ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul232

A Pipeline-Based Approach for Enhancing Political Threat Detection Using Machine Learning

Chandra Sekhar Sanaboina[1]

[1]Assistant Professor Department of Computer Science and Engineering University College of Engineering Kakinada JNTUK - Kakinada

Publication Date: 2025/07/10

Abstract: Especially on social media and other online platforms, the internet provides a strong venue for the expression of ideas, feelings, and views. The public's sentiments are frequently reflected in these internet messages, which, if unregulated, might cause major problems like rioting or instability, which could affect the safety of the country. In order to avoid any security issues, it is essential to monitor such emotions. A novel approach to predicting political security threats is presented in this project. It combines two methods: (i) lexical analysis, which involves searching for words that typically convey strong emotions like anger or fear, and (ii) machine learning, which involves training computers to identify patterns in data in order to improve threat prediction. Examining online material for emotional content using classifiers such as Decision Tree, Naive Bayes, and Support Vector Machine (SVM) allows the method to detect and anticipate indications of instability. From data processing to prediction, the whole process is automated in this project thanks to the establishment of a pipeline. The data cleaning, model training, and prediction processes are all integrated into one streamlined flow thanks to scikit-learn. To improve outcomes, the project intends to test different algorithm combinations within the pipeline and see which ones work best. In order to avert political instability, it efficiently analyzes internet messages for indicators of disturbance and allows authorities to take swift action.

Keywords: *Political Threat, Machine Learning, Security, Lexical Analysis, Decision Tree, Support Vector Machines, Naïve Bayes, Pipeline Based Approach Social Media Platforms.*

How to Cite: Chandra Sekhar Sanaboina; (2025) A Pipeline-Based Approach for Enhancing Political Threat Detection Using Machine Learning. *International Journal of Innovative Science and Research Technology,* 10(7), 189-198. https://doi.org/10.38124/ijisrt/25jul232

I. INTRODUCTION

The internet, empowered by smartphones and high-speed connectivity, has emerged as a dominant medium for expressing political opinions and public sentiment. Given the textual nature of most online content, monitoring and analyzing these sentiments is critical to identifying extreme emotional expressions that may incite national security risks, including riots and political unrest. The previous research proves that there is a close association between online emotions and political dynamics of threat, and thus the necessity of a proper sentiment analysis mechanism and threat analysis device is emphasized [1]. In a bid to curb the same, this paper has suggested a pipeline-based hybrid system that integrates lexicon-based analysis of emotions with supervised machine learning engines like Decision Tree, Naive Bayes and Support Vector Machine (SVM). Threat detection models are made much more accurate and interpretable when decision-based learning is combined with tools like NRC Emotion Lexicon, WordNet, CentiWordNet, and many others. [1].

Along with political attitude, online resources also promote hate speeches and racial discrimination that may also destabilize societies. GRU-based models have also been traced in deep learning frameworks like the Gated Convolutional Recurrent Neural Network (GCR-NN) which has layers of GRU, convolutional, and recurrent neural networks; they have demonstrated their efficiency in identifying offensive or hostile texts in social media posts [2]. Moreover, sentiment analysis has been also utilized to gauge geopolitical risks by analyzing texts of resolutions adopted by the organization, where it is possible to cast a wider scope of political risks [3]. In darker digital space such as the Dark Web, cyber criminals do activities that are hard to follow. The systematic literature reviews endorse the deployment of better forensic and analytical tools to minimize the threat in such spaces [4]. In addition to this, in an age of natural language generation tools, the boundary between what. A person wrote and something that was generated by a computer is becoming more ambiguous, conjuring up yet additional worries over misinformation and manipulation [5]. These emerging forces require any systematic, smart pipeline that can detect and handle direct and indirect political threats in digital ecosystems.

II. LITERATURE REVIEW

With the help of smartphone and continuous connections, the internet became one of the dominant platforms upon which the public share opinions and emotions. Considering that the majority of this information is textual, it is crucial to monitor sentiment so as to detect an overload of sentimental expressions which could be indicative of such security threats as riots or civil unrests as far as political security is concerned. Scientists have shown the close linkage between emotions, sentiment and political instabilities and it is important to have advanced opinion-mining methods. One possible solution to this issue is to implement a hybrid architecture that combines lexical and machine learning-based classifiers such as Support Vector Machine, Naive Bayes, and Decision Tree. In terms of forecasting a political danger in cyberspace, the best accurate predictions were generated by combining the Decision Tree classifier with the lexicon-based technique, according to the experiment results [1].

Racism has also become so rampant in the social media since it is not limited to ethnicity, but is also based on color, religion, language and culture. Racism reveals itself directly in the form of hate speech and indirectly in the form of memes and codes of language, which often cause violence and instability. Such content is difficult to detect with the use of powerful sentiment analysis models. Gated Convolutional Recurrent Neural Network (GCR-NN) is a framework that was applied regarding identifying and filtering racist content on such platforms as Twitter because of its integrations related to Gated Recurrent Units (GRU), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) [2]. On the same note, sentiment analysis has also been used to interpret international relations such as in the analysis of NATO Parliamentary Assembly resolutions to understand the change in the nature of the indirect threats over the years; thus providing a leverage on understanding the global behavior and patterns of conflict [3].

The Dark Web is another highly dangerous sphere of concern where cybercriminals, terrorists, and hackers operate and cannot be easily traced. The Dark Web is so anonymous and huge that it is difficult to monitor illegal activity and even combat it. The analysis of 65 studies among the most crucial databases carried out within the framework of the Systematic Literature Review discloses the character of these developing cyber threats and their socio-economic impact. The review singles out, among others, the necessity of improved and more sophisticated forensics tools, forums/crypto market supervision, and the harmonization of digital evidence practice with the framework of law [4]. Also, as Natural Language Generation (NLG) such as ChatGPT is being increasingly advanced, it has become a necessity to detect machine-generated text to avoid misinformation and manipulation. An extended survey provides descriptions of threat models associated with NLG systems and examines detection techniques with emphasis on detection systems that enhance accountability, trustworthiness, and adversarial resiliency [5].

Security threats in cyber space also have become a burning issue in advanced technologies such as self driving cars. The current threat detection models, such as the traditional Generative Adversarial Networks (GANs), have limitations in detecting advanced encroachment, including data tampering. A better form of GAN model has been designed to produce data more in line with reality to enhance detection of threats in the car networks, and this model has shown better performance in accuracy and reliability whenever compared to old models [6]. Yet, in network traffic analysis, the application of the traditional graph-based models is ineffective to spot the new or low-data threats. To bypass this, authors proposed the fine-grains approach to detecting behavior with the use of flow semantic structure and the topology mapping to isolate behavioral characteristics. The method has proved more accurate and flexible even through there is less training data [7][8].

