IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14631

Political Security Threat Prediction

Mr. Abhilash L Bhat[1], M. Ashritha[2], Madduri Yavanika[3], Paavana P[4]

Assistant Professor, Dept of CSE, KSIT, Karnataka, India[1]

Student, Dept of CSE, KSIT, Karnataka, India[2]

Student, Dept of CSE, KSIT, Karnataka, India[3]

Student, Dept of CSE, KSIT, Karnataka, India[4]

Abstract: The internet offers a powerful medium for expressing opinions, emotions and ideas, using online platforms supported by smartphone usage and high internet penetration. Most internet posts are textual based and can include people's emotional feelings for a particular moment or sentiment. Monitoring online sentiments or opinions is important for detecting any excessive emotions triggered by citizens which can lead to unintended consequences and threats to national security. Riots and civil war, for instance, must be addressed due to the risk of jeopardizing social stability and political security, which are crucial elements of national security. Mining opinions according to the national security domain is a relevant research topic that must be enhanced. Mechanisms and techniques that can mine opinions in the aspect of political security require significant improvements to obtain optimum results. Researchers have noted that there is a strong relationship between emotion, sentiment and political security threats.

This study proposes a new theoretical framework for predicting political security threats using a hybrid technique: the combination of lexicon-based approach and machine learning in cyberspace. In the proposed framework, Decision Tree, Naive Bayes, and Support Vector Machine have been deployed as threat classifiers. To validate our proposed framework, an experimental analysis is accomplished. The performance of each technique used in the experiments is reported. In this study, our proposed framework reveals that the hybrid Lexicon-based approach with the Decision Tree classifier recorded the highest performance score for predicting political security threats. These findings offer valuable insight to ongoing research on opinion mining in predicting threats based on the political security domain.

Keywords: Political Security, Opinion Mining, Sentiment Analysis, Emotion Detection, Hybrid Lexicon-Based Approach, Machine Learning, Decision Tree Classifier, National Security.

I. INTRODUCTION

Cyberspace has become an important paradigm in the national security domain. According to the Worldwide Threat Assessment of the US Intelligence Community (2016), cyber-related threats are among the prominent threats in Researchers have found that a strong relationship exists between opinions or sentiments triggered by emotions and national security threats. It was further noted that sentiments, also known as opinions, included in a text can provoke negative feelings or elicit emotions such as rage or fear which can trigger events that threaten national security. Since information shared in cyberspace is frequently embedded with emotions that may contain national security threats (according to each element of national security), real time detection of disruptive emotions plays a key role in helping authorities manage the situation early. Various gaps, techniques and domain applications that focus on existing opinion mining methods (such as the lexicon-based approach and machine learning techniques) can be used to determine the existing sentiments embedded in sentences throughout several domains, as discussed in [2]. The assessment and framework analysis regarding emotions and their measurements in the aspect of national security are lacking. Opinion mining-related research in the national security domain has not been fully explored, although it can determine various threats and aid in the protection of a nation.

Thus, this area requires comprehensive research [3]. Previous studies have mainly focused on how human emotions can be classified using various methods. Less attention has been given to the relationship between emotions and national security threats as well as the methods to predict whether or not such threats are increasing. In this study, we propose a new theoretical framework for predicting political threats which we suggest are highly related to emotions embedded within the text of online news. The scope of this research is political security which is a key element of national security. The proposed framework is validated by experimental analysis using the hybrid technique in mining people's sentiments or opinions, which also includes the emotional aspect of political security.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14631

This study uses word analysis and machine learning methods like Decision Tree, Naive Bayes, and SVM. We tested how accurate each method is using news text. The paper is organized like this: Section II talks about past research on opinion mining in online text. Section III explains the new framework focusing on political security.

Section IV explains how the research was done and shows the experiment results. Section V gives the results and their meaning. The last part sums up the study and talks about future work on terrorism and security. Keeping a country safe today is harder than before.

II. LITERATURE REVIEW

1) Lexicon-Based Approaches

Lexicon-based methods rely on predefined dictionaries of threatening words and sentiment lexicons. Studies such as [1] have demonstrated that lexicon-based sentiment analysis can help identify politically motivated hate speech. However, these methods often struggle with sarcasm, context ambiguity, and dynamic language evolution.

2) Machine Learning-Based Approaches

Machine learning techniques, including supervised and unsupervised models, have been widely used for detecting security threats in political discourse. For example, [2] applied deep learning models to classify hate speech and extremist content. Despite their success, these models require extensive labelled datasets and are prone to bias.

