. *Complex Intell. Syst.* **6**(3), 721–740 (2020).
17. Soliman, G. M. A. & Abou-El-Enien, T. H. M. Terrorism Prediction Using Artificial Neural Network. *Revue d'Intelligence Artificielle* **33**(2), 81–87 (2019).
18. Tolan, G. M. & Soliman, O. S. An experimental study of classification algorithms for terrorism prediction. *Int. J. Knowl. Eng.-IACSIT* **1**(2), 107–112 (2015).
19. Alfatih, M., Li, C. & Saadalla, N. E. Prediction of Groups Responsible for Terrorism Attack Using Tree Based Models. In *Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science* 320–324 (2019).
20. Maniraj, S. P. et al. Data aggregation and terror group prediction using machine learning algorithms. *Int. J. Recent Technol. Eng.* **8**(4), 1467–1469 (2019).
21. Pilley, P. H. & Sikchi, S. S. Model for Predicting Terrorist Group by CLOPE Algorithm (2014).
22. Verma, C., Malhotra, S. & Verma, V. Predictive modeling of terrorist attacks using machine learning. *Int. J. Pure Appl. Math.* **119**, 06 (2018).
23. Olabanjo, O. A. et al. An ensemble machine learning model for the prediction of danger zones: Towards a global counter-terrorism. *Soft Comput. Lett.* **3**, 100020 (2021).
24. Ibrahim, T., & Aryya, G. Real time big data analytics for predicting terrorist incidents. In *IEEE Symposium on Technologies for Homeland Security (HST)* 1–6 (IEEE, 2016).
25. Ismail, H. M. & Kazi, H. Use of predictive modeling for prediction of future terrorist attacks in Pakistan. *Int. J. Comput. Appl.* **975**, 8887 (2018).
26. Liu, Q. et al. Predicting the next location: A recurrent model with spatial and temporal contexts. In *Thirtieth AAAI Conference on Artificial Intelligence* (2016).
27. Huamanı, E. L. Alicia, A. M. & Roman-Gonzalez, A. machine learning techniques to visualize and predict terrorist attacks worldwide using the global terrorism database. *Machine Learning* **11**(4) (2020).
28. Taheri, R. & Ahmadzadeh, M. & Kharazmi, M. R. A new approach for feature selection in intrusion detection system. Fen Bilimleri Dergisi (CFD) 36.6 (2015).
29. Taheri, R. & Ahmadzadeh, M. Studying the effect of discretization of data on accuracy of predicting Naïve Bayes algorithm, case study KDD99 CUP. *J. Curr. Res. Sci.* 457–462 (2016).
30. Elsworth, S. & Güttel, S. Time series forecasting using LSTM networks: A symbolic approach. In *arXiv preprint*. arXiv:2003.05672 (2020).
31. Wang, H., Song, Y. & Tang, S. LSTM-based Flow Prediction. In *arXiv preprint*. arXiv:1908.03571 (2019).
32. Nápoles, G. et al. Long short-term cognitive networks. In *Neural Computing and Applications* 1–13 (2022).
33. Siika, J., Wieczorek, M. & Woźniak, M. Recurrent neural network model for high-speed train vibration prediction from time series. In *Neural Computing and Applications* 1–14 (2022).
34. Kang, D., Lv, Y. & Chen, Y-Y. Short-term traffic flow prediction with LSTM recurrent neural network. In *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)* 1–6 (IEEE, 2017).
35. Kiranyaz, S. et al. 1D convolutional neural networks and applications: A survey. arXiv preprint. arXiv:1905.03554 (2019).
36. Miller, E. E., Smarick, K., & Simone, J. Jr. Profiles of perpetrators of terrorism in the United States (PPTUS): Data collection and descriptive analysis. In *Interim Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, US Department of Homeland Security* (2011).
37. Rae, J. A. Will it ever be possible to profile the terrorist? *J. Terror. Res.* (2012).
38. Phillips, B. J. *How Terrorist Organizations Survive: Cooperation and Competition in Terrorist Group Networks*.
39. Asal, V. & Karl Rethemeyer, R. The nature of the beast: Organizational structures and the lethality of terrorist attacks. *J. Polit.* **70**(2), 437–449 (2008).

Acknowledgements

Ongoing Research funding program, (ORF-2025-476), King Saud University, Riyadh, Saudi Arabia.

Declarations

Conflict of Interest

On behalf of all the authors, the corresponding author states that there is no conflict of interest.

Additional information

Correspondence and requests for materials should be addressed to A.A. or F.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.