STM JOURNALS

International Journal of
Information Security Engineering

Volume 2, Issue 2, 2024
July–December
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

Counter Terrorism Prediction and Risk Evaluation (C-TRIP)

Yash Shirsath[1,*], Vedant Bhosale[1], Manoj Deshpande[2], Shilpali Bansu[3]

Abstract

The global landscape in the 21st century is marked by complex and evolving security challenges, none more pressing than the threat of terrorism. Acts of terror have left a profound impact on societies, economies, and governments worldwide, underscoring the critical importance of effective counter terrorism strategies. The "Counter Terrorism Prediction and Risk Evaluation (C-TRIP)" represents a significant stride in addressing this ever-pressing challenge. In a time marked by global security challenges, "Counter Terrorism Prediction and Risk Evaluation (C-TRIP)" is emerging as an innovative solution to deal with the ever-evolving terrorist threats. The project arises from the pressing need for predictive systems. It can anticipate and mitigate the possibility of terrorism. The motivation is external This effort is reflected in the rise and proliferation of terrorist incidents dramatically in recent years. Traditional counter terrorism response strategies are not the right length of time. Timely, data-driven interventions are needed to address this matter of great importance. This offers an extensive overview of current literature. Critically examines the strengths and limitations of past research. Define what is important is the research gap in the current work, and the search for a new framework was emphasized which can provide an accurate risk assessment and early warning. It employs a data-driven methodology utilizing machine learning and data analysis techniques to predict and assess terrorist incidents. C-TRIP aims to enhance decision-making in counter terrorism efforts by providing timely and accurate insights into the likelihood and severity of potential terrorist events.

Keywords: Counterterrorism, terrorism, security challenges, global landscape, predictive systems, data-driven interventions, global security, predictive systems, threat assessment, early warning, decision-making, methodology, architecture, experimental results

***Author for Correspondence**
Yash Shirsath
E-mail: yashshirsath2410@gmail.com

[1]Student, Department of Artificial Intelligence and Data Science, Jawahar Education Society's AC Patil College of Engineering, Kharghar, Navi Mumbai, Maharashtra, India
[2]Head and Professor, Department of Computer Engineering, Jawahar Education Society's AC Patil College of Engineering, Kharghar, Navi Mumbai, Maharashtra, India
[3]Head and Assistant Professor, Department of Artificial Intelligence and Data Science, Jawahar Education Society's AC Patil College of Engineering, Kharghar, Navi Mumbai, Maharashtra, India

Received Date: June 27, 2024
Accepted Date: August 18, 2024
Published Date: October 24, 2024

Citation: Yash Shirsath, Vedant Bhosale, Manoj Deshpande, Shilpali Bansu. Counter Terrorism Prediction and Risk Evaluation (C-TRIP). International Journal of Information Security Engineering. 2024; 2(2): 14–24p.

INTRODUCTION

The current global scenario is fraught with an array of complex security challenges, among which terrorism stands out as one of the most urgent and pervasive threats. Incidents of terrorism have cast a long shadow on nations, economies, and governmental bodies globally, accentuating the critical need for robust and effective countermeasures. In response to these escalating threats, it is imperative to develop advanced technologies capable of forecasting and evaluating terrorist activities in a timely manner [1].

This imperative has led to the emergence of innovative solutions such as the "Counter Terrorism Prediction and Risk Evaluation (C-TRIP)" system, which represents a significant advancement in the realm of counterterrorism. C-TRIP is designed as a comprehensive framework that harnesses diverse

data sources and analytical methodologies to forecast terrorist activities and assess associated risks. By leveraging a multitude of information streams, including intelligence reports, law enforcement records, and social media data, the C-TRIP aims to identify patterns and trends indicative of potential terrorist threats. Moreover, C-TRIP is envisioned as a proactive tool that empowers law enforcement agencies, intelligent communities, and other stakeholders to prevent, mitigate, and respond effectively to terrorist attacks. Through its data-driven approach and advanced analytical techniques, C-TRIP seeks to revolutionize decision-making processes in counterterrorism efforts, thereby providing actionable insights into the likelihood and severity of potential terrorist events. This research endeavors to provide a comprehensive overview of C-TRIP, elucidating its conceptual framework, methodological underpinnings, and practical implications in the counterterrorism domain. By critically examining the strengths and limitations of existing research, identifying research gaps, and proposing innovative risk assessment and early warning frameworks, this study aims to address the fundamental challenge of anticipating, assessing, and responding to terrorist activities effectively. C-TRIP represents a significant step forward in the ongoing battle against terrorism, offering a proactive and data-driven approach to enhancing global security [2]. Through its methodology, architecture, and empirical findings, C-TRIP has the potential to transform the landscape of counterterrorism efforts, enabling stakeholders to remain one step ahead of evolving threats and safeguarding societies against the scourge of terrorism.