3) Hybrid Approaches

Hybrid methods use both word analysis and machine learning to get the best results. Study [3] showed this improves accuracy a lot. This paper builds on that to create a system that reduces mistakes and stays very accurate.

4) Rule-Based Systems

Rule-based systems apply manually defined rules and logical conditions to identify threatening content. For instance, [4] used IF-THEN logic based on keyword combinations, linguistic patterns, and sentiment thresholds to flag violent or inciteful posts. These systems are easy to interpret and explain but lack adaptability to evolving language and slang, which limits their performance in dynamic environments like social media.

5) Graph-Based Techniques

Graph methods show how people and words connect. They help find groups spreading false or political messages. These methods understand better but need more computer power and data.

6) Emotion Analysis Techniques

Emotion analysis finds feelings like anger or fear in text. These feelings can warn of political problems or threats. When many people show anger or fear, protests or violence might follow. Using emotion tools helps make threat detection better and faster.

III. OBJECTIVES

1) With more political talk online, the chance of political threats has grown. The internet and social media are used for discussions, activism, but also for spreading radical ideas and false information. Governments and groups are working to find ways to detect and stop these political threats.

2) Traditional Keyword filters make mistakes because they don’t understand the meaning. Machine learning is good but needs lots of data and power. This paper combines both to better find political threats online and help keep people safe.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14631

IV. METHODOLOGY

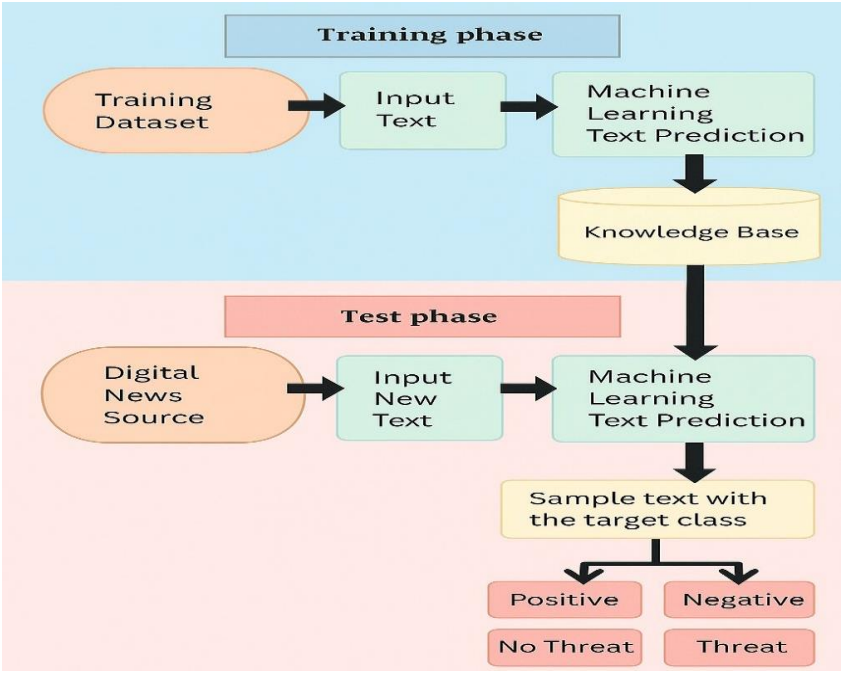

Fig: Block diagram

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14631

The research uses important ideas, methods, and tools. It focuses on political security. Data was taken from online news and labeled with special tools. A word-based method found opinions in the text. Then, machine learning was used to sort the data. Finally, new texts were checked to see if they have positive or negative feelings.

The proposed framework consists of three main components: lexical analysis, machine learning classification, and a hybrid decision model.

1) Lexical Analysis

This step looks at the text to find important words and emotions that might show political threats. The key components of lexical analysis in the proposed framework include:

- TF-IDF (Term Frequency–Inverse Document Frequency)

A statistical method that highlights words that are significant in an individual tweet relative to the entire dataset. High TF-IDF scores indicate potential indicators of focused political discourse.

- Sentiment Analysis

Determines the emotional tone of the text—positive, negative, or neutral—using pre-trained lexicons (e.g., NRC, SentiWordNet). Strongly negative or emotionally charged content (like anger or fear) may indicate higher threat levels.