Threat detection in IoT and other dedicated industries such as healthcare and satellite communication is essential. An example is the HSPFSID model in the healthcare IoT environment which employs ensemble learning and a novel feature selection process that is based on the activities of pigeons whose performance in intrusion detection is exceptional [9]. The LAN model can feasibly prevent insider attacks in the real-time setting since the graph structure learning method has shown high accuracy on benchmark datasets due to modeling the temporal dependency and addressing the problem of data imbalance [10]. The Deep Federated Learning (DFL) and Variational Autoencoders (VAEs) have also been used in satellite communications to enhance anomaly detection by preserving the confidentiality of data and providing explanations of models by using SHAP values [11]. Additionally, the DNNLSTM model, because of the ability advanced by deep learning compared to other conventional classifiers stands a better fit in detecting both frequent and less frequently occurring threats in IoT networks [12].

Stealthy malwares that optimally assume profiles of normal activity have been countered with intelligence systems such as Anteater to track anomalies in the normal activities of the network by profiling normal network activities. This method has shown to be able to detect intrusion of malware infections with near zero false positives in practical enterprise settings [13]. Another approach that has been incorporated to identify insider threats is through the Graph Neural Networks (GNNs) that employed models, such as MEWRGNN, to examine the behaviour of the users over time to rank how each feature contributed towards a better understanding and accuracy prediction [14]. Other proposals such as applying the Isolation Forest algorithm perform very well when provided with an imbalanced dataset, and they have also demonstrated good performances in insider threat detection on the CERT data sets [15]. In ADAS, uncertainty in the prediction may be directly used to enhance the reliability of threat detection when there is noise or uncertainty in the detection itself and this result has been demonstrated across ADAS applications [16].

Composite models that comprise stream and batch learning methods have been put forward to deal with the issue of insider threats in dynamic setting. Such frameworks combine semi-supervised learning with stream analysis of data and regular retraining, and methods such as Isolation Forest are found to perform the best [17]. In the case of IoT Edge in which targets require low latency and data imbalance, models based on Enhanced Geometric SMOTE (EG-SMOTE) and better Growing Self-Organizing Maps (GSOM) provide an efficient and real-time threat detection mechanism based on learning unlabeled data streams [18]. A second way of identifying insider threats is unlabeled data representations based on unsupervised learning ensembles that can identify the insider threat based on unlabeled data with minimal false positives [19]. The development of dynamic directed multigraph models with a proactive approach to the fight against misinformation is presented to analyze the user embedding trajectory on such platforms as Twitter. It permits early identification of misinformation operations and restricts threats prior to their development, as compared to where they could be detected conventionally after occurrence of an incident [20]. Growth in the speed of fake news transmission on social networks causes problems of misinformation, political polarization and morality. Discovering fake news is the key to maintaining information integrity. Using textual and visual data, this work introduces an ensemble learning-based method for multi-modal false news identification. Using the Fakeddit dataset (over a million samples), [21]the method applies Natural Language Processing (NLP) for text preprocessing and sentiment analysis. Visual Bidirectional Encoder Representations from Transformers (V-BERT) generate embeddings for both text and images, which are then processed by a deep learning ensemble model. A 10-fold evaluation technique validates the model's effectiveness, showing significant improvements over existing detection methods.Natural Language Processing (NLP) is evolving with the rise of pre-trained Large Language Models (LLMs) based on Transformer architectures. With increasing cybersecurity threats, accurate incident detection in IoT networks is essential. [22] introduces SecurityBERT, a novel cyber threat detection model leveraging Bidirectional Encoder Representations from Transformers (BERT) for IoT security. To enhance privacy, it integrates Privacy-Preserving Fixed-Length Encoding (PPFLE) with Byte-level Byte-Pair Encoding (BBPE) Tokenizer for structured network traffic representation. Experimental analysis using the Edge-IIoTset dataset shows that SecurityBERT outperforms traditional Machine Learning (ML) and Deep Learning (DL) methods, including CNNs and RNNs. With low inference time and a compact model size, SecurityBERT is optimized for real-time traffic analysis on resource-limited IoT devices.

[23] Insider threat identification is a hard task in business and government organizations owing to imbalanced data, limited ground truth, and dynamic user behavior. Malicious insider assaults constitute a big concern in these settings. This research proposes a machine learning-based system that conducts multi-level data analysis to detect both malicious behaviors and insiders under realistic conditions. It examines common insider threat scenarios and evaluates detection performance using multiple metrics. since a consequence, security analysts now have more information to work with when analyzing insider risks, since the system can learn from sparse ground truth, discover new malevolent insiders in hidden data, and allow fast threat identification.

III. DATASET-SET DESCRIPTION

The dataset india-news-headlines.csv includes 1,048,575 news headlines, their dates of publication and labels of categories. On it, there are three columns: publish_date in YYYYMMDD format, headline_category that is now identified as unknown, and headline_text where the actual news headlines are placed. The database is inter-annual, contains text-intensive information of use to such activities as sentiment analysis, emotion classification, topic modeling, and political threat analysis. It is large and hence suitable to train and test models of machine learning in NLP.

