Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

17

An Approach Utilizing Opinion Mining for the Detection of Radicalized Content in Social Media Platforms

Neha Gupta

Associate Professor

Abstract

Through the widespread use of social broadcasting as a primary platform for message among individuals and communities, the potential for its misuse has grown significantly. One notable misuse is the dissemination of radical content, facilitated by the ease of sharing information across various networks. This poses a significant challenge for social media and security agencies, as they must sift through vast amounts of data to identify such content. The task becomes even more complex due to the lack of a clear difference between radical and non-radical material, especially as the volume of data continues to grow.

To address this issue, the study proposes an artificial intelligence-based method for detecting fundamental content. This method employs glossary learning to train a Bayesian Regularized Artificial Neural Network (ANN). Key recital metrics considered include the amount of iterations, processing time, and accuracy. The results demonstrate that the planned system achieves a organization accuracy of 97%, outperforming the previous benchmark of 89%.

Keywords: Radical Content, Counter-terrorism, social networks, text analysis, Bayesian Regularization, correctness

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Introduction

As social media becomes increasingly influential across various aspects of life, it has also emerged as a tool for spreading hatred and radical content (Agarwal et al., 2015). Neither the U.S.-led international anti-terror coalition nor Russia's defence ministry discloses specific timelines for addressing the ISIS threat, which is a banned organization in Russia (Akhgar et al., 2014; Al-Zewairi & Naymat, 2017; Ball, 2016). This relatively young organisation is notable for its aggressive tactics and provocative stance towards other Islamist terrorist groups, further amplifying its impact in the Middle East (Bobashev et al., 2019).

To maximize their impact on the Islamic world, counting tech-savvy Occidentalized Muslim youth, ISIS has actively utilized media technologies and public relations (Cherif et al., 2014; Drouin, 2014; Frank et al., 2015). Modern terrorist organizations frequently disseminate professionally created videos, interviews, and propaganda online to further their agendas. This strategy, often referred to as "Media Jihad," has solidified its place trendy the worldwide info space as a critical tool for recruiting new fighters and consolidating territorial power (Ishitaki et al., 2017; Johnston & Weiss, 2017).

Radical groups also exploit instant messaging platforms and social media accounts to spread propaganda, with account blocking being one effective countermeasure (Kapitanov et al., 2022; Lara-Cabrera & Gonzalez-Pardo, 2017; López-Sánchez et al., 2020). However, analysts must process massive amounts of information to monitor and combat this activity (Lourentzou et al., 2017). Table I demonstrates the frequency of messages across various platforms (Modupe et al., 2014).

ISIS, known as "Islamic State of Iraq and the Levant" or "Islamic State," represents a unique phenomenon in modern terrorism due to its rapid development and unprecedented ideological and informational activities (Oda et al., 2016; Sabbah & Selamat, 2015). The organization's ability to adapt media technologies has significantly amplified its influence and reach (Scrivens & Frank, 2016).

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

In the context of social media's overwhelming data volume, artificial intelligence techniques are critical for effective analysis and radical content detection (Tundis et al., 2018; Wadhwa & Bhatia, 2015). Methods, like Named Entity Recognition (NER), clustering, and Bayesian classifiers, have proven effective, though challenges remain due to the complexity and multilingual nature of terrorist communications (Yucel & Koltuksuz, 2014).

Literature Review

The sheer volume of data generated on social networking platforms is overwhelming, making it impossible for humans to manually analyze and monitor effectively. To highlight the scale and complexity of this data, a frequency analysis of various social media platforms is presented.

Table.1 Frequency Analysis of Different Social Media Applications [1]

Application	Per Second	Per Day	Per Month
WhatsApp	636 (thousand)	55 (billion)	1.6 (trillion)
Telegram	175 (thousand)	15 (billion)	450 (trillion)
Facebook	2.5 (thousand)	216 (billion)	6.5 (trillion)
Twitter	5.8 (thousand)	500 (billion)	15 (trillion)
Instagram	1 (thousand)	95 (billion)	2.8 (trillion)

Artificial intelligence-based methods are required for social media data analysis due to the vast volume of communications and their complexity (Lourentzou et al., 2017; Modupe et al., 2014). Artificial neural networks (ANNs) are developed to practically apply such AI-based methodologies. Texts containing radical content are frequently analysed using a variety of machine learning techniques. Named Entity Recognition (NER), for example, is effective when used on brief text messages and may extract organized information from formless or semi-structured texts (Ishitaki et al., 2015). Dynamic Query Expansion (DQE), logistic regression, and clustering are more suited for forecasting riots, protests, or terrorist attacks (Sabbah et al., 2016).