In essence, this research contributes to the advancement of the field of counterterrorism by providing a robust framework for proactive threat assessment and mitigation strategies. By leveraging cutting-edge technologies and innovative methodologies, C-TRIP holds the promise of ushering in a new era of security preparedness, where data-driven insights empower stakeholders to anticipate, preempt, and combat the ever-evolving threat of terrorism [3]. In this study, we detail the methodology, architecture, and experimental results of C-TRIP, demonstrating its efficacy in forecasting terrorist activities and assessing risk levels. Through case studies and comparisons with existing systems, we illustrate the value and potential applications of C-TRIP for addressing real-world security challenges. Our research contributes to advancing the field of counterterrorism by providing a comprehensive framework for proactive threat assessment and mitigation strategies.

LITERATURE REVIEW

Existing System

In this chapter, we embark on a thorough examination of the existing systems and methodologies pertaining to counterterrorism, risk assessment, and the prediction of terrorist activities. Our survey endeavors to provide a comprehensive overview of the current landscape in the field, shedding light on the various approaches and frameworks employed by organizations and agencies worldwide. By delving into the intricacies of these existing systems, we seek to gain valuable insights into their functionalities, strengths, and limitations, thereby laying the groundwork for the development of the "Counter Terrorism Prediction and Risk Evaluation(C-TRIP)." Among the notable systems analyzed in our survey is the Homeland Security Information Network (HSIN) established by the United States Department of Homeland Security [4]. Serving as a shared network for law enforcement and intelligence agencies, the HSIN facilitates the exchange of critical information pertaining to terrorist threats and incidents. Similarly, the Counter Terrorism Strategy (CONTEST) system, overseen by the United Kingdom's National Counter Terrorism Security Office (NaCTSO), employs a diverse array of data sources and analytical methodologies to assess the risk of terrorism within the United Kingdom.

Furthermore, our survey encompasses systems such as the Integrated Terrorism Assessment Centre (ITAC) operated by the Canadian Security Intelligence Service (CSIS) and the Terrorism Information Management System (TIMS) managed by the Australian Security Intelligence Organization (ASIO). These systems play pivotal roles in collecting, managing, and analyzing information related to terrorism threats and incidents, thereby contributing to broader efforts aimed at enhancing national security. Additionally, we explored the National Counter terrorism Information Centre (NCIC), administered by the Federal Bureau of Investigation (FBI) in the United States [5]. Through its comprehensive data collection and

analysis capabilities, NCIC plays a crucial role in providing actionable intelligence to law enforcement agencies and policymakers, thereby bolstering the nation's counterterrorism efforts. By meticulously examining these types of existing systems and methodologies, we aim to identify the gaps and shortcomings that necessitate the development of an innovative and comprehensive solution, such as C-TRIP.

Research Gaps

The effectiveness of C-TRIP systems is contingent on several critical factors that influence their accuracy, reliability, and transparency. First, the accuracy of C-TRIP systems depends on the quality and completeness of the data utilized [6]. Inaccurate or incomplete data can significantly compromise a system's ability to generate precise forecasts and risk assessments, thereby limiting its overall effectiveness. Moreover, C-TRIP systems may exhibit bias if the data on which they rely are inherently biased. For instance, if a C-TRIP system predominantly utilizes data sourced from law enforcement agencies, it may inadvertently exhibit bias toward identifying and monitoring terrorist groups and individuals already known to law enforcement. Addressing such biases is paramount for ensuring the fairness and impartiality of C-TRIP systems. Transparency has also emerged as a critical concern for C-TRIP systems. Often characterized by their opacity and complexity, these systems can be challenging for users to comprehend and scrutinize. The lack of transparency not only undermines user trust but also impedes efforts to identify and rectify any biases or errors present within the system [7].

PROPOSED SYSTEM OF C-TRIP AND METHODOLOGIES

Let us now examine the proposed scheme. In this regard, we introduce the proposed framework and emphasize the importance of this alternative in data aggregation [8]. We discuss the background and motivation behind this new approach and formulate a detailed analysis of the framework. We divided this study into three parts.