IV. THEORETICAL FRAMEWORK / PROPOSED METHODOLOGY

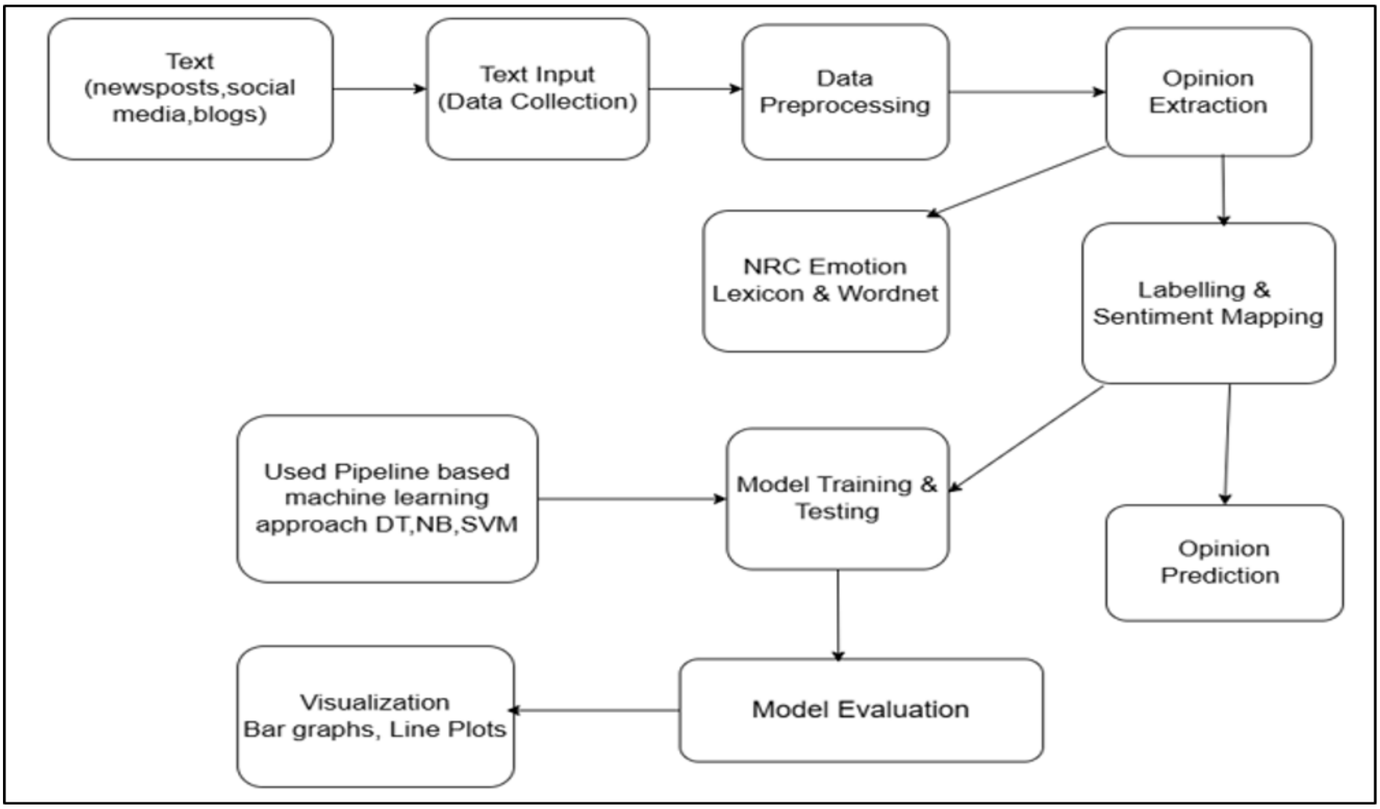

Text (newsposts,social media,blogs)
Text Input (Data Collection)
Data Preprocessing
Opinion Extraction
NRC Emotion Lexicon & Wordnet
Labelling & Sentiment Mapping
Used Pipeline based machine learning approach DT,NB,SVM
Model Training & Testing
Opinion Prediction
Visualization Bar graphs, Line Plots
Model Evaluation

Fig 1 Workflow of the Proposed System

- *Data Collection*

The system starts with the data extraction of political news where the main interest is headlines or piece of note of the articles. The short texts suit well to the analysis of emotions and sentiments as, in many cases, they convey highly emotional or emotional response. The information is obtained through reputable Malaysian news agencies including the Star, New Straits Times and Free Malaysia Today. The gathering is either done by hand or done with automated web scraping software. This aim is to achieve a positively representative data that calls into consideration the prevailing political events and moods. Single sentences or headlines are common as a single record, paving the way to a detailed and narrowed study of emotional and political cues.

- *Data Preprocessing*

A preprocessing process is performed in order to make the text data ready to analyse. This would be done by starting with changing everything to lower case so as to keep everything same, with no sensitivity to paragraph written in small case or capital letters. The punctuation marks, special characters, numbers, and the URLs are filter out, and these details do not usually add to the process of emotion or sentiment detection. Common words which are of low semantic value like: is, the, and are also excluded as they are stop words. The last involves tokenisation which splits the sentences into individual words or the token. This produces a clean,ordered data lying in line with linguistics and machine learning tasks.

- *Emotion Detection Using Lexicons and Semantic Resources*

In order to identify emotional signals in the text, several tools based on lexicon and semantics are incorporated in the system, NRC Emotion Lexicon, WordNet, and CentiWordNet. Emotion Emotion Words The NRC Emotion Lexicon is detailed mapping of words to eight primary emotions - anger, fear, anticipation, trust, surprise, sadness, joy, and disgust, along with binary sentiment values (positive and negative). Any word in the sentence is matched with this lexicon and in case it is represented, emotional values are noted.

In order to make the process of emotion detection even more advanced, WordNet, a large English-based lexical database, is used to retrieve the synonyms, hypernym and related forms of each token. This extends the range of the emotional associations to cover terms that are semantically similar to those directly in the list of terms of the NRC lexicon. As an extension, Sentiment-marked extensions of wordnet such as CentiWordNet are employed to compute polarity scores of words, which allow selection of positive and negative sentiments in a more subtle fashion. With the advantage of relative strengths provided by predefined emotion dictionaries and semantic richness offered by the resources based on WordNet, the system recognizes emotions more accurately in a context-sensitive manner. The emotion and sentiment scores of aggregated emotion and sentiment scores at sentence level are used with respect to inference of the emotional tone, as well as to detection of possible threats.

➢ *Sentiment Labeling*

Once the extraction of emotion features is done, the individual sentences are then assigned either Positive or Negative labels according to the strength of emotional hints. The type of sentences showing such emotions as joy, trust, or anticipation is characterized as Positive, which means that this is not a threatening or negative situation. On the contrary, sentences matching fear, anger or disgust are marked as Negative indicating that a political tension or turbulence might be coming. This categorization algorithm transforms the mission into a binary classification problem and the emotion-tinted sentiment to be a class designator of supervised classes of machine learning models.

➢ *Feature Extraction Using TF-IDF*

To make machine learning a possibility, the text will have to be digitalized. It is done through the Term Frequency-Inverse Document Frequency (TF-IDF) approach. TF-IDF measures the weight of each word according to how often it occurs in a specific sentence and how uncommon it would be throughout the whole data set. Words used in one sentence often and unusual in the rest of the texts are used as more informative. The output is a feature vector that represents each sentence numerically, highlighting its most distinctive words. In order to train classification algorithms, these vectors are used.

➢ *Machine Learning Algorithms for Classification*

The system employs Decision Tree (DT), Naïve Bayes (NB), and Support Vector Machine (SVM) as supervised machine learning methods to categorize political material as either hostile or non-threatening.

- *Decision Tree:*

In order to make decisions, the Decision Tree algorithm uses feature values to build a structure like a tree. There are nodes at the root of the data set that stand for conditions, and nodes at the branch ends that stand for classification results. Decision Trees are easy to understand and visualize, making them highly interpretable, especially for rule-based text classifications

- *Naïve Bayes:*

It is assumed that features are independent in the Naïve Bayes classifier, a probabilistic model that employs Bayes' theorem. Based on the sentence's word distribution, it determines the likelihood of each class. Naïve Bayes is particularly well-suited for text data because it performs efficiently on high-dimensional inputs like TF-IDF vectors and yields reliable results when classifying sentiment or emotion.

- *SVM:*

To function, the Support Vector Machine (SVM) algorithm seeks for the hyperplane that most effectively divides data points into their respective classes. It excels at high-dimensional, sparse datasets and is ideal for binary classification jobs. In the context of political text analysis, SVM helps to distinguish clearly between content that may pose a threat and that which does not.

Each model is trained using the labeled TF-IDF vectors and evaluated for performance. Depending on the context and accuracy requirements, the best-performing classifier can be selected for real-time prediction and deployment.