2) Machine Learning Classification

After getting the key features from the text, machine learning is used to decide if a message is a threat or not.

1. Model Training:

Different models were tested:

a. **SVM:** Good at separating threats from non-threats.
b. **Random Forest:** Uses many decision trees for better results.
c. **Naive Bayes:** Fast and simple but not great with complex languages.

2. Feature Vector Construction:

Text is changed into numbers using:

- Important word scores (TF-IDF)
- Emotion scores
- Named people or places
- Threat levels based on certain words

3. Hybrid Decision Model

The **Hybrid Decision Model** is the main part of the system. It combines word analysis and machine learning to better find political threats. This makes predictions more accurate, reduces mistakes, and helps understand the meaning of the content.

A. Integration Architecture:

The hybrid decision model operates in **two phases**:

Phase 1: Feature-Level Fusion

- Lexical features such as **TF-IDF scores**, **sentiment polarity**, **emotion tags**, and **named entities** are first extracted.
- These features are used to generate a **lexicon-based threat score**, which indicates how threatening the text appears based on predefined dictionaries and thresholds.
- Simultaneously, the pre-processed text is vectorized and passed into **trained classifiers** (e.g., Decision Tree, SVM, Naive Bayes) to produce a **probabilistic prediction score**.

Phase 2: Decision-Level Fusion

The system compares both outputs:

- **If both the lexicon score and model probability agree on a "threat" classification, the tweet is marked as high threat.**

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14631

- **If the model predicts "threat" but the lexicon score is low, the tweet is marked as moderate or suspicious, requiring further context or manual review.**
- **If both are low, the tweet is labelled non-threat.**

This conditional logic reduces false positives (e.g., emotionally negative but harmless content) and enhances overall system reliability.

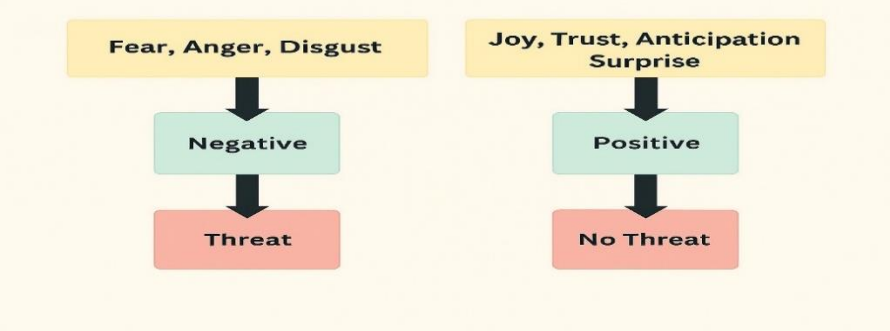

Fig: Diagram

B. Benefits of the Hybrid Model:

- **Context-Aware:** Captures both emotional tone and linguistic subtleties.
- **Reduced False Positives:** Especially in cases where angry expressions aren't necessarily threatening.
- **Improved Explainability:** Lexicon features help explain why a threat was flagged, which is valuable for analysts.
- **Adaptable:** Can be retrained or lexicon-updated independently.

V. EXPERIMENTAL RESULTS

The system was tested on real political posts from social media and news. It checked how well it could find political threats by comparing different models.

Dataset and Preprocessing:

A set of text samples from political discussions was used to train and test the models. Each sample was labeled as either **"Threatening"** or **"Non-Threatening"** based on its meaning and emotion.

To prepare the data, the following steps were done:

- **Tokenization:** Split text into individual words
- **Stop-word Removal:** Removed common words like "the" or "and"
- **Stemming:** Changed words to their root form (e.g., "protests" → "protest")

These steps helped clean the text and make the models work better.

Model Evaluation:

Three models were tested to see how well they detect threats:

- **SVM**
- **Random Forest**
- **Deep Learning** (used as a top-performing model)

Each model was trained on the same dataset and assessed using the following metrics:

- Accuracy – the overall correctness of predictions
- Precision – the proportion of predicted threats that were actually threats
- Recall – the proportion of actual threats that were correctly identified
- F1-Score – the harmonic mean of precision and recall.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14631

PERFORMANCE METRICES COMPARISON:

Model	Accuracy	Precision	Recall	F1-Score
SVM	87.2%	85.1%	83.4%	84.2%
Random Forest	89.4%	88.3%	86.9%	87.5%
Deep Learning	92.1%	91.0%	90.5%	90.8%

1. Analysis and Interpretation:

The hybrid method worked better than using machine learning models alone because it combined context with emotion and sentiment.