1. *Prediction of terrorist activity:* The main goal of this project is to develop a system that can predict future terrorist acts. This shows where and when a crime is likely to occur.
2. *Risk analysis:* In addition to forecasting, the system identifies the level of risk associated with potential terrorist attacks. This assessment considers factors such as the severity, likelihood, and probability of the impact of an attack.
3. *About our databases:* This database reflects the assembly rule agreement of the Global Terrorism Database. The Global Terrorism Database (GTD) is an event database with more than 200,000 records of terrorist attacks since 1970. Managed by the National Society for the Study of Terrorism (START) at the University of Maryland can reduce error This enables you to log attacks that have been verified as "fixed". The GTD defines a terrorist attack as the deliberate use of unlawful force or violence by an individual or group outside governmental authority to achieve a political, economic, religious, or social goal through fear or coercion types, especially to include a statement in the GTD, which results from a conscious decision-making process archiving, maintenance, and development is supported by:
    i. United States Department of Justice [MD–1.1]
    ii. United States Department of Homeland Security Department of Science and Technology [MD–1.1]
    iii. United States Department of State, Office of Counterterrorism and Violent Extremism [MD–1.2]
    iv. United States Department of Defense, Counterterrorism Technical Assistance Division [MD–1.1]
    v. German Foreign Ministry [MD–2.1]
    vi. United Kingdom Department of Foreign Affairs, Commonwealth and Development [MD–2.1]

Methodologies

Data Collection

During the data collection process for the C-TRIP system, we gathered a comprehensive dataset consisting of 209,709 rows and 36 columns. This dataset encompasses a wide range of variables relevant to terrorist activities, including but not limited to geographical locations, demographic information, historical incident data, and socioeconomic indicators. Each row of the dataset represents a distinct observation, whereas the columns capture the various attributes and characteristics associated with terrorist incidents.

Data Preprocessing

Once data is collected, they must be cleaned, standardized, and processed to ensure accuracy and reliability. This can include tasks, such as removing duplicates, handling missing values, encoding categorical variables, and normalizing numeric features.

Feature Engineering

After preprocessing, the data were converted into a format suitable for machine learning algorithms. This includes feature engineering techniques such as reducing dimensions, feature scaling, and creating new features based on domain knowledge.

Model Selection

Next, appropriate machine learning algorithms were selected based on the nature of the prediction task and the characteristics of the dataset. The commonly used algorithms for forecasting terrorist activities include decision trees, random forests, support vector machines, and neural networks.

Model Training

A portion of the dataset was used to train the selected machine learning models on the preprocessed data. During training, modelers learn patterns and relationships in the data that allow them to make predictions about future terrorist activities.

Model Evaluation

Once trained, the models were evaluated using a separate portion of the dataset that was not used during training. Evaluation metrics such as accuracy, precision, recall, and F1-score were used to assess the performance of the models and identify areas for improvement.

Model Deployment

After successful analysis, the trained model is deployed in a manufacturing environment that can be used to make real-time predictions regarding future terrorism. This may involve integrating the models into web applications, dashboards, or other decision-support systems for easy stakeholder access.

Review and Maintenance

The images used were constantly monitored and updated to ensure their long-term accuracy and effectiveness. This may include periodically retraining models with new data, fine-tuning hyperparameters, and addressing the issues or biases that arise during processing.

RESULTS AND ANALYSIS

Data Collection and Exploration

As mentioned in the GTD archive, I captured this dataset. After cleaning the entire data, our final data shape is (40130, 10); in the data cleaning process, we removed missing columns, removed unwanted columns, retained important columns, and fixed latitude and longitude columns and their degrees; accordingly, it fits according to our needs so that it is not a problem in model building [9]. In data preprocessing, we change the date time format, add encoding to some categorical columns, and then perform some normalization on numerical columns.

Data Visualization

We conducted sentiment analysis of the "Explanation" column using the Vader sentiment analysis tool, as shown in Figure 1. This study revealed the following.

1. *Negative incidents:* 34,698
2. *Positive incidents:* 3,608
3. *Neutral incidents:* 1,822

To perform this analysis, we employed the punkt tokenizer, wordnet, and corpus to pre-process the text data. Additionally, we utilized lemmatized text to generate a word cloud map [10]. However, we

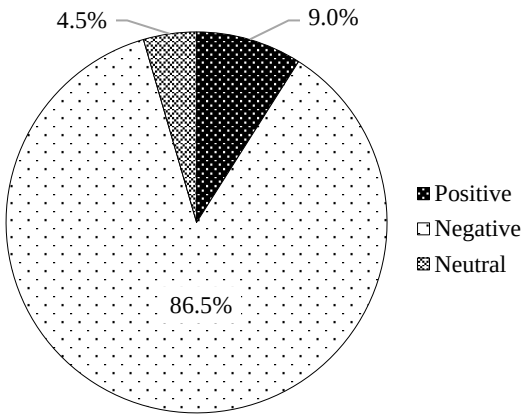

Figure 1. Pie chart of sentiment analysis results with the highest 86.5 Negative, 9.0 Positive, and 4.5 Neutral.

