JSRT JOURNAL
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY
PAGES: 217-228
26/06/25
VOLUME-3 ISSUE-6 JUNE

Data Driven Insights: Machine Learning For Terrorist Attacks Region Predication

Dr. Sridevi M Hosmani[1], M Divya Lalitha[2], Sneha R H[3], Vaishnavi R A[4], Vidya shree B H[5]

[1]*Assistant Professor, Department Of Artificial Intelligence and Machine Learning, Godutai Engineering College, Kalaburagi, India.*

[2,3,4,5]*Students, Department Of Artificial Intelligence and Machine Learning, Godutai Engineering College, Kalaburagi, India*

ABSTRACT

The use of purposeful violence for the aim of achieving political or religious goals is what is meant by the term "terrorism." This paper's purpose is to provide a prediction about the location and nation in which terrorist strikes will occur. In addition to this, it evaluates the effectiveness of machine learning algorithms in predicting the nation and the location where terrorist attacks would occur. When it comes to predicting both the nation and the area, Logistic Regression has an accuracy rate of 82%. For the purpose of this study, the Global Terrorism Database (GTD) is used. This database is open source and contains information on terrorist incidents that have occurred all over the globe since 1970. This body of work has the potential to be used in the future by policymakers in order to create policies and defense systems that are capable of monitoring and forecasting terrorist operations.

Keywords: Machine Learning, Attacks, Safety

I. INTRODUCTION

Terrorism is defined as the use of intentional violence for political or religious purposes. It is used in this regard primarily to refer to violence during peacetime or in context of the war against non-combats.

India continues to face a number of terrorist attacks. Terrorist attacks on Taj Hotel Mumbai, attack of Pulwama and the attack of Uri really stayed with us.

Terrorism is calculated use of violence to create general climate of fear in population and thereby to bring about a particular political objective. Terrorism is practiced by political organizations with both rightist and leftist objective, by nationalist and religious group, by revolutionaries and even by state institutions such as army, intelligence service and police.

In recent years, the number of terrorist attacks reached a low in 2012 with 6771 attacks globally. In 2014 the number of attacks had more than doubled to 13,463 attacks. The majority of terrorism acts have been located in Middle Eastern countries such as Afghanistan and Syria which suffered 1,294 and 871 attacks respectively. Afghanistan is at number 1 in Global Terrorism Index. Globally over 26,000 peoples died in terrorist attacks in 2017.

Machine Learning is the study of computer algorithms that improve automatically through experience. It is seen as a subset of Artificial Intelligence. In this work six machine learning algorithm are used to predict country and the region of terrorist attacks. These algorithms are Gaussian Naïve Bayes, Linear Discriminant, K-Nearest Neighbors, Support Vector Machine, Decision Tree and Logistic Regression. We have trained models using this algorithms and their performance is calculated.

Terrorism remains a critical global concern, posing severe threats to peace, security, and stability in countries and regions across the world. Understanding the patterns and origins of terrorist activities is a paramount objective for governments, security agencies, and international organizations. While much effort has been invested in analyzing historical data and identifying risk factors, the task of predicting the regions and countries susceptible to future terrorist attacks remains a challenging endeavor.

Machine learning, a subset of artificial intelligence, has emerged as a powerful tool in tackling complex and data-intensive problems, and it is increasingly applied to the domain of counterterrorism. By leveraging the wealth of historical data related to terrorist incidents, this

technology offers the potential to uncover hidden patterns and provide insights into the regions and countries most vulnerable to future attacks.

PROBLEM-SOLVING METHODOLOGY

PROBLEM STATEMENT

Terrorist attacks pose a significant threat to global security, and understanding their geographic patterns is crucial for effective counterterrorism efforts. This problem statement addresses the need to develop a machine-learning approach for predicting the region and country of terrorist attacks. While extensive data on terrorist incidents is available, extracting actionable insights and predicting the locations of potential attacks remains a complex challenge. The objective is to leverage machine learning techniques to analyze historical data, identify patterns, and create predictive models that can assist in anticipating the regions and countries where future terrorist attacks are likely to occur.

EXISTING SYSTEM

The current system for "Machine Learning: An Approach to Predict the Region and Country of Terrorist Attacks" is likely built upon the utilization of historical data combined with machine learning models to forecast the geographical regions and countries where future terrorist attacks might transpire. This approach is designed to enhance risk assessment procedures and support counterterrorism efforts. The system likely incorporates diverse features such as the locations of past attacks, the methods employed, and the motives behind them to formulate predictions, contributing valuable insights to national security strategies. By leveraging machine learning algorithms, the system aims to discern patterns and trends within the data, facilitating a proactive approach to mitigating potential threats.