➢ *Prediction on New Text Samples*

Once trained, the machine learning models are used to predict the sentiment of new and unseen political text samples. These may include recent news headlines, political speeches, or user-generated social media posts. Every new sentence is passed through the entire pipeline, preprocessing, lexicon-based emotion detection, TF-IDF feature extraction, and finally, classification. The system outputs a sentiment label: Positive (safe) or Negative (potential threat). This prediction enables the early identification of potentially destabilizing content in political discourse and can serve as a decision-support tool for analysts and policymakers.

➢ *Pipeline-Based Approach with Combined Algorithms*

The system uses a pipeline structure where different steps like cleaning the text, extracting features, and classifying the data are carried out one after another in a fixed sequence. To improve accuracy, the system combines two or more machine learning algorithms within this pipeline.

- **SVM + Naive Bayes:** SVM separates the data, and Naive Bayes refines the output using word probabilities.
- **Naive Bayes + Decision Tree:** Naive Bayes classifies quickly, while the decision Tree adjusts results using rules.
- **Decision Tree + SVM**: The Decision Tree splits data, and SVM improves accuracy within each group.
- **All-in-One Pipeline**: Combines all three models in sequence or through voting, improving stability and accuracy.

➢ *Performance Metrics*

- *Accuracy*

To find the model's overall performance, we may look at its accuracy, which is defined as the percentage of positive and negative cases that were properly identified out of all the predictions. While it serves as a good overall performance measure, it could fall short in cases when there is a large class imbalance in the dataset. A model may get good accuracy by only projecting the majority class, for instance, in a dataset where one class is much more prevalent than the other. Accordingly, accuracy is crucial, but it has to be considered alongside other metrics for proper interpretation.

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN)$$

- *Precision*

One way to evaluate a model's performance is by looking at its precision, which is another name for positive predictive value. It shows us what proportion of good things happen that are really good. This figure takes on even more significance in settings where the cost of false positives is substantial, such in the detection of disinformation or cybersecurity. In these cases, the wrongly labeling of typical activity as a danger might result in needless actions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul232

Precision = TP / (TP + FP)

- *Recall*

The accuracy with which the model identifies all genuine positive instances is quantified by its recall, sensitivity, or true positive rate. The importance is especially in the cases where missing of a positive example (false negative) may have any severe repercussions- failing to identify an actual political threat or a vital security breach. When the value of recall is associated with a high value, it tends to portray that the model has the ability to capture as many true positives as possible.

Recall = TP / (TP + FN)

- *F1-Score*

An F1-Score, which is a harmonic mean of recall and accuracy, provides a fair assessment of the model's ability to generate accurate positive predictions. It shines in situations when class distributions aren't uniform and where a balance between recall and accuracy is required. Contrary to accuracy, F1-score does not imply one or the other any false positives or false negatives, and therefore it is the most suitable to test on those models that should be used in the real world where there are serious consequences of false negative and positive errors.

F1-Score = 2 × (Precision × Recall) / (Precision + Recall)

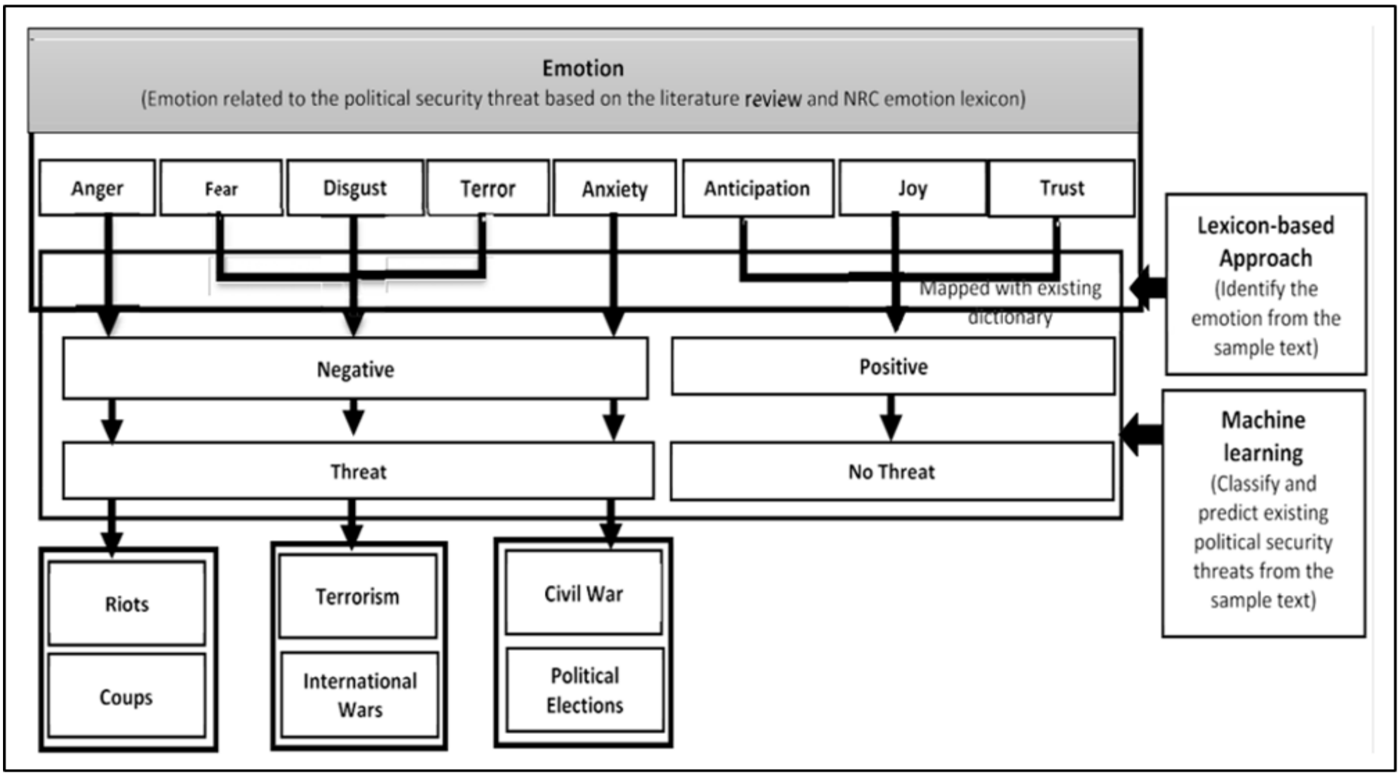

Emotion
(Emotion related to the political security threat based on the literature review and NRC emotion lexicon)
Anger
Fear
Disgust
Terror
Anxiety
Anticipation
Joy
Trust
Mapped with existing dictionary
Lexicon-based Approach (Identify the emotion from the sample text)
Negative
Positive
Threat
No Threat
Machine learning (Classify and predict existing political security threats from the sample text)
Riots
Coups
Terrorism
International Wars
Civil War
Political Elections