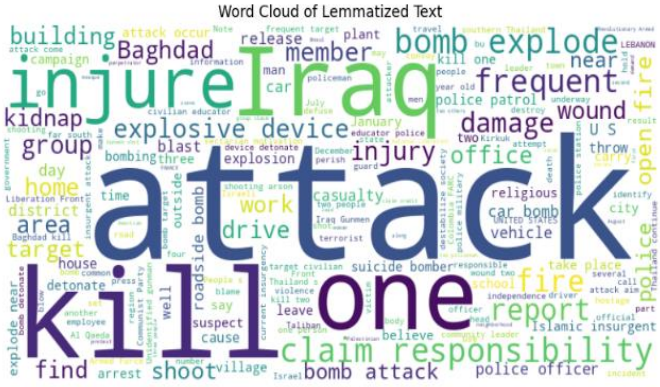

Figure 2. Word cloud map shows the highest number of frequent words from data.

observed discrepancies in the generated word cloud map and made the necessary corrections to ensure accuracy, as shown in Figure 2.

Then, by performing a time series analysis of terrorist events over time, we constructed graphs to visualize the temporal patterns and patterns. These graphs show the frequency of terrorism in different time periods, such as days, months, or years, depending on the granularity of the data by comparing the number of incidents over time. We were able to identify any factors that were continuous, periodic, or abnormal in the data [11]. This time series analysis provided valuable insights into the temporal dynamics of terrorist activities, enabling us to identify patterns and make informed decisions on counterterrorism strategies and interventions, as shown in Figure 3.

We then created a pie chart showing the distribution of incidents in each country and the corresponding number of incidents. This graphic provides a detailed overview of the geographic distribution of terrorist activities, highlighting the regions of repeated incidents. A pie chart visually representing the proportion of incidents in each country allowed for comparison of ease of access and identification of hotspots or areas of concern, provided quantitative insight into size, and informed strategic decision-making and resource allocation in efforts to fight terrorism (Figure 4).

We then continued to explore the relationship between injury and mortality using the heat map. The heat map provides a visual representation of the relationships between these variables, allowing us to identify any significant relationships or patterns. The correlational model provides insight into the strength and direction of the relationship between injury and death in terrorism (Figure 5).

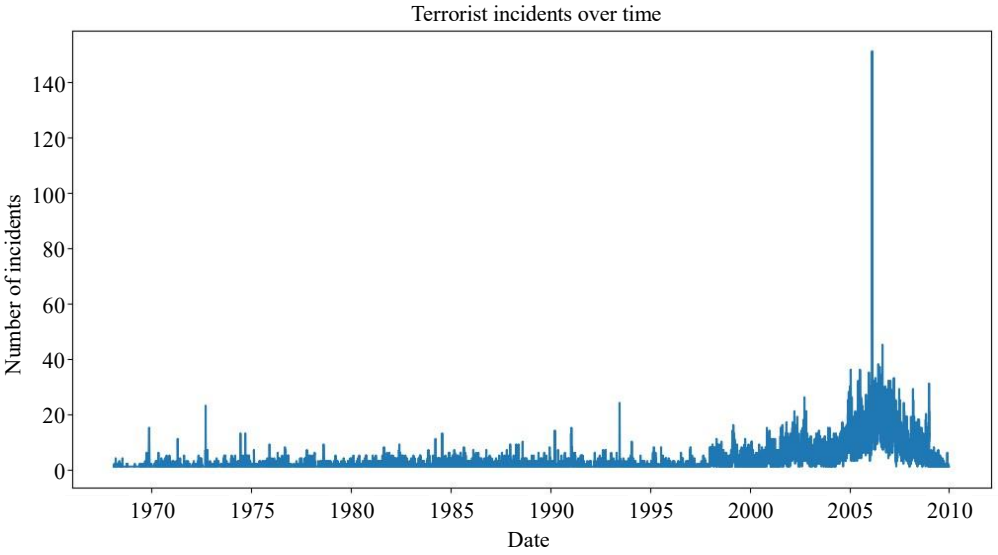

Figure 3. Time series analysis on time and incident.

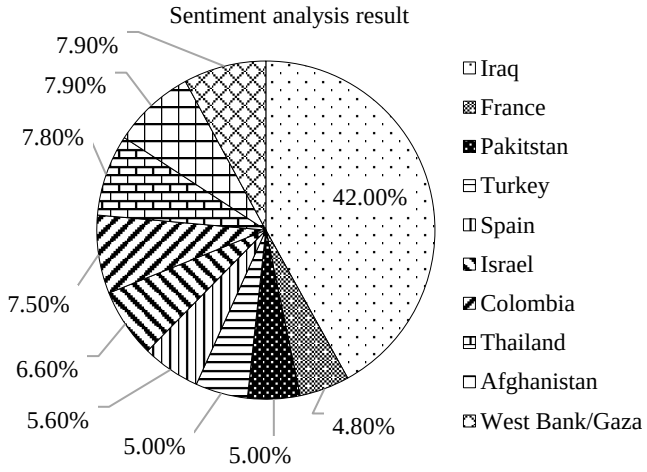

Figure 4. Now using a pie chart, we distribute here terrorist attacks by country.