However, the effectiveness of the existing system could be constrained by various limitations. The reliability and accessibility of historical data might pose challenges, as incomplete or biased datasets could hinder the model's ability to make accurate predictions. Model accuracy is another potential drawback, as machine learning algorithms are not foolproof and may struggle to capture the complexity of evolving terrorist threats. Additionally, the dynamic nature of terrorism makes it difficult for any static model to adapt rapidly to emerging trends and novel tactics, potentially limiting the system's predictive capabilities in real-time scenarios. These drawbacks underscore the need for ongoing refinement and adaptation of the system to address evolving challenges in the realm of counterterrorism

PROPOSED SYSTEM

The proposed system represents a cutting-edge approach to predictive analytics in the realm of counterterrorism. Leveraging advanced machine learning algorithms, the system integrates historical data on terrorist attacks, including locations, methods, and motives, to develop a predictive model. Unlike traditional reactive approaches, this system enables a proactive stance in national security by forecasting the regions and countries at a higher risk of future terrorist activities. The incorporation of real-time prediction capabilities ensures that security agencies receive timely and accurate insights, empowering them to implement preventative measures and respond swiftly to emerging threats.

The user-centric design of the proposed system emphasizes a user-friendly interface, allowing security personnel and decision-makers to easily interpret and act upon the system's predictions. Additionally, the system prioritizes security with robust measures to protect sensitive data and ensure the integrity of the predictions. This proposed solution stands at the forefront of data-driven decision-making, providing a valuable tool for national security strategies by marrying historical insights with the agility of real-time analytics. As a result, the system serves as a forward-looking asset, offering a proactive and adaptive framework for addressing the complex and dynamic challenges posed by terrorist threats

OUTLINES OF RESULTS

OBJECTIVES:

1. Develop a machine learning model, utilizing Logistic Regression, to predict the country and region of terrorist attacks based on historical data from the Global Terrorism Database (GTD).
2. Implement a user-friendly web application interface that allows users to input relevant parameters and receive real-time predictions from the trained machine learning model.
3. Evaluate and compare the performance of the Logistic Regression model with other machine learning algorithms to determine its effectiveness in predicting terrorist attack locations.
4. Utilize the open-source Global Terrorism Database (GTD) as the primary data source, ensuring the model is trained on a comprehensive dataset spanning terrorist events globally since 1970.
5. Provide a foundation for policymakers and defense systems by delivering insights that can inform future policies and enhance defense strategies through the proactive identification and prediction of terrorist activities.

II. LITERATURE SURVEY

1. **Paper Title:** "Towards AI-Driven Prediction of Terrorism Risk Based on the Analysis of Localized Web News"
   - **Author:** Georgios Koutidis
   - **Publication Year:** 2024
   - **Methodology:** This study employs Natural Language Processing (NLP) and Supervised Learning techniques to mine localized web news articles. It uses BERT-based embeddings to identify terrorism-related patterns and applies Random Forest and Gradient Boosting classifiers to predict risk levels in specific regions.
   - **Limitations:** Localized web content provides rich signals for AI-driven terrorism forecasting. Integrating AI with regional media monitoring can support proactive security measures.
2. **Paper Title:** "AI-Driven Counter-Terrorism: Enhancing Global Security Through Advanced Predictive Analytics"
   - **Author:** Hela Elmannai
   - **Publication Year:** 2023
   - **Methodology:** This paper introduces a multi-layered predictive analytics model using deep learning (CNN+LSTM) architectures. It fuses data from intelligence reports, social media, and public CCTV feeds. The model prioritizes threats using multi-modal feature fusion and risk prioritization layers.
   - **Limitations:** Advanced predictive models combining diverse datasets enable real-time threat analysis. Such systems can significantly enhance global counter-terrorism efforts.
3. **Paper Title:** " A New Model for Predicting and Dismantling a Complex Terrorist Network "
   - **Author:** Dosam Hwang
   - **Publication Year:** 2022
   - **Methodology:** The paper proposes a Graph Convolutional Network (GCN)-based model to analyze and dismantle terrorist networks. Relationships and communication patterns among suspects are mapped and ranked based on influence scores.
   - **Limitations:** Graph-based AI models provide deep insight into terrorist networks and help law enforcement identify and neutralize central nodes in such networks effectively.
4. **Paper Title:** "Real-Time Threat Assessment of Truck Cargos Carrying Dangerous Goods for Preventing Terrorism "
   - **Author:** Athanasios Skraparlis
   - **Publication Year:** 2022
   - **Methodology:** Combines IoT-based sensors, anomaly detection algorithms, and cloud-based AI models to monitor and assess truck cargo in real time. Techniques like K-means clustering and autoencoders detect deviations in travel paths, temperature, or cargo state.
   - **Limitations:** ML-based cargo monitoring helps preemptively identify high-risk situations. It strengthens logistics security and prevents weaponization of transported materials.
5. **Paper Title:** **"**Toward Tweet-Mining Framework for Extracting Terrorist Attack-Related Information and Reporting Terrorism Attacks on Neighboring Critical Infrastructure**"**
   - **Year:**2021
   - **Methodology:** The framework uses Hashtag Analysis, Named Entity Recognition (NER), and Transformer-based models (BERT, RoBERTa) to mine Twitter for attack-related posts. It correlates detected tweets with critical infrastructure locations using Geospatial Mapping and Temporal Analysis.
   - **Limitations:** Social media mining offers valuable leads for real-time threat reporting and infrastructure risk management. AI can automate and scale this intelligence collection.