The most frequently used methods for identifying extremism and radicalism in real-time are K-Nearest Neighbour, Naive Bayes classifiers, Support Vector Machine (SVM) with unlike kernel functions, result trees, and others (Scrivens & Frank, 2016). However, deprived of a clear border amongst different classes, a probabilistic classifier becomes necessary.

Thematic analysis of such data is complex by some factors. Information dispersed by terrorist clusters is heterogeneous, with short social network messages that contain dialect and coded words, making semantic study challenging (Cherif et al., 2014). Forums often feature communication in multiple languages or their combinations, complicating the analysis further (Lara-Cabrera & Gonzalez-Pardo, 2017). Simple keyword or phrase searches do not effectively differentiate terrorist sites from news activities since terrorist places are frequently masked as news sites or religious media (Al-Zewairi & Naymat, 2017).

The volume of such sites makes manual analysis inefficient, requiring automated tools for effective selection and filtering (Wadhwa & Bhatia, 2015). Identifying which terrorist group disseminated specific content is even more challenging because ideologically similar groups may use overlapping vocabulary (Bobashev et al., 2019).

Another tactic employed by ISIS, forbidden in the Russian Federation, is the promotion of specific hashtags to establish posts by subject or group. Activists repeatedly post messages with relevant hashtags at specific times of day. During the assault on Mosul, for example, over 40,000 tweets supported ISIS, manipulating the news agenda with hashtags like #ISIS and #Iraqwar (Frank et al., 2015).

The approach planned in this paper consists of numerous successive stages. First, texts are cleared of "information noise" such as links, emoticons, and filler words. Then, typos in keywords are corrected using Levenshtein distance metrics (Oda et al., 2016). A Naive Bayes classifier is trained on test data to categorize messages into those containing radical content and those that do not. However, separating messages advocating extremism from those condemning it requires tone analysis (Kapitanov et al., 2022).

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Scheme Design Using Reversion Learning-Based Bayesian Regularized ANN

Neural networks, with their extraordinary aptitude to derive meaning from complex or inexact data, can extract designs and notice trends that are too subtle for human observation or other computer techniques (Agarwal et al., 2015). They offer several advantages, including:

1. Adaptive Learning: The aptitude to learn tasks based on exercise data.
2. Self-Organization: The capability to organize and represent information autonomously during learning.
3. Real-Time Operation: Parallel computations that leverage specialized hardware for increased efficiency.

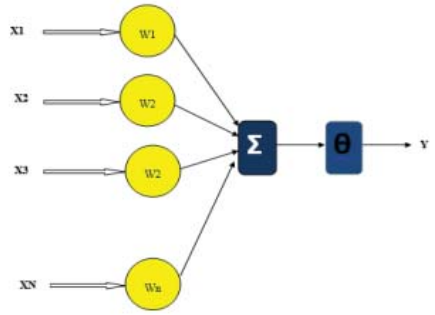

Fig.1 Accurate Classical of Neural Network

The yield of the neural system is given by:

$$\sum \mathbf{XiWi} + \Theta \; \mathbf{n\ i=1} \quad (1)$$

Here, XiX_iXi represents the inputs arriving from various paths, while WiW_iWi denotes the weights assigned to these paths, and θ\thetaθ represents the bias. Each input signal traversing a specific path is associated with a unique weight, WWW. The signal is scaled by its respective weight as it moves through the network, and the cumulative summation of these weighted signals is passed to the neuron. The neuron's response is influenced by the bias θ\thetaθ, which plays a crucial role in determining the activation of the neuron.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

The beginning function ϕ\phiϕ is then applied to produce the final output, shaping the network's decision-making process. The ability of the artificial neural network (ANN) to learn is governed by temporal learning dynamics, which are expressed through a specific mathematical relationship.