Fig 2 Theoretical framework for predicting political security threats using a combination of lexicons and machine learning [1]

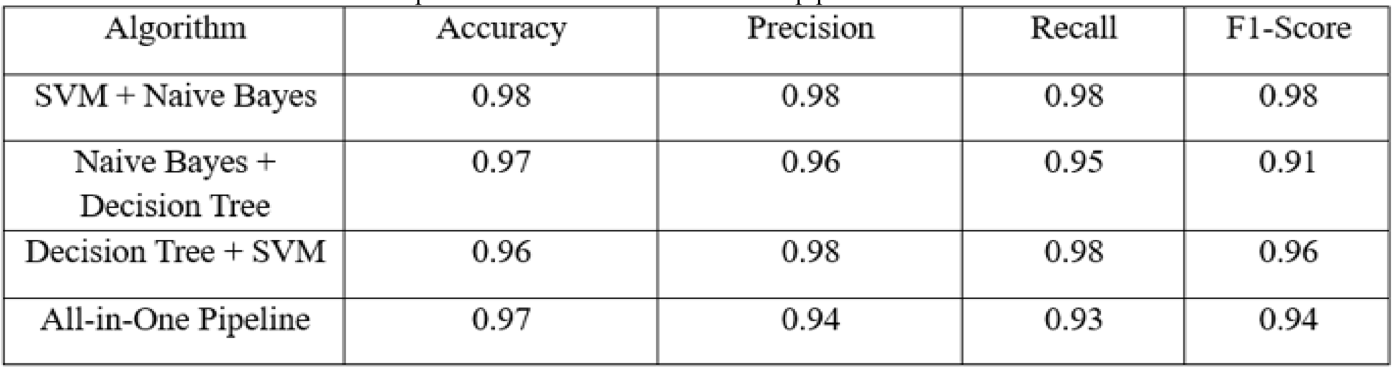
V. RESULTS AND ANALYSIS

Table 1 Comparison of Performance for various pipeline models with NRC

Algorithm	Accuracy	Precision	Recall	F1-Score
SVM + Naive Bayes	0.90	0.89	0.89	0.89
Naive Bayes + Decision Tree	0.85	0.87	0.85	0.85
Decision Tree + SVM	0.89	0.89	0.89	0.92
All-in-One Pipeline	0.94	0.93	0.93	0.94

As the comparison of the models shows, All-in-One Pipeline demonstrates a better performance than other combinations in all the measures of determining the performance in all the aspects of evaluation and, therefore, this method can be viewed as highly effective and balanced way of inculcating into the process of classification. Naive Bayes and SVM combination is also proven to be very strong most of the time indicating a stable synergy between the two algorithms. Although the other hybrid models-Naive Bayes with Decision Tree and Decision Tree with SVM are moderately effective, they seem to be not so consistent and this can be because such models are sensitive to data features. Overall, the findings point out the All-in-One pipeline as the most scalable and robust to detect threats precisely and reliably.

Table 2 Comparison of Performance for various pipeline models with Wordnet



Algorithm	Accuracy	Precision	Recall	F1-Score
SVM + Naive Bayes	0.98	0.98	0.98	0.98
Naive Bayes + Decision Tree	0.97	0.96	0.95	0.91
Decision Tree + SVM	0.96	0.98	0.98	0.96
All-in-One Pipeline	0.97	0.94	0.93	0.94

The relative assessment of the combinations of the hybrid models shows that SVM and Naive Bayes combination showed the most consistent and best performance in every assessment, which shows that the combination is strong in its classification and serves both with good precision and recall competency. Decision Tree and SVM model manages to perform the same, especially in precision and recognition but lower in accuracy and F1-score. The Naive Bayes and Decision Tree combination compares favorably in terms of the level of accuracy but it indicates a significant decrease in F1-score, which indicates an imbalanced precision and recall. The overall performance is pretty high with the All-in-One Pipeline, but it is slightly lower in precision and recall suggesting a more generalized and slightly less specific classification behaviour. In general, the best combination which should be considered the most effective and reliable one is the SVM + Naive Bayes model.

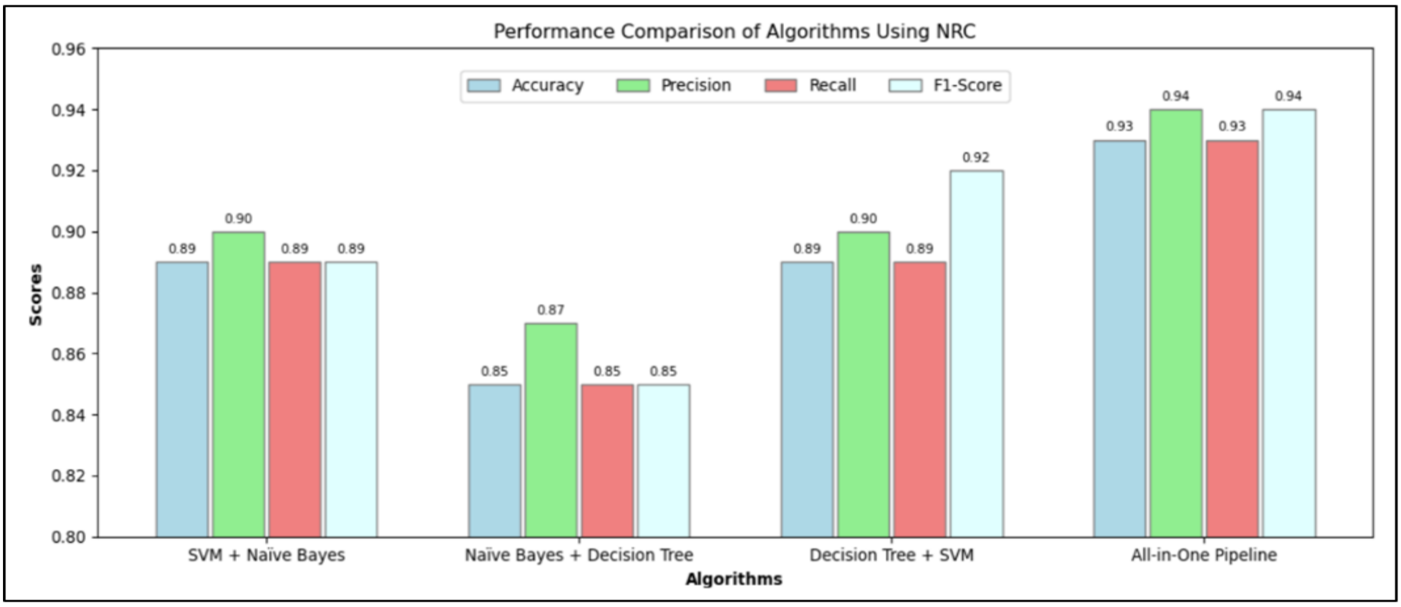


Fig 3 Performance evaluation of various pipeline models with NRC

The bar graph shows how four different algorithmic combinations performed when tested using the NRC Emotion Lexicon. These combinations were SVM + Naïve Bayes, Naïve Bayes + Decision Tree, Decision Tree + SVM, and All-in-One Pipeline. The All-in-One Pipeline stands out with the highest overall scores (Accuracy: 0.93, Precision & F1: 0.94, Recall: 0.93), indicating its superior effectiveness in capturing and classifying emotional signals. While Decision Tree + SVM also performs well, especially in F1-Score (0.92), Naïve Bayes + Decision Tree shows the lowest metrics across the board. This comparison emphasizes that integrating multiple models in a single pipeline boosts classification performance, especially in emotion-based political threat detection.