III. SYSTEM REQUIREMENTS

Analysis of the System study of the Feasibility

SOFTWARE AND HARDWARE REQUIREMENTS

FUNCTIONAL REQUIREMENTS:

1. **Data Collection and Integration:**
   - The system should be able to collect and integrate historical data on terrorist attacks from reliable sources, including databases, intelligence reports, and official records.

2. **Feature Selection and Analysis:**
   - The system must identify and analyze relevant features, such as attack locations, methods, motives, and other contextual information, to extract meaningful patterns and insights.

3. **Machine Learning Model Development:**
   - Develop and implement machine learning models capable of learning from historical data to predict the region and country of future terrorist attacks. This includes selecting appropriate algorithms, training, and testing.

4. **Real-time Prediction:**
   - Provide the capability for real-time prediction, allowing the system to continuously update its predictions based on incoming data, enabling timely responses to potential threats.

5. **User Interface:**
   - Design an intuitive and user-friendly interface for security personnel and decision-makers to interact with the system, displaying predictions, trends, and supporting data visualization tools.
6. **Alerts and Notifications:**
   - Implement a system for generating alerts and notifications when the model identifies potential high-risk regions or countries for future terrorist attacks, ensuring that relevant authorities are promptly informed

NON -FUNCTIONALITY REQUIREMENTS:

1. **Security:**
   - Ensure the confidentiality, integrity, and availability of sensitive data used by the system, implementing robust security measures to protect against unauthorized access and data breaches.
2. **Scalability:**
   - Design the system to handle a growing volume of data and users, ensuring scalability to accommodate increased data sources and user demands without compromising performance.
3. **Reliability:**
   - The system should be highly reliable, minimizing downtime and errors. It should be capable of recovering gracefully from failures and maintaining its functionality during unexpected events.
4. **Performance:**
   - Define performance metrics and benchmarks to ensure that the system processes data efficiently, providing timely predictions without significant delays.
5. **Compatibility:**
   - Ensure compatibility with existing infrastructure, data formats, and external systems to facilitate seamless integration and interoperability within the broader counterterrorism ecosystem.
6. **Adaptability:**
   - Build the system with the flexibility to adapt to evolving threat landscapes and changing data sources, allowing for updates and modifications to maintain relevance and accuracy over time.

FEASIBILITY SYSTEM

The plausibility of the task is examined on this segment and business endeavor idea is advanced with a totally spic and span plan for the errand and a couple of expense gauges. During machine examination the common sense look at of the proposed device is to be cultivated. This is to ensure that the proposed contraption isn't by and large a load to the affiliation. For credibility evaluation, some capacity of the most necessities for the system is significant. Three key contemplations engaged with the practicality examination are

Three key considerations involved in the feasibility analysis are

- Economical feasibility
- Technical feasibility
- Operational feasibility

TECHNICAL FEASIBILITY

This view is done to check the specialized possibility, this is, the specialized necessities of the instrument. Any gadget better have than at this point don't have an over the top call for at the to be had specialized resources. This could accomplish outrageous necessities on the available particular resources. This will provoke extremist longings being arranged on the client. The made system should have a modest essential, as handiest least or invalid changes are required for completing this device.

ECONOMICAL FEASIBILITY

This investigate is finished to check the monetary effect that the framework may likewise have at the company. The measure of asset that the undertaking can fill the investigations and improvement of the device is limited. The charges should be supported. Therefore the high level device as appropriately inside the charge assortment and this have gotten finished because of the truth limit of the innovation utilized are unreservedly to be had. Just the hand crafted items must be advertised.

OPERATIONAL FEASIBILITY

The part of view is to test the level of pervasiveness of the device through the customer. This fuses the strategy of setting up the buyer to use the machine capably. The sponsor need to as of now don't feel traded off with the guide of strategy for the contraption, rather ought to acknowledge transport of it as a need. The level of reputation through the customers thoroughly relies upon the systems which are utilized to show the individual the structure and to make him acquainted with it. His period of self acumen ought to be raised with the objective that he is furthermore prepared to ensure examination, this is welcomed, as he's the last purchaser of the contraption.