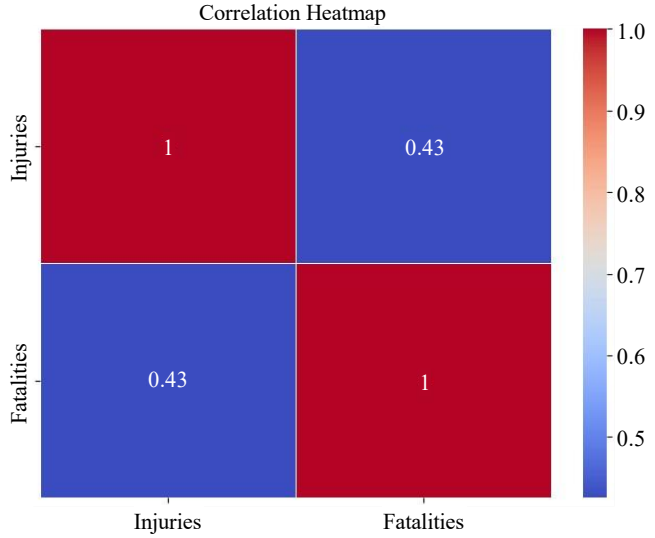

Figure 5. Now we find a correlation heatmap of injuries and fatalities.

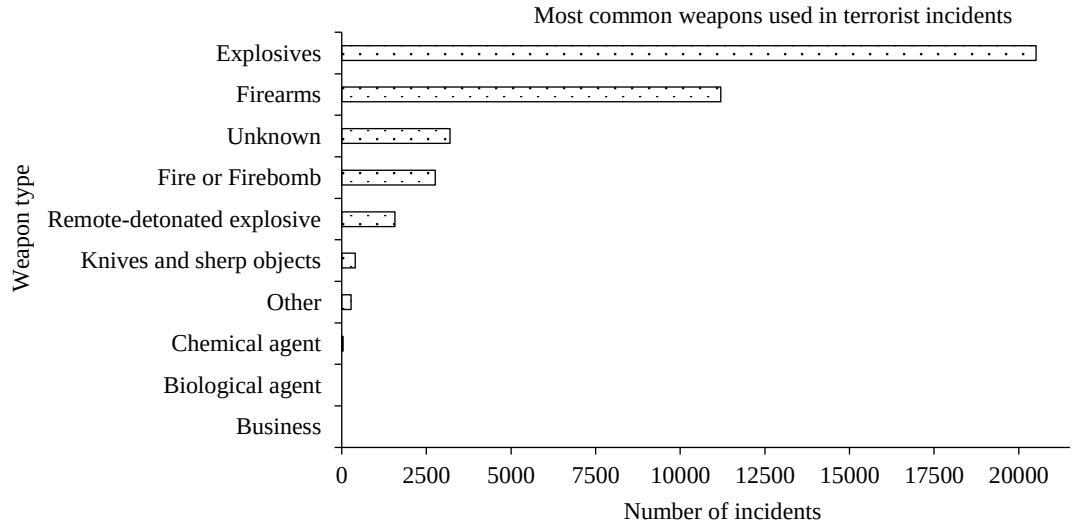

Figure 6. Now we find the most commonly used weapons during terrorist attacks.

To visualize the most common weapons used in terrorist incidents, we created a bar plot displaying the frequency of each weapon category. This bar plot allowed us to easily identify the weapons most frequently used in terrorist attacks, as shown in Figure 6. In addition to capturing this information, we gained insights into the types of weapons commonly associated with terrorism, which can inform security measures and counterterrorism strategies, providing valuable information for policymakers, law enforcement councils, and others involved in the fight against terrorism.

Entity Recognition Analysis Result

- *Entity:* Abu Bakr al-Baghdadi, Label: PERSON
- *Entity:* ISIS, Label: ORG
- *Entity:* The Middle East, Label: LOC
- *Entity:* July 15, 2023, Label: DATE

NMF Model Analysis

- *Topic #1:* Police patrol Iraq frequent wounding attacks killing roadside Baghdad near
- *Topic #2:* Thailand Insurgents Drive Islamic Shootings Insurgency 2004 educator's arson underway
- *Topic #3:* Bomb attack exploded device injured people car explosive detonated blast
- *Topic #4:* Gunmen killed Iraq attacks frequent Baghdad shot al opened attack
- *Topic #5:* Fired settlement reported claimed Gaza rockets Hamas Israeli wing rocket

Network Analysis

Network analysis in the context of extremist activities involves studying the connections and interactions between individuals and groups associated with extremist ideologies, as shown in Figures 7 and 8. We extracted data from the dataset and created a time series dataset. Visualizations such as line plots and seasonal decomposition help identify trends and seasonal patterns. Statistical methods such as autoregressive integrated moving average (ARIMA) modeling are used to forecast future incidents. This analysis aids in the understanding of the temporal dynamics of proactive security measures.