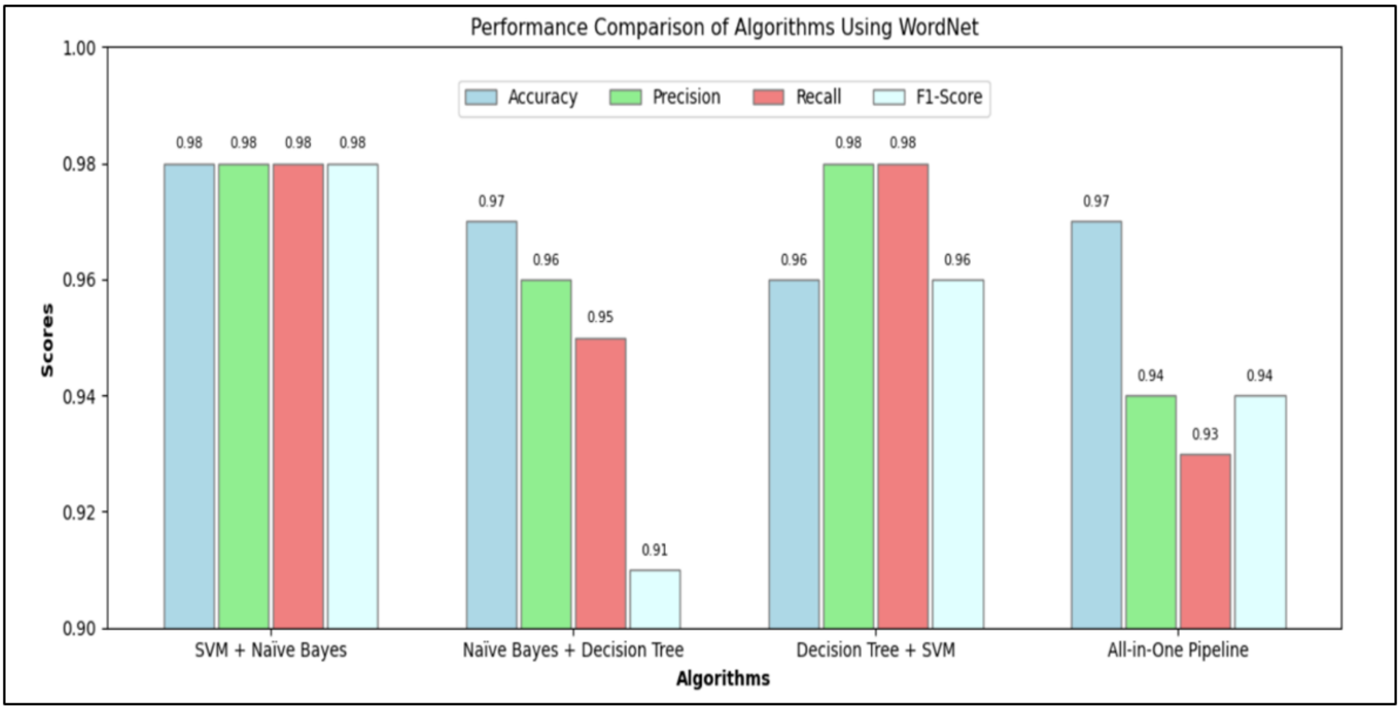


Fig 4 Performance evaluation of various pipeline models with Wordnet

This bar graph shows the results of four different algorithm combinations that were tested using WordNet features: SVM + Naïve Bayes, Naïve Bayes + Decision Tree, Decision Tree + SVM, and All-in-One Pipeline. The algorithms were assessed using Accuracy, Precision, Recall, and F1-Score. The SVM + Naïve Bayes combination achieves perfect balance with all metrics scoring 0.98, indicating high consistency and reliability. Decision Tree + SVM also performs strongly in Precision and Recall (0.98), though its Accuracy and F1-Score are slightly lower at 0.96. Naïve Bayes + Decision Tree shows a drop in Recall and F1-Score (0.95 and 0.91), while the All-in-One Pipeline achieves decent Accuracy (0.97) but slightly lower Precision and Recall. In terms of sentiment-driven threat identification using WordNet, the most successful combination seems to be SVM + Naïve Bayes.