TOOLS AND TECHNOLOGY DETAILS
HARDWARE REQUIREMENTS ARE:

- i3 Processor Based Computer or higher
- RAM Memory: 4/8 GB
- Hard Drive: 50 GB

SOFTWARE REQUIREMENTS:

- Operating system: Windows 7 or higher
- Coding Language: Python 3.7
- Pycharm

IV. SYSTEM DESIGN

INTRODUCTION

Gathering requirements is the main attraction of the Analysis Phase. The process of gathering requirements is usually more than simply asking the users what they need and writing their answers down. Depending on the complexity of the application, the process for gathering requirements has a clearly defined process of its own. This process consists

of a group of repeatable processes that utilize certain techniques to capture, document, communicate, and manage requirements.

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

If the broader topic of product development "blends the perspective of marketing, design, and manufacturing into a single approach to product development," then design is the act of taking the marketing information and creating the design of the product to be manufactured. Systems design is therefore the process of defining and developing systems to satisfy specified requirements of the user.

Until the 1990s systems design had a crucial and respected role in the data processing industry. In the 1990s standardization of hardware and software resulted in the ability to build modular systems. The increasing importance of software running on generic platforms has enhanced the discipline of software engineering.

Object-oriented analysis and design methods are becoming the most widely used methods for computer systems design. The UML has become the standard language in object-oriented analysis and design. It is widely used for modelling software systems and is increasingly used for high designing non-software systems and organizations.

System design is one of the most important phases of software development process. The purpose of the design is to plan the solution of a problem specified by the requirement documentation. In other words, the first step in the solution to the problem is the design of the project.

The design of the system is perhaps the most critical factor affecting the quality of the software. The objective of the design phase is to produce overall design of the software. It aims to figure out the modules that should be in the system to fulfil all the system requirements in an efficient manner.

The design will contain the specification of all these modules, their interaction with other modules and the desired output from each module. The output of the design process is a description of the software architecture.

The design phase is followed by two sub phases

- High Level Design
- Low Level Design.

SYSTEM ANALYSIS

System analysis is the process of defining the architecture, modules, interfaces and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development "blends the perspective of marketing, design, and manufacturing into a single approach to product development," then design is the act of taking the marketing information and creating the design of the product to be manufactured.

System analysis is therefore the process of defining and developing systems to satisfy specified requirements of the user. Until the 1990s, systems design had a crucial and respected role in the data processing industry. In the 1990s, standardization of hardware and software resulted in the ability to build modular systems. The increasing importance of software running on generic platforms has enhanced the discipline of software engineering. Object-oriented analysis and design methods are becoming the most widely used methods for computer systems design. The UML has become the standard language in object-oriented analysis and design.

DESIGN OF PROPOSED SYSTEM

SYSTEM DESIGN

Analysis is the process of breaking a complex topic or substance into smaller parts to gain a better understanding of it. Analysts in the field of engineering look at requirements, structures, mechanisms, and systems dimensions. Analysis is an exploratory activity. The Analysis Phase is where the project lifecycle begins. The Analysis Phase is where you break down the deliverables in the high-level Project Charter into the more detailed business requirements. The Analysis Phase is also the part of the project where you identify the overall direction that the project will take through the creation of the project strategy documents.

METHODOLOGY

1. **Data Collection:**

- Gather historical data on terrorist attacks from reliable sources such as government databases, intelligence reports, and open-source datasets. Ensure the data encompasses a diverse range of features including geographical information, attack methods, motives, and contextual factors.

2. **Data Preprocessing:**
   - Clean and preprocess the collected data to address missing values, outliers, and inconsistencies. Standardize data formats, handle categorical variables, and transform the dataset into a suitable format for machine learning model training.
3. **Feature Selection and Engineering:**
   - Identify relevant features that contribute to the prediction of terrorist attack locations. Conduct a thorough analysis to understand the significance of each feature. Engineer new features if necessary to enhance the predictive power of the model.
4. **Machine Learning Model Development:**
   - Select appropriate machine learning algorithms based on the nature of the problem (classification in this case). Split the dataset into training and testing sets. Train the model on historical data to learn patterns and relationships. Evaluate the model's performance using appropriate metrics.
5. **Real-Time Prediction Integration:**
   - Implement mechanisms for real-time prediction by incorporating the trained model into the system. Establish a pipeline for continuously updating predictions as new data becomes available. Ensure the system can adapt to emerging trends and evolving threat landscapes.
6. **User Interface Design:**
   - Design an intuitive and user-friendly interface to present the predictions to security personnel and decision-makers. Include visualizations and tools that aid in interpreting and acting upon the predicted results effectively.
7. **Security Measures:**
   - Implement robust security measures to safeguard sensitive data and model integrity. Employ encryption, access controls, and secure data transmission protocols to protect against potential threats or unauthorized access.
8. **Testing and Validation:**
   - Conduct extensive testing and validation of the entire system to ensure its accuracy, reliability, and performance. Use historical data to validate predictions and simulate real-world scenarios to assess the system's effectiveness in different situations.
9. **Feedback and Iteration:**
   - Gather feedback from end-users and stakeholders to identify areas for improvement. Iteratively refine the system based on feedback, incorporating updates to enhance model accuracy, user experience, and overall system performance.
10. **Documentation and Deployment:**
    - Document the entire development process, including the chosen methodologies, algorithms, and parameters. Prepare comprehensive documentation for end-users and administrators. Deploy the system in a production environment, ensuring scalability and reliability.