Machine Learning App. (ML Part)

In this section, we present the performance measures of a random forest model trained for terrorist activity prediction and risk assessment using the C-TRIP framework. The model was evaluated based on various classification parameters, including the accuracy, precision, recall, F1-score, and confusion matrix.

1. *Accuracy:* The accuracy of the random forest sample was 62%. This indicates that the model correctly predicted the outcome in 62% of the models in the test dataset.

Figure 7. Finding extremist terrorist groups using network analysis.

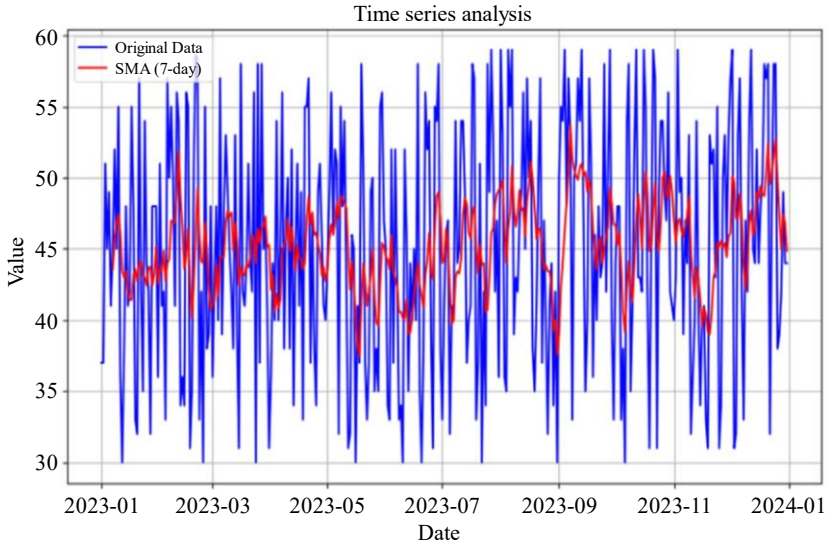

Figure 8. Time series analysis using Date and values and years.

2. *Accuracy:* Accuracy for the "False" class: 67%, Accuracy for the "True" class: 28%Precision represents the proportion of cases predicted positively (or negatively) that are positive (or negative). The accuracy of the "False" class indicates that 67% of all cases predicted as "False" are in fact "False" False. Similarly, the accuracy of the "True" class indicates that only 28% of the observations predicted as "True" were in fact "True" True.
3. *Recall:* Recall for "False" subject: 88%, Recall for "True" subject: 10%.
   The recall represents the proportion of positive (or negative) actual examples that were correctly predicted as positive (or negative). Recall for the "False" class means that the model predicted 88% correctly the actual "False" model. However, the recall for the "True" class indicates that the sample made up only 10% of the actual "True" sample.
4. *F1-score:* F1-score for "False" class: 0.76, F1-score for "True" class: 0.15. The F1 score is the harmonic mean of the precision and recall. This strikes a balance between accuracy and recall. The F1-score of the "False" class (0.76) indicates slightly better performance, while the F1-score of the "True" class (0.15) indicates poorer performance.

5. *Confusion matrix:* The confusion matrix provides a detailed description of the model's predictions. The confusion matrix shows that of the 1680 samples of the "False" class, 1473 samples are correctly classified as "False" (True Negatives), and 207 are incorrectly classified as "True" (False). Positives) Instance 811 of the "True" class is "True" (True Positives). were correctly classified, while 729 were incorrectly classified as "Counterfeit" (Counterfeit Items/FN). Individual cross-validation scores: The individual cross-validation scores of the model reflect its accuracy for different sets of training data. These scores ranged from 60.32% to 63.63%, showing some variability owing to differences in the training and validation procedures among the clusters.
6. *Mean cross-validation accuracy:* The mean cross-validation accuracy, computed as the average of the individual scores, was approximately 62.01%. This metric offers a stable estimate of a model's performance across multiple folds, indicating its general applicability. A higher accuracy indicates a better overall performance.
7. *Interpretation:* With an average cross-validation accuracy of 62.01%, the random forest model exhibits moderate performance in predicting terrorist activities and assessing associated risks while reasonably accurate, there's potential for enhancement through hyperparameter tuning, feature optimization, or exploring alternative algorithms.