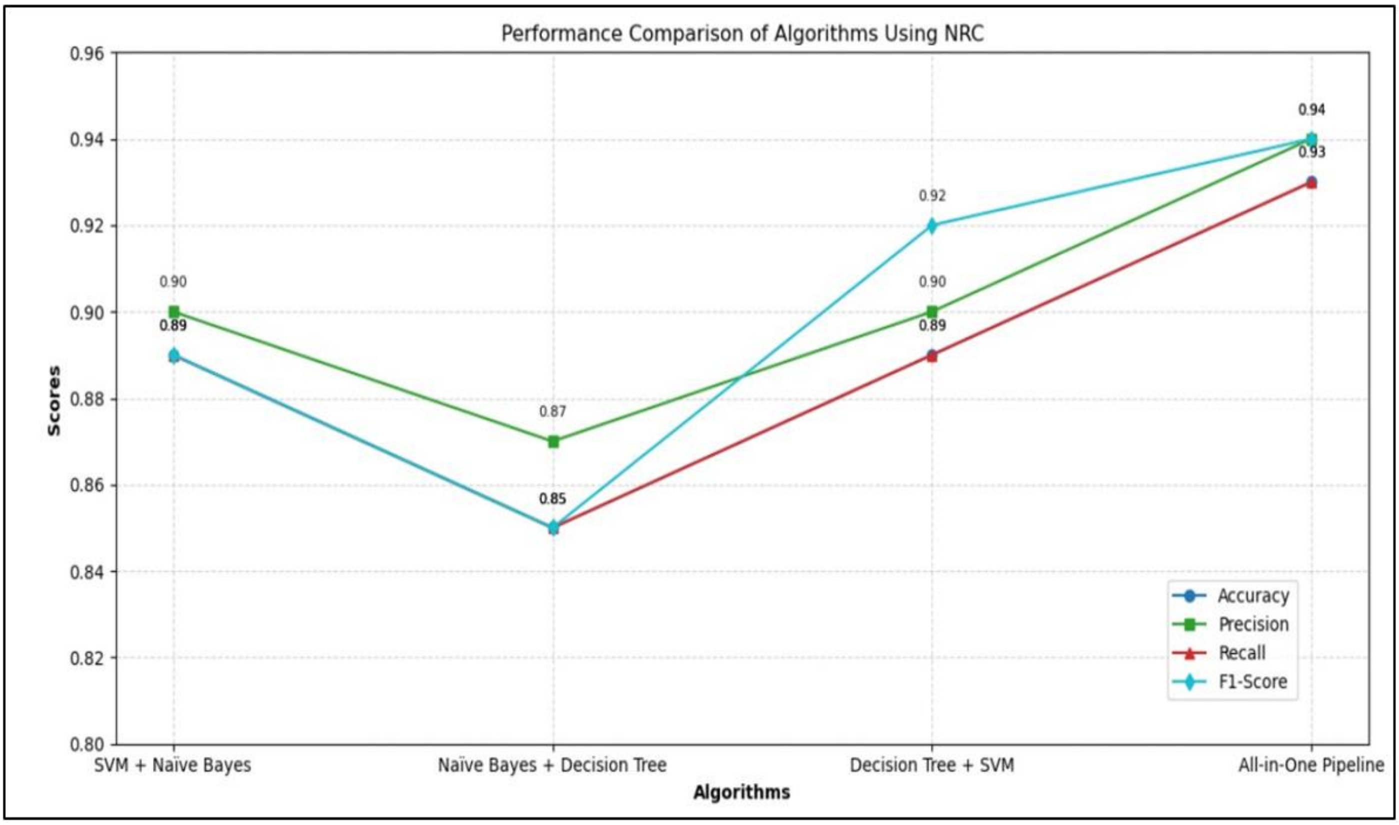


Fig 5 Performance evaluation for various pipeline models with NRC

Accuracy, Precision, Recall, and F1-Score are the four assessment metrics used to compare the performance of hybrid algorithm combinations utilizing NRC Emotion Lexicon. The results are shown in the line graph. With the best Precision(0.94), Recall(0.93), and F1-Score (0.94), the All-in-One Pipeline outperforms all other measures. The combination of Decision Tree + SVM follows closely, showing balanced and strong performance, especially in F1-Score (0.92). In contrast, Naïve Bayes + Decision Tree performs the weakest, with all metrics around 0.85–0.87. SVM + Naïve Bayes offers slightly better performance than this, but still lower than the top two. Overall, the graph indicates that integrating multiple classifiers in a pipeline significantly boosts the detection performance using the NRC lexicon.

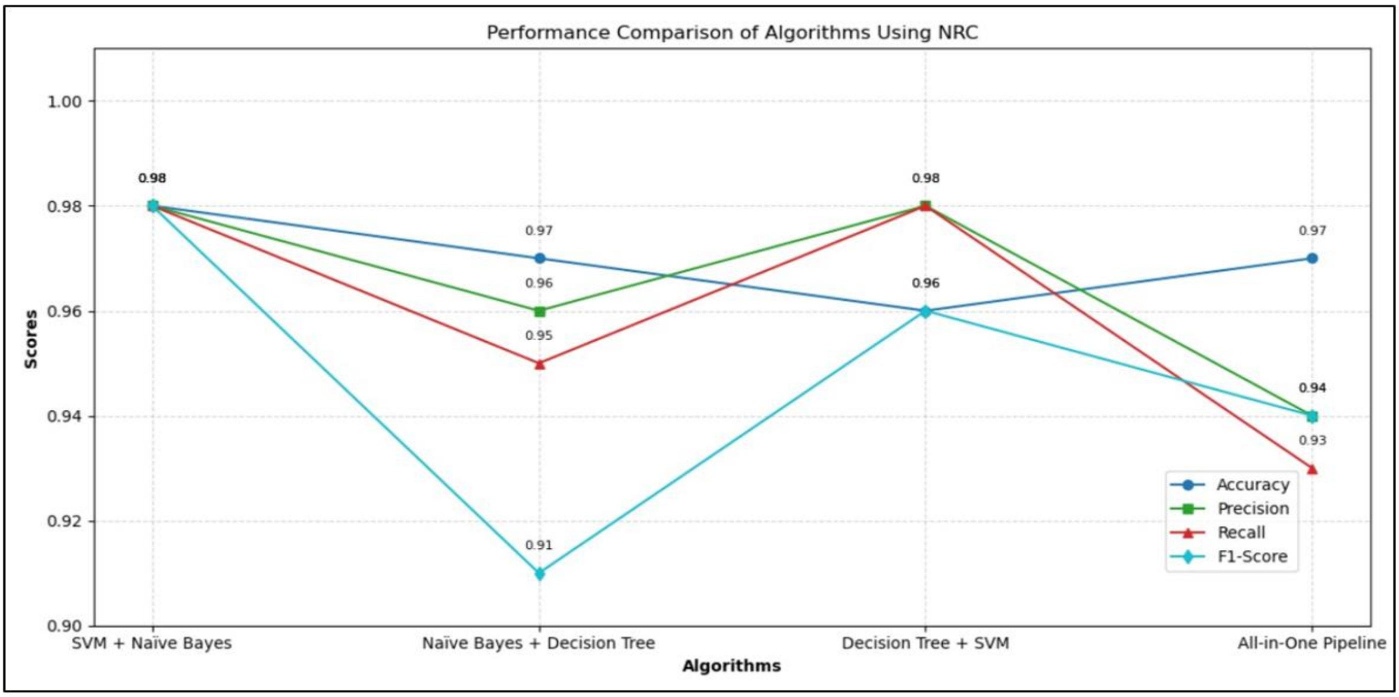


Fig 6 Performance evaluation for various pipeline models with Wordnet

Accuracy, Precision, Recall, and F1-Score are the four main metrics used to assess the performance of hybrid algorithm combinations using WordNet. The results are shown in the line graph. The highest overall performance is shown by the SVM + Naïve Bayes combo, which consistently scores 0.98 across all measures. Precision and Recall are two areas where the Decision Tree + SVM combination shines at 0.98, while Accuracy and F1-Score are somewhat worse at 0.96. On the other hand, Naïve Bayes + Decision Tree performs relatively lower, with its F1-Score dropping to 0.91. The All-in-One Pipeline achieves moderate scores (Accuracy: 0.97, F1-Score: 0.94), slightly below the best-performing hybrid models. Overall, the graph highlights that combining classifiers, particularly SVM with Naïve Bayes, significantly enhances detection performance when leveraging WordNet.

VI. CONCLUSION AND FUTURE SCOPE

In this project, we leveraged advanced machine learning and sentiment analysis to identify political threats within news headlines. We used a powerful pipeline-driven approach that included preprocessing and cleaning of text, emotion extraction, and the use of advanced machine learning models. We integrated WordNet for improved semantic understanding via lemmatization and the NRC Emotion Lexicon to identify crucial emotions including wrath, fear, and trust.