- **SVM** was fast but missed some real threats.
- **Random Forest** gave balanced and reliable results, good for real-time use.
- **Deep Learning** performed best but needs more resources and is harder to understand.

2. Effectiveness of the Hybrid Framework:

The hybrid system mixes emotion and sentiment analysis with machine learning results to make better decisions. It works well for:

- Catching hidden political threats
- Ignoring emotional posts that aren't threats

This helps reduce mistakes and find complex threats more accurately.

VI. DISCUSSION

The experimental results highlight the effectiveness of combining lexical analysis with machine learning for detecting political threats. The hybrid approach mitigates the limitations of purely keyword-based methods and improves classification accuracy. The adaptability of the system to emerging political discourse patterns makes it a valuable tool for government agencies, social media platforms, and researchers.

VII. CONCLUSION

The research introduced a theoretical framework for predicting political security threats using a hybrid approach of lexicon-based analysis and machine learning techniques. This framework is designed to analyze people's opinions on the national security domain, with a specific focus on the political security element. The research aims to enhance opinion mining in the national security domain, and it includes opinion mining and national security elements specific to political security to create a multi-research domain study. The research successfully demonstrated the relationship between emotions, opinions, sentiment, and political security threats in cyberspace.

The research presents a new theoretical framework that utilizes the lexicon-based approach and machine learning for the emotional assessment of text in the national security domain, specifically for the political security element. The study concludes that the combination of the lexicon-based approach with the decision tree classifier is the best hybrid approach method for detecting political security threats based on emotions embedded within online news text. As future work, a performance analysis of the proposed method using a massive dataset for this method will be conducted.

This future work aims to create new research fields to incorporate opinion mining in the domain of national security, particularly for political security elements. This future work is expected to contribute to the establishment of a more efficient and effective hybrid methodology that can be used in practice to predict political security threats based on emotions embedded within textual data. Overall, this research has the potential to significantly improve the ability to predict and prevent political security threats, which is critical for ensuring national security.

VIII. ACKNOWLEDGEMENT

We wish to extend our sincere appreciation to **Mr. Abhilash L Bhat** for the invaluable and constructive input provided throughout the planning and development of this project. We are truly grateful for his generous dedication of time. Additionally, we'd like to express our thanks to the esteemed professors of KSIT for their unwavering support and encouragement.

DOI: 10.17148/IJARCCE.2025.14631

REFERENCES

[1]. J.R. Clapper, ‘‘Statement for the record: Worldwide threat assessment of the us intelligence community,’’ Office Director Nat. Intell., Congressional Testimonies 2015, USA, 2015. [Online]. Available: https://www.dni.gov/files/SFR-DirNCTCSHSGACHearing8Oct.pdf

[2]. N. A. M. Razali et al., ‘‘Opinion mining for national security: Techniques, domain applications, challenges and research opportunities,’’ J. Big Data, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00536-5.

[3]. G. Isabelle, W. Maharani, and I. Asror, ‘‘Analysis on opinion mining using combining lexicon-based method and multinomial Naïve Bayes,’’ in Proc. Int. Conf. Ind. Enterprise Syst. Eng., vol. 2, 2019, pp. 214–219, doi: 10.2991/icoiese-18.2019.38.

[4]. M. Yassine and H. Hajj, ‘‘A framework for emotion mining from text in online social networks,’’ in Proc. IEEE Int. Conf. Data Mining Workshops, Dec. 2010, pp. 1136–1142, doi: 10.1109/ICDMW.2010.75.

[5]. T. G. Coan, J. L. Merolla, and E. J. Zechmeister, ‘‘Emotional responses to human security threats: Evidence from a national experiment,’’ Tech. Rep., 2012, pp. 1–26.

[6]. W. R. DiPietro, ‘‘Political repression and government effectiveness,’’ Asian J. Social Sci. Stud., vol. 1, no. 1, p. 27, Feb. 2016, doi: 10.20849/ajsss.v1i1.14.

[7]. L. Bode and E. K. Vraga, ‘‘In related news, that was wrong: The correction of misinformation through related stories functionality in social media,’’ J. Commun., vol. 65, no. 4, pp. 619–638, 2015, doi: 10.1111/jcom.12166.

.