Predict Future Attacks

We analyzed historical data updates for terrorist events, which are important for training and machine learning models aimed at predicting future attacks, as shown in Figures 9–11. It starts an empty DF and fills it with randomly generated values for attributes such as year, month, geographic coordinates, lethality,

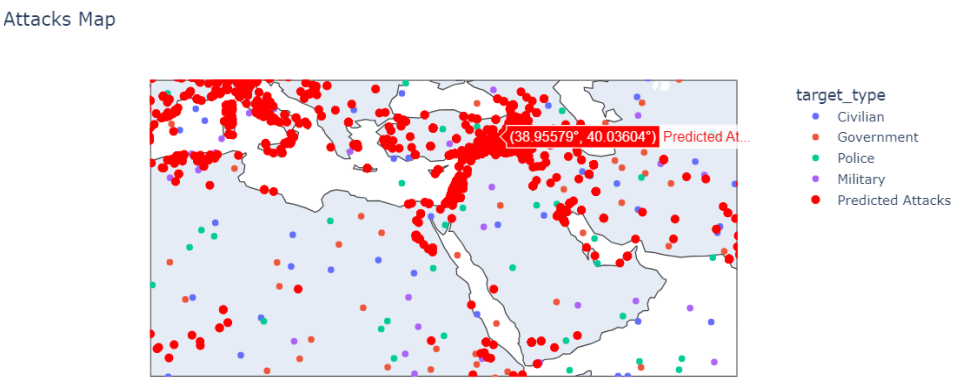

Figure 9. Correctly predicted attacks by Hamas and Hezbollah on Israel as well as conflict between Yemen and the Houthis

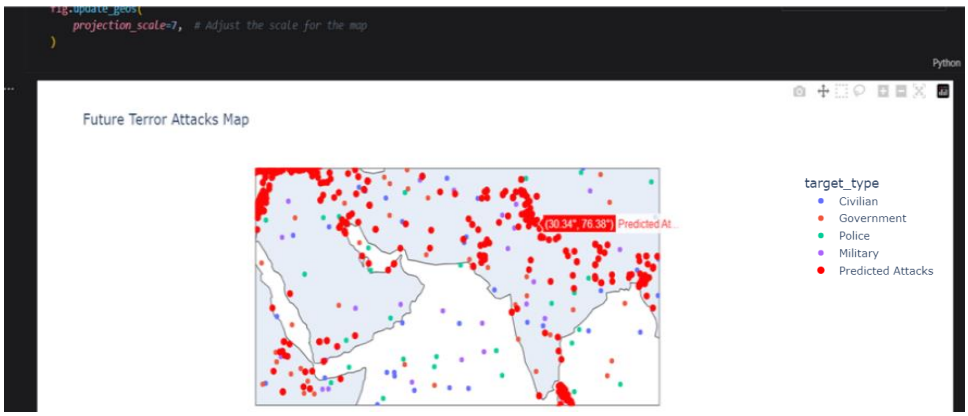

Figure 10. Successfully predicted attacks on Assam Rifles and CRPF and civilians at Manipur by kuki terrorists at northeast and also predicted naxal moment in Chhattisgarh during election time in east India and conflict between terrorist militia army and C60.


```
# Show the map
fig.show()
```

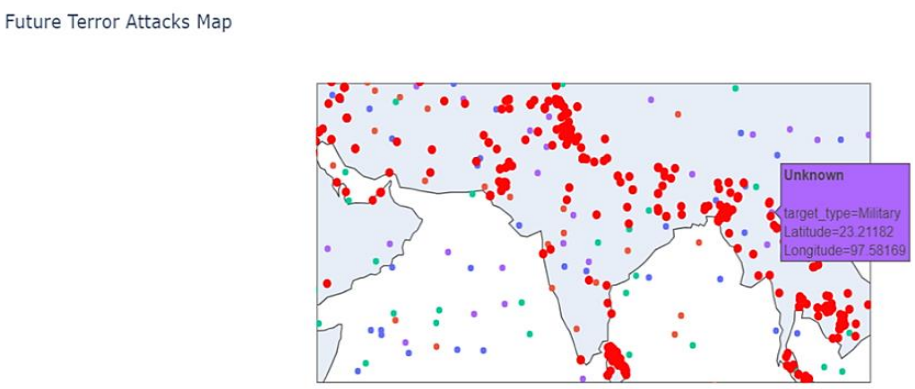

Figure 11. Prediction of Indian subcontinent.

target type, and group name. This generated historical data helps simulate real-world scenarios, facilitating the development and testing of predictive models for counterterrorism efforts.