These emotion scores served as critical input features for machine learning models, including Naïve Bayes, Support Vector Machines (SVM), and Decision Trees, which were strategically combined (e.g., SVM + Decision Tree, Decision Tree + Naïve Bayes, Naïve Bayes + SVM) within the pipeline to optimize classification performance. Model efficacy was rigorously assessed using metrics such as accuracy, precision, recall, and F1-score. Visualization tools, including bar graphs and pie charts, effectively illuminated emotional patterns and model results. Ultimately, this project demonstrates that a structured integration of sentiment analysis and machine learning within a cohesive pipeline can proficiently detect and interpret political threats.

REFERENCES

[1]. N. A. M. Razali *et al.*, “Political Security Threat Prediction Framework Using Hybrid Lexicon-Based Approach and Machine Learning Technique,” *IEEE Access*, vol. 11, pp. 17151–17164, 2023, doi: 10.1109/ACCESS.2023.3246162.

[2]. E. Lee, F. Rustam, P. B. Washington, F. El Barakaz, W. Aljedaani, and I. Ashraf, “Racism Detection by Analyzing Differential Opinions Through Sentiment Analysis of Tweets Using Stacked Ensemble GCR-NN Model,” *IEEE Access*, vol. 10, pp. 9717–9728, 2022, doi: 10.1109/ACCESS.2022.3144266.

[3]. R. Mubarak, T. Alsboui, O. Alshaikh, I. Inuwa-Dutse, S. Khan, and S. Parkinson, "A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats," *IEEE Access*, vol. 11, pp. 144497–144529, 2023, doi: 10.1109/ACCESS.2023.3344653.

[4]. S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," *IEEE Access*, vol. 8, pp. 171796–171819, 2020, doi: 10.1109/ACCESS.2020.3024198.

[5]. E. N. Crothers, N. Japkowicz, and H. L. Viktor, "Machine-Generated Text: A Comprehensive Survey of Threat Models and Detection Methods," *IEEE Access*, vol. 11, pp. 70977–71002, 2023, doi: 10.1109/ACCESS.2023.3294090.

[6]. G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, "Threat Analysis for Automotive CAN Networks: A GAN Model-Based Intrusion Detection Technique," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4467–4477, Jul. 2021, doi: 10.1109/TITS.2021.3055351.

[7]. Y. Luo, M. He, and X. Wang, "Analyzing the semantic structure of network flow: a threat detection method with independent generalization capabilities," *IEEE Trans Netw Sci Eng*, 2024, doi: 10.1109/TNSE.2024.3483216.

[8]. X. Tao *et al.*, "User Behavior Threat Detection Based on Adaptive Sliding Window GAN," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2493–2503, Apr. 2024, doi: 10.1109/TNSM.2024.3355698.

[9]. R. Rajesh, S. Hemalatha, S. M. Nagarajan, G. G. Devarajan, M. Omar, and A. K. Bashir, "Threat Detection and Mitigation for Tactile Internet Driven Consumer IoT-Healthcare System," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4249–4257, Feb. 2024, doi: 10.1109/TCE.2024.3370193.

[10]. X. Cai *et al.*, "LAN: Learning Adaptive Neighbors for Real-Time Insider Threat Detection," Mar. 2024, doi: 10.1109/TIFS.2024.3488527.

[11]. S. Salim, N. Moustafa, and A. Almorjan, "Responsible Deep Federated Learning-based Threat Detection for Satellite Communications," *IEEE Internet Things J*, 2025, doi: 10.1109/JIOT.2025.3531884.

[12]. M. Al Razib, D. Javeed, M. T. Khan, R. Alkanhel, and M. S. A. Muthanna, "Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework," *IEEE Access*, vol. 10, pp. 53015–53026, 2022, doi: 10.1109/ACCESS.2022.3172304.

[13]. Y. Zhang, W. Liu, K. Kuok, and N. Cheong, "Anteater: Advanced Persistent Threat Detection With Program Network Traffic Behavior," *IEEE Access*, vol. 12, pp. 8536–8551, 2024, doi: 10.1109/ACCESS.2024.3349943.

[14]. J. Xiao, L. Yang, F. Zhong, X. Wang, H. Chen, and D. Li, "Robust Anomaly-Based Insider Threat Detection Using Graph Neural Network," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 3717–3733, Sep. 2023, doi: 10.1109/TNSM.2022.3222635.

[15]. T. Al-Shehari, M. Al-Razgan, T. Alfakih, R. A. Alsowail, and S. Pandiaraj, "Insider Threat Detection Model Using Anomaly-Based Isolation Forest Algorithm," *IEEE Access*, vol. 11, pp. 118170–118185, 2023, doi: 10.1109/ACCESS.2023.3326750.

[16]. J. Dahl, G. R. De Campos, and J. Fredriksson, "Prediction-Uncertainty-Aware Threat Detection for ADAS: A Case Study on Lane-Keeping Assistance," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 4, pp. 2914–2925, Apr. 2023, doi: 10.1109/TIV.2023.3253555.

[17]. R. B. Peccatiello, J. J. C. Gondim, and L. P. F. Garcia, "Applying One-Class Algorithms for Data Stream-Based Insider Threat Detection," *IEEE Access*, vol. 11, pp. 70560–70573, 2023, doi: 10.1109/ACCESS.2023.3293825.

[18]. V. Christopher *et al.*, "Minority Resampling Boosted Unsupervised Learning with Hyperdimensional Computing for Threat Detection at the Edge of Internet of Things," *IEEE Access*, vol. 9, pp. 126646–126657, 2021, doi: 10.1109/ACCESS.2021.3111053.

[19]. D. C. Le and N. Zincir-Heywood, "Anomaly Detection for Insider Threats Using Unsupervised Ensembles," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1152–1164, Jun. 2021, doi: 10.1109/TNSM.2021.3071928.

[20]. R. Sánchez-Corcuera, A. Zubiaga, and A. Almeida, "Early Detection and Prevention of Malicious User Behavior on Twitter Using Deep Learning Techniques," *IEEE Trans Comput Soc Syst*, pp. 1–13, Jul. 2024, doi: 10.1109/tcss.2024.3419171.

[21]. M. Luqman, M. Faheem, W. Y. Ramay, M. K. Saeed, and M. B. Ahmad, "Utilizing Ensemble Learning for Detecting Multi-Modal Fake News," *IEEE Access*, vol. 12, pp. 15037–15049, 2024, doi: 10.1109/ACCESS.2024.3357661.

[22]. M. A. Ferrag *et al.*, "Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices," *IEEE Access*, vol. 12, pp. 23733–23750, 2024, doi: 10.1109/ACCESS.2024.3363469.

[23]. D. C. Le, N. Zincir-Heywood, and M. I. Heywood, "Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 30–44, Mar. 2020, doi: 10.1109/TNSM.2020.2967721.