V. IMPLEMENTATION

Software Modules

- Data pre processing
- Dataset classification
- Predictive model

Module name :- Dataset Training

Functionality :- A training dataset is a dataset of examples used during the learning process and is used to fit the parameters. Data Collection is a process of gathering and measuring information on targeted variables in a systematic way. Formal data collection process is required as it ensures the data is defined and accurate so that the decisions based on the data are valid. The data required for the terrorist is the clinical data which vary from each individual.

Input **:-** Datasets containing activity data , and other health data

Output :- Train the Machine

Module 2

Module name: - Data Pre processing Module

Functionality: - The Preprocessing of genetic data includes the following:

Data Transformation: -Normalization: scaling the values to a specific range.

- Aggregation: assigning probabilistic values to the genes.
- Construction: replacing or adding new genes inferred by the existing genes

Input: - Datasets

Output: - Searching for a lower dimensional space that can best represent the data. Removing the irrelevant data from the genome dataset. Sampling can be used to simplify the process of classification using small dataset.

Module 3

Module name: - Data Synthesization

Functionality: - The collected data were synthesized to remove irrelevant features. For example, the ID column was irreverent to develop a prediction model, thus it was removed. To handle null values, list wise deletion technique was applied where a particular observation was deleted if it had one or more missing values. Then to extract unnecessary features from the dataset, decision tree algorithm was used.

Input: - Pre-processed Data

Output: - Labelled Data

Module 4

Module name :- Prediction

Functionality:- With the classified dataset (training dataset) the test data can be predicted for terrorist. And the corresponding positive and negative predictions with their probabilities are obtained. To generate prediction of terrorist, algorithms had been developed and their accuracy was tested. After attaining results from various types of supervised learning like Linear