CONCLUSION

The Terrorist Activity Forecasting Risk Assessment System (C-TRIP) represents a significant advancement in addressing the multifaceted challenges posed by terrorism in the 21st century. By leveraging advanced machine learning and data analytics techniques, C-TRIP offers a proactive approach to predicting future terrorist activities and assessing associated risks. Through an extensive review of the existing literature and a critical analysis of prior research, C-TRIP identifies and addresses gaps in current counterterrorism methodologies, presenting a novel framework for accurate risk management and early warning. The methodology, architecture, and experimental results of the C-TRIP underscore its effectiveness in forecasting terrorist activities and evaluating risk levels. Case studies and comparisons with existing systems further highlight the value of C-TRIP for addressing real-world security challenges. While demonstrating moderate performance, C-TRIP also emphasizes the need for continuous enhancement through hyperparameter tuning, feature optimization, and the exploration of alternative algorithms. Looking forward to future work in the realm of C-TRIP will involve several avenues for improvement and expansion. Enhancing the accuracy and reliability of predictive models remains a priority, necessitating the refinement of machine learning algorithms, incorporation of additional data sources, and improvement of feature-selection techniques to capture the intricate dynamics of terrorist activities. Furthermore, the development of real-time monitoring capabilities in C-TRIP is imperative to enable timely response to emerging threats. This may entail integrating data source pipelines, deploying advanced anomaly detection algorithms, and leveraging natural language processing techniques to extract actionable insights from informal sources, such as social media and online forums. The C-TRIP offers a promising framework for bolstering global security and mitigating the evolving threat of terrorism. As we continue to refine and optimize C-TRIP, it holds the potential to significantly contribute to the advancement of counterterrorism efforts, emphasizing the importance of quality, transparency, and continuous improvement in effective counterterrorism strategies.

Future Work

Future work in the realm of C-TRIP will involve several avenues for improvement and expansion. First, improving the precision and dependability of predictive models is a priority. This could involve refining machine learning algorithms, incorporating additional data sources, and improving feature-selection techniques to better capture the complex dynamics of terrorist activities. In addition, real-time monitoring capabilities must be developed in C-TRIP to enable timely response to emerging threats. This can include integrating data source pipelines, using advanced anomaly detection algorithms, and

using natural language processing techniques to extract actionable insights from data from informal sources, such as social media and online forums.

REFERENCES

1. Miller E. (2022). A look back at 2020: Trends from the Global Terrorism Database (GTD)™. [Online] National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland, College Park; A Department of Homeland Security Emeritus Center of Excellence led by the University of Maryland. Available from: https://www.start.umd.edu/look-back-2020-trends-global-terrorism-database-gtd
2. United States Department of Homeland Security (DHS). (2024). All/PIA-084 Joint-Threat Information Management System (J-TIMS) [Online]. United States Department of Homeland Security. Available from: https://www.dhs.gov/publication/dhsallpia-084-joint-threat-information-management-system-j-tims
3. ICSR Team. (2023). Financing violent extremism: An examination of maligned creativity in the use of financial technologies [Online]. ICSR. Available from: https://icsr.info/2023/04/12/financing-violent-extremism-an-examination-of-maligned-creativity-in-the-use-of-financial-technologies/
4. ProtectUK. (2022). Publicly Accessible Locations (PALs) Guidance. ProtectUK. [online] Available from: https://www.protectuk.police.uk/advice-and-guidance/risk/publicly-accessible-locations-pals-guidance
5. Jones SG, Libicki MC. How Terrorist Groups End: Lessons for Countering al Qa'ida. Santa Monica (CA): RAND Corporation; 2008. Available from: https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG741-1.pdf
6. Aolain FN, Campbell C. Managing terrorism. J Nat'l Sec Law Policy. 2017;9:367–411.
7. Gayathri Y, Sri Lalitha Y, Aditya Nag MV, Althaf Hussain Basha S. Data-driven prediction model for crime patterns. In: Satapathy SC, Bhateja V, Favorskaya MN, Adilakshmi T, editors. Smart computing techniques and applications. Smart Innovation, Systems and Technologies. Vol. 225. Singapore: Springer; 2021. pp. 47–58. DOI: 10.1007/978-981-16-0878-0_6.
8. Goodchild MF, Janelle DG. Toward critical spatial thinking in the social sciences and humanities. GeoJournal. 2010;75:3–13. doi: 10.1007/s10708-010-9340-3.
9. Kesavan T, Krishnamoorthy RK. An efficient recurrent neural network with ensemble classifier-based weighted model for disease prediction. J Intell Syst. 2022;31:979–91. doi: 10.1515/jisys-2022-0068.
10. Valk CA, Lovei P, Cornelis H, Chuang Y, Visser T, Pu P, et al. Identifying a motivational profile for older adults towards increased physical activity. Int J Des. 2021;15:17–32.
11. Sharma A, Bajaj V, Arora J. Machine learning techniques for real-time emotion detection from facial expressions. 2023 2nd Edition of IEEE Delhi Section Flagship Conference (DELCON), Rajpura, India. 2023. pp. 1–6. DOI: 10.1109/DELCON57910.2023.10127369.