$$\boldsymbol{w(i) = f(i, e)} \text{ (2)}$$

Here, w (i) represents the prompt masses i is the repetition e is the forecast error. The weight variations animatedly and is given by:

$$\boldsymbol{Wk\ e,i \rightarrow Wk+1} \text{ (3)}$$

Here, Wk is the weight of the existing iteration. Wk+1 is the weight of the following iteration

Methodology

Model of Reversion Learning Numerous supervised learning techniques that need regression analysis between dependent and independent variables have been found use for regression learning. Regression models vary depending on the kind of relationship between independent and dependent variables, the number of independent variables, and other factors. Predicting a reliant on variable value (y) from a given independent variable (x) is what regression does. Thus, a relationship between x (input) and y (output) is determined by this regression technique. In terms of mathematics,

$$\boldsymbol{y = \theta 1 + \theta 2 x} \text{ (4)}$$

In this case, x stands for the input variables' state vector and y for the output variables' state vector. The coefficients ¸1 and ¸2 attempt to match the input vector to the output vector of the regression learning model. The model seeks to predict a y worth such that the error gap between the anticipated and true values is as small as possible by obtaining the best-fit regression line. To minimise the error between the predicted y value (pred) and the true y value (y), it is crucial to update the θ1 and θ2 values. The mathematical definition of the cost function J is:

$$\boldsymbol{J = 1\ n \sum (pred1 - yi)\ n\ 2\ i=1} \text{ (5)}$$

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

In this case, the target is y, the actual output is pred, and n is the number of samples. (ii) Regression Learning Using Gradient Descent The model services Gradient Descent to update θ1 and θ2 values in order to minimise the MSE value and minimise the Cost function, which results in the best-fit line. The goal is to get the lowest cost by iteratively updating the initial random θ1 and θ2 values. Reducing the cost function J is the primary goal. Bayesian Regularisation (iii) A modified variant of the LM weight update process, the Bayesian Regularisation (BR) algorithm has the added benefit of applying the Baye's theorem of provisional probability to the final classification. The following is the weight updating rule for the Bayesian Regularisation:

$$\boldsymbol{wk}+\mathbf{1} = \boldsymbol{wk} - (\boldsymbol{JkJk}\,\boldsymbol{T} + \boldsymbol{\mu I})\text{^}- \mathbf{1}(\boldsymbol{Jk}\,\boldsymbol{Tek}) \quad (6)$$

In this case, the weight of the current repetition is wk, and the weight of the following iteration is wk+1. The Jacobian matrix is Jk. $Jk\ T$ is the Jacobian matrix in reverse. The mistake of Current Version Step size is represented by μ. I is a matrix of identities. The graph theory method provides a visual representation of the Bayesian Classifier's decision-making process. The set theory method demonstrated in the following steps can be used to comprehend the method for calculating the probability among several disjoint sets. The decision to be made in situations where distinct lapping data value categories exist is clearly shown in the images.

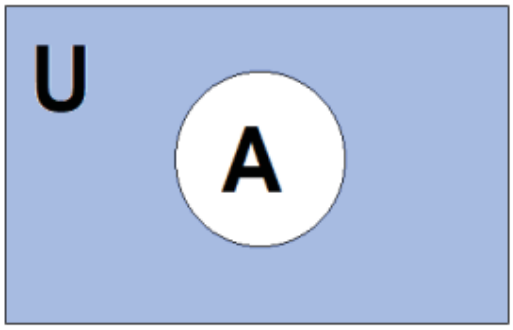

Fig.2 Universal Set Comprising a Subset 'A'

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

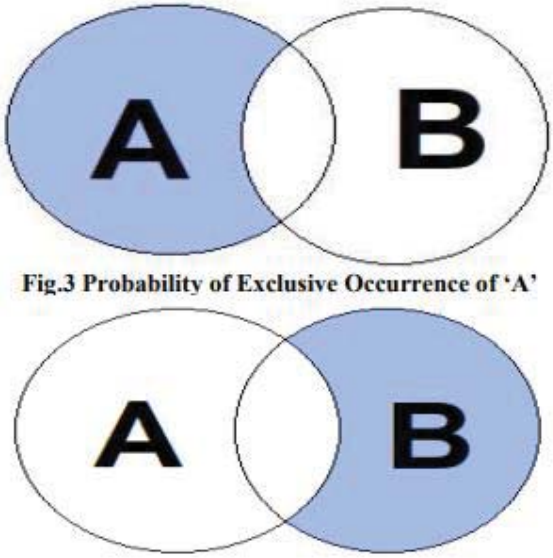

Fig.3 Probability of Exclusive Occurrence of 'A'

Fig.4 Probability of Select Incidence of 'B'

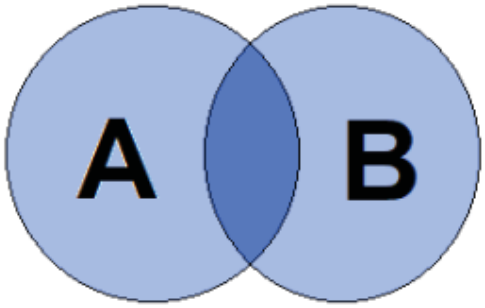

Fig.5 Prospect of Union of A and B

Results

Dataset:

The organization algorithms for text documents related to radical content were evaluated using a dataset compiled by researchers at the Artificial Intelligence Lab, University of Arizona. This dataset includes information gathered from multiple online sources such as websites, forums, chats, blogs, and social media platforms linked to designated terrorist organizations.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Normalization:

Text normalization is the process of converting text into a uniform format suitable for subsequent analysis. When handling large volumes of data, it is essential to remove non-essential elements from the text, such as prepositions, particles, and conjunctions, to focus only on the meaningful content.

Fig.6 Sample Text data for examination [1]

The symbol reduces a sample screenshot of the text data to be analysed from dissimilar social media requests for conclusion fundamental content.

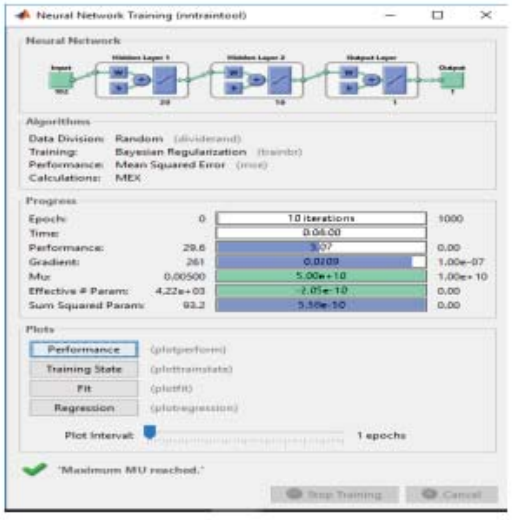

Fig.7 Calculated Neural Network and its exercise parameters

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Conclusion

From the earlier discussions, it is evident that the rise of social media as a widely used communication platform among diverse individuals and communities has significantly increased the potential for its misuse. A prominent example of such misuse is the dissemination of radical content, facilitated by the ease of sharing among users and groups. Social media and security agencies face the complex task of analysing massive volumes of data to identify such harmful content. This challenge is compounded by the lack of clear distinctions between radical and non-radical content, making organization increasingly difficult as data volume grows.

The planned method leverages a Regression Learning-based Bayesian Regularized Artificial Neural Network (ANN) to address this issue. The results demonstrate that the proposed approach achieves a significantly higher accuracy of 97% compared to the 89% accuracy reported in prior studies.

Acknowledgement:

The conclusion of this research paper would not have been possible without the provision and donations of various individuals and organizations. I would like to rapid my genuine gratitude to my academic advisors and mentors for their priceless guidance and insights throughout the research process. Their expertise and encouragement have meaningfully shaped my understanding of 6G networks and inspired me to delve deeper into this emerging field. Additionally, I would like to thank my peers for their positive feedback and cooperative spirit, which enriched my research experience.

I also acknowledge the various authors and investigators whose work laid the foundation for this study. Their pioneering efforts in the realm of telecommunications have greatly informed my analysis and conclusions.

Conflict of Interest:

There are no conflicts of interest regarding the publication of this research paper. No financial or personal relationships influenced the research outcomes or interpretations presented herein. The research was conducted independently, and all findings are based solely on the reviewed literature and theoretical frameworks developed during the study.

References

1. Agarwal, B., Poria, S., Mittal, N., Gelbukh, A., & Hussain, A. (2015). Concept-level sentiment analysis with dependency-based semantic parsing: A novel approach. *Springer*.
2. Akhgar, B., Tabatabayi, F., & Bayerl, P. S. (2014). Investigating radicalized individual profiles through fuzzy cognitive maps. *Elsevier*.
3. Al-Zewairi, M., & Naymat, G. (2017). Spotting the Islamist radical within Religious extremists profiling in the United States. *Elsevier*.
4. Ball, L. (2016). Automating social network analysis: A power tool for counter-terrorism. *Springer*.
5. Bobashev, G., Sageman, M., & Evans, A. L. (2019). Turning narrative descriptions of individual behaviour into network visualization and analysis: Example of terrorist group dynamics. *IEEE*.
6. Cherif, W., Madani, A., & Kissi, M. (2014). Integrating effective rules to improve Arabic text stemming. *IEEE*.
7. Drouin, J. (2014). Close- and distant-reading modernism: Network analysis, text mining, and teaching *The Little Review*. *JSTOR*.
8. Frank, R., Bouchard, M., Davies, G., & Mei, J. (2015). Spreading the message digitally: A look into extremist organizations' use of the internet. *Springer*.
9. Ishitaki, T., Obukata, R., & Oda, T. (2017). Application of deep recurrent neural networks for prediction of user behaviour in Tor networks. *IEEE*.
10. Ishitaki, T., Oda, T., & Barolli, L. (2015). Application of neural networks and Friedman test for user identification in Tor networks. *IEEE*.
11. Ishitaki, T., Oda, T., & Barolli, L. (2016). A neural network-based user identification for Tor networks: Data analysis using Friedman test. *IEEE*.
12. Johnston, A. H., & Weiss, G. M. (2017). Identifying Sunni extremist propaganda with deep learning. *IEEE*.
13. Kapitanov, A. I., Kapitanova, I. I., Troyanovskiy, V. M., Shangin, V. F., & Krylikov, N. O. (2022). Approach to automatic identification of terrorist and radical content in social networks message. *IEEE*.

14. Lara-Cabrera, R., & Gonzalez-Pardo, A. (2017). Extracting radicalization behavioral patterns from social network data. *IEEE*.
15. Li, Z., Sun, D., Li, B., Li, Z., & Li, A. (2018). Terrorist group behavior prediction by wavelet transform-based pattern recognition. *Hindawi*.
16. López-Sáncez, D., Revuelta, J., & de la Prieta, F. (2020). Towards the automatic identification and monitoring of radicalization activities in Twitter. *IEEE*.
17. Lourentzou, I., Morales, A., & Zhai, C. X. (2017). Text-based geolocation prediction of social media users with neural networks. *IEEE*.
18. Modupe, A., Olugbara, O. O., & Ojo, S. O. (2014). Filtering of mobile short messaging service communication using latent Dirichlet allocation with social network analysis. *Springer*.
19. Oda, T., Obukata, R., & Yamada, M. (2016). A neural network-based user identification for Tor networks: Comparison analysis of different activation functions using Friedman test. *IEEE*.
20. Sabbah, T., & Selamat, A. (2015). Hybridized feature set for accurate Arabic dark web pages classification. *Springer*.
21. Sabbah, T., & Selamat, A. (2015). Hybridized feature set for accurate content Arabic dark web pages classification. *ResearchGate*.
22. Sabbah, T., Selamat, A., Selamat, M. H., Ibrahim, R., & Fujita, H. (2016). Hybridized term-weighting method for dark web classification. *Elsevier*.
23. Scrivens, R., & Frank, R. (2016). Sentiment-based classification of radical text on the web. *IEEE*.
24. Tundis, A., Bhatia, G., & Jain, A. (2018). Supporting the identification and the assessment of suspicious users on Twitter social media. *IEEE*.
25. Wadhwa, P., & Bhatia, M. P. S. (2015). Tracking online radicalization using investigative data mining. *IEEE*.
26. Yucel, C., & Koltuksuz, A. (2014). An annotated bibliographical survey on cyber intelligence for cyber intelligence officers. *JSTOR*.