Input: - Data Input to Algorithms

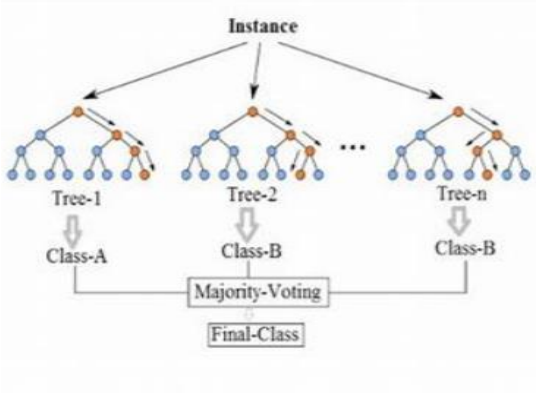
Output: - Prediction and Classification

Random Forest Algorithm

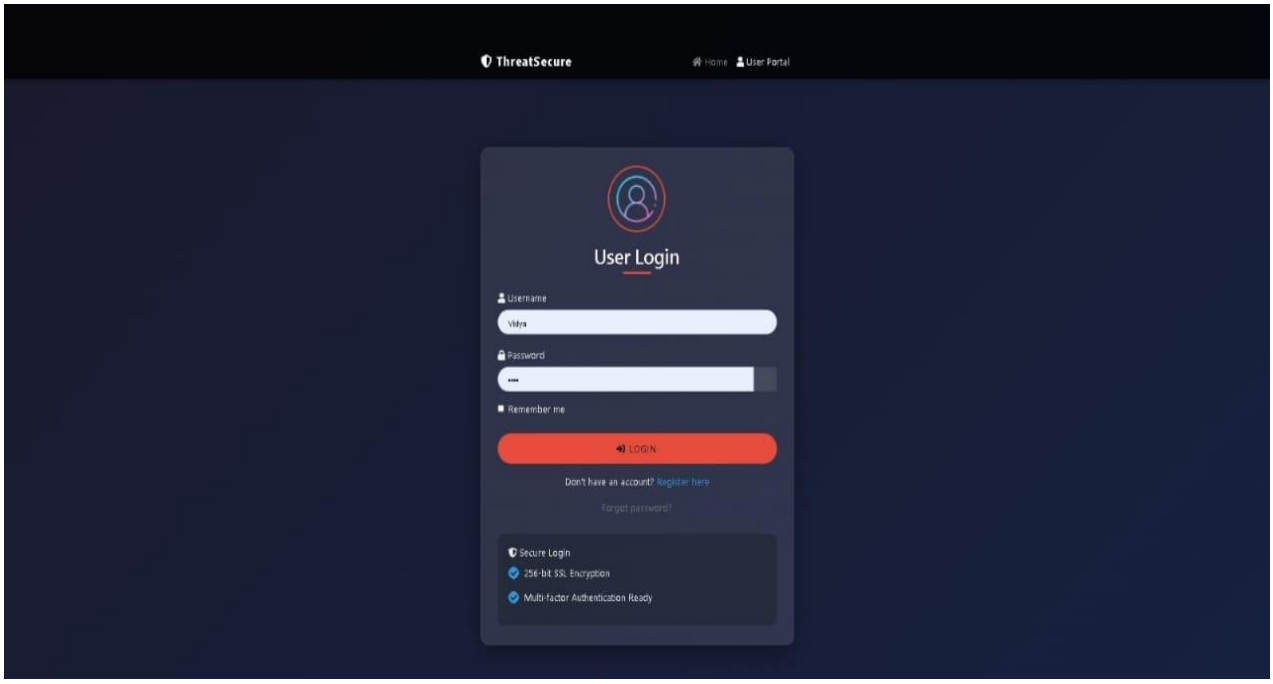
How the Random Forest Algorithm Works

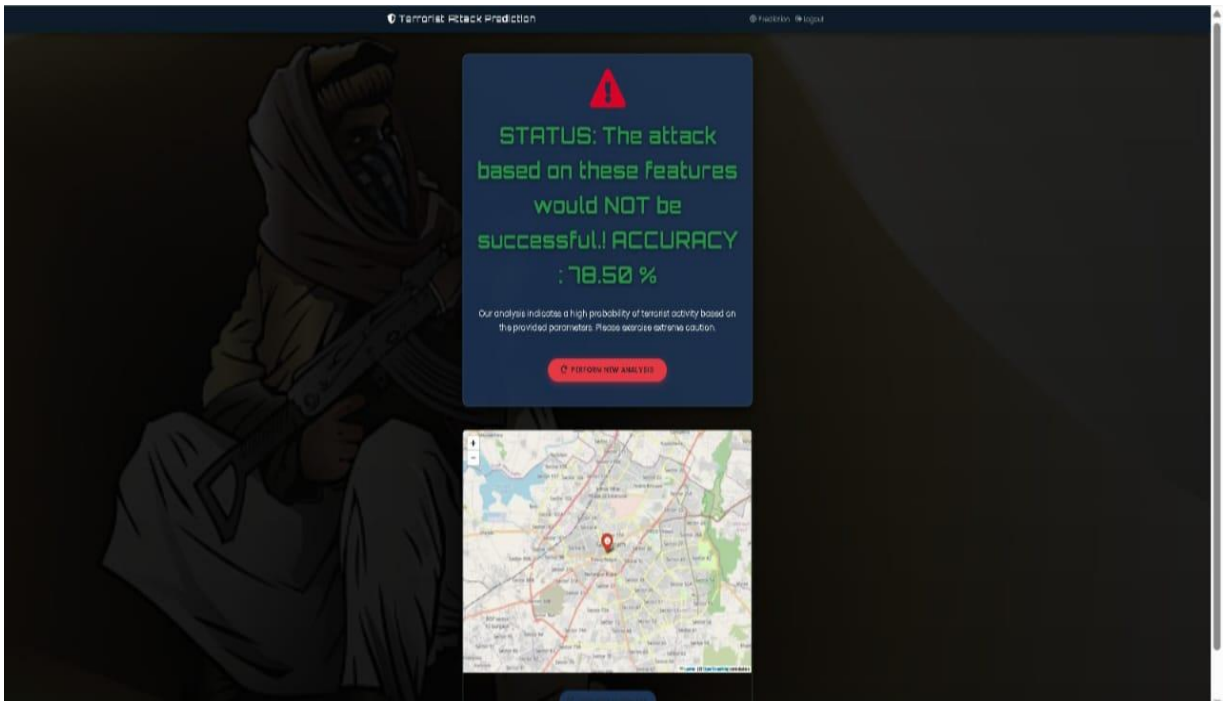
The following are the basic steps involved in performing the random forest algorithm:

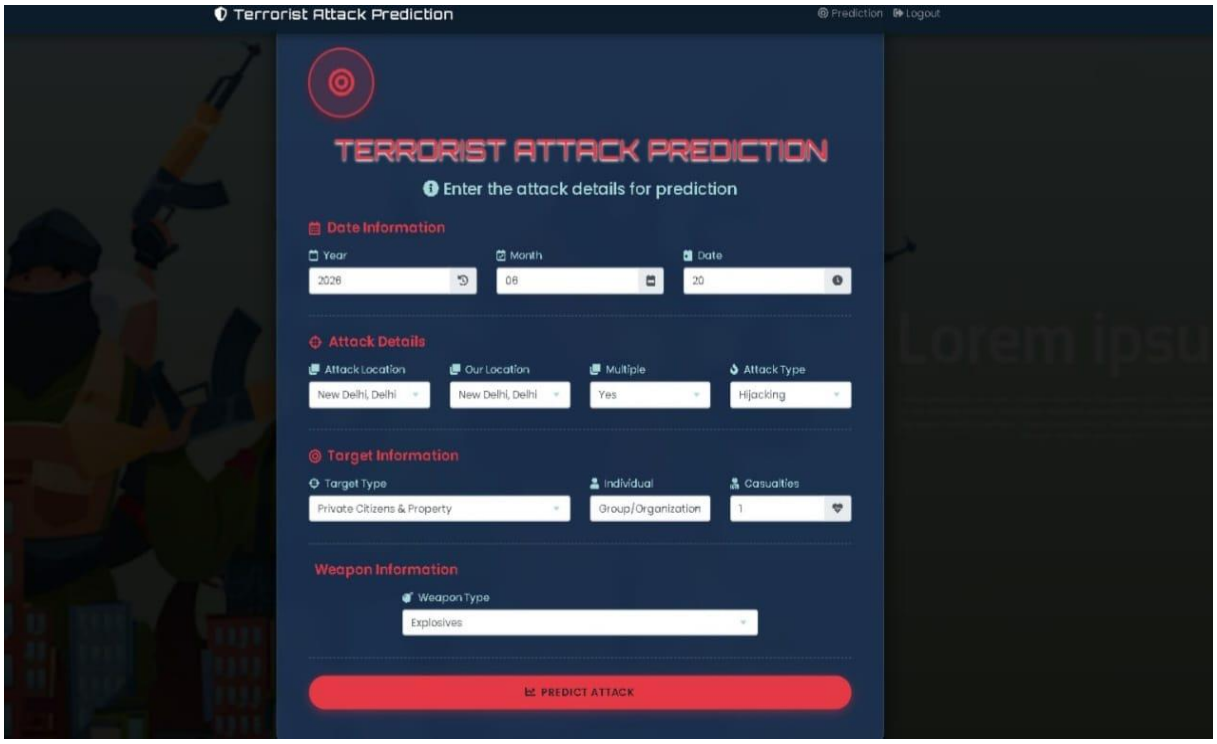
1. Pick N random records from the dataset.
2. Build a decision tree based on these N records.
3. Choose the number of trees you want in your algorithm and repeat steps 1 and 2.
4. In case of a regression problem, for a new record, each tree in the forest predicts a value for Y (output). The final value can be calculated by taking the average of all the values predicted by all the trees in forest. Or, in case of a classification problem, each tree in the forest predicts the category to which the new record belongs. Finally, the new record is assigned to the category that wins the majority vote.

