

# A Survey on Radical and Terrorist Content Detection using Artificial Neural Networks

Vishal Singh Gurjar<sup>1</sup>; Preeti Ahirwar<sup>2</sup>

M.Tech Scholar<sup>1</sup>, Asst.Professor<sup>2</sup>, Department of Computer Science, VITM Indore<sup>1,2</sup>

## ABSTRACT

Modern day warfare is not limited to the battleground alone but has been waged on the cyberspace domain. Modern terrorist organizations weekly, and even daily put in the Internet space professionally shot and orchestrated videos of public executions, cultural monuments destruction, fighting, interviews with their commanders, the radical preachers and activists, photos of the trophies and killed enemies. Cyber Terrorism has firmly won its place in the international information space and became one of the most important activities of terrorists. Due to the enormity and the complexity of the datasets to be analyzed, manual or even conventional statistical techniques are not competent enough to extract radical content from the large plethora of textual information vented out into cyberspace. Hence it becomes mandatory to use artificial intelligence and artificial neural networks for the purpose. The present work cites the fundamental work done in the domain along with its salient features. Moreover, the fundamentals of neural networks and its applicability to classification problems has also been explained.

**Keywords:** Web Mining, Text mining, radical content, artificial neural networks, classifiers, accuracy.

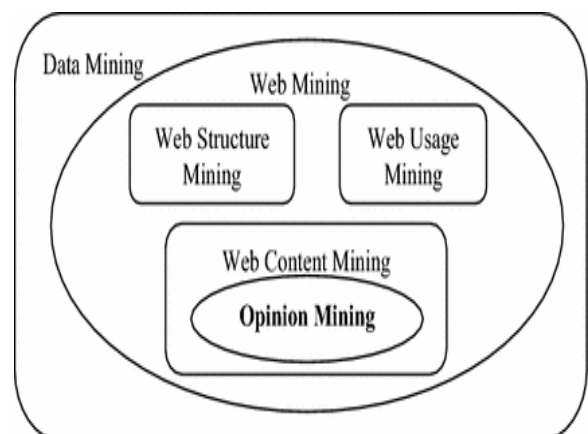
## 1. INTRODUCTION

In the recent years, several terrorist groups have started to make an intensive use of the Internet and various online social networks to spread their message and radicalize vulnerable individuals. In this context, security forces are in charge of detecting and monitoring ongoing radicalization processes, which often take place publicly, in social networks such as Twitter. Unfortunately, effective countermeasures can

only be adopted through early detection, which is not always possible through manual analysis due to the growing amount of information to be analyzed. Hence it is necessary to enable the automatic detection and monitoring of radicalization processes that occur on social media. In particular, the system perform should perform two different tasks:

- (1) Detects influential users with a radicalization agenda, suggesting relevant profiles to human supervisors; and
- (2) Monitors the interactions of confirmed radical users, estimating the risk of radicalization for vulnerable users that interact with them.

This is basically a subset of web mining whose relation to opinion mining and the adjoining concepts are illustrated in the figure below:



**Fig.1 Various sub-sections of web mining pertaining to opinion mining**

The opinion mining workflow starts from the retrieval of useful information from the social network. This is achieved by filtering among all the published tweets. A collection of dictionaries which contain words and

communication patterns used by radical users in different topics is used for the identification of radical users. This corpus is designed earlier by experts during the process. Essentially, the existing system uses several dictionaries that contain common patterns and keywords used by radical users in different domains. These dictionaries may be created by human experts, capturing in this manner their expert knowledge. By doing so, the dictionaries provide a flexible preliminary filter to radical user detection. In addition, as more insight is acquired on the communication habits of a certain group of radical individuals, the set of relevant patterns and keywords can be refined.