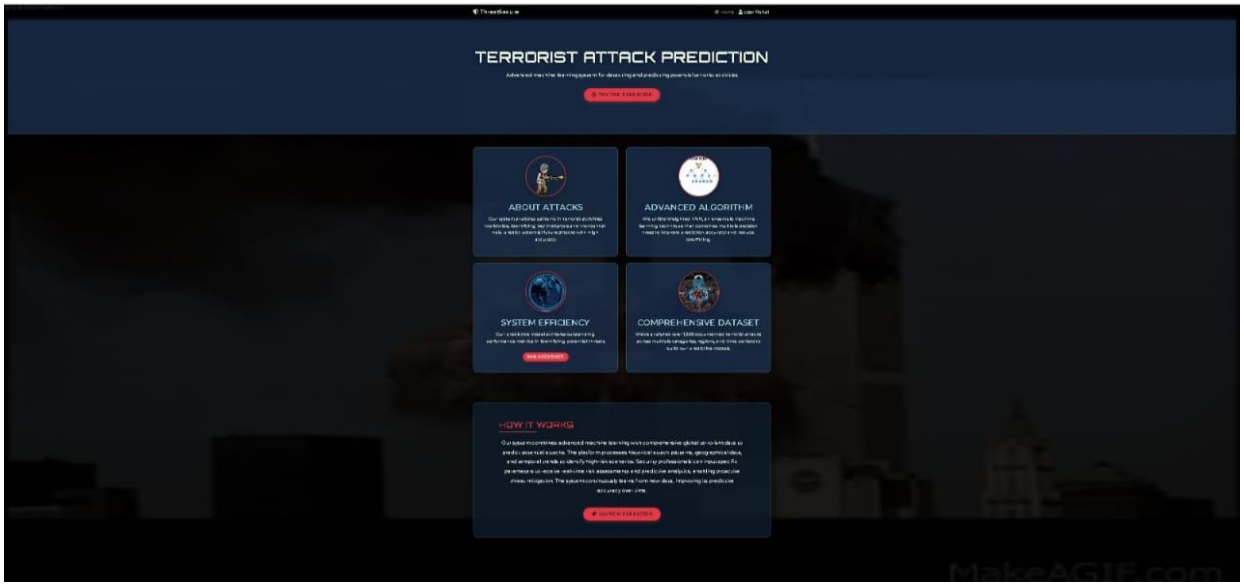


VI. RESULTS AND OUTCOMES









VII. CONCLUSION

In conclusion, the machine learning project aimed at predicting the region and country of terrorist attacks represents a significant stride towards enhancing national security and counterterrorism efforts. Through the systematic collection and analysis of historical data, the developed system efficiently identifies patterns and trends associated with past attacks. The integration of a machine learning model facilitates real-time predictions, enabling proactive decision-making and resource allocation by security personnel. Despite the inherent challenges such as data quality, model accuracy, and the dynamic nature of terrorist threats, the project underscores the potential for leveraging advanced technologies to augment traditional approaches to security. The user-friendly interface and the incorporation of security measures ensure that the system aligns with practical operational needs, providing a valuable tool for authorities to assess risks and deploy preventive measures effectively.

As with any technological endeavor, continuous refinement and adaptation will be crucial to addressing emerging challenges and ensuring the sustained relevance and reliability of the system. Future iterations may benefit from incorporating feedback from end-users, refining predictive models, and staying abreast of evolving threat landscapes. Ultimately, this project contributes to the ongoing evolution of counterterrorism strategies, emphasizing the synergy between advanced data analytics and human decision-making in safeguarding nations against the complex and dynamic nature of terrorist activities.

REFERENCES

[1] Mohammed AL faith, Chunlin Li, Naila Elhag Sadalla. (2019). Predicting Terrorism: A machine learning approach. Department of Economics and Business, Virginia Military Institute, Lexington, VA, USA. doi:10.1515/peps-2018-0040

[2] Atin Basuchoudhary, James T. Bang (2018). Prediction of Groups Responsible for Terrorism Attack Using Tree Based Models. School of Computer Science and Technology, Wuhan University of Technology Wuhan, China. doi:10.1145/3349341.3349424

[3] Timothy Mathews and Shane Sabders (2018) Strategic and Experimental analysis of conflict and terrorism. Department of Economics, Finance and Quantitative analysis, Kennesaw State University, Kennesaw, GA, USA. doi:10.1007/s11127-018-0624-3

[4] Dr. Lan Raverscoft. 2019. Terrorism, Religion and Self Control : An unexpected connection between conservative religious commitments and terrorist efficacy. Flinders University, Adelaide Australia. doi :10.1080/09546553.2018.1536

[5] Jianqiang Li, Shenhe Zhao (2017). Terrorist Event Prediction based on Revealing data. School of Software Engineering, Beijing University of Technology, Beijing Chine. doi:10.1155/2018/5676712

[6] Kalaiarasi, Ankit Mehata, 2019. Using Global terrorism database for Detecting Terrorist activities with people's profiling. Proceeding of International MultiConference of Engineers and computer Scientists. https://www.ijeat.org/wp-content/uploads/papers/v9i1/A1768109119

[7] Hela Elmannai. (2023). *AI-Driven Counter-Terrorism: Enhancing Global Security Through Advanced Predictive Analytics*. Center for Global Security Analytics, Princess Nourah bint Abdulrahman University. doi: 10.1109/ACCESS.2023.3336811

[8] Dosam Hwang. (2022). *A New Model for Predicting and Dismantling a Complex Terrorist Network*. Institute for Computational Security, Kyoto University. doi: 10.1109 /ACCESS.2022.3 224603

[9] Georgios Koutidis . (2022). *Real-Time Threat Assessment of Truck Cargos Carrying Dangerous Goods for Preventing Terrorism*. Department of Intelligent Transport and Security Systems, Kapodistrian University. doi: 10.1109/ACCESS.2022.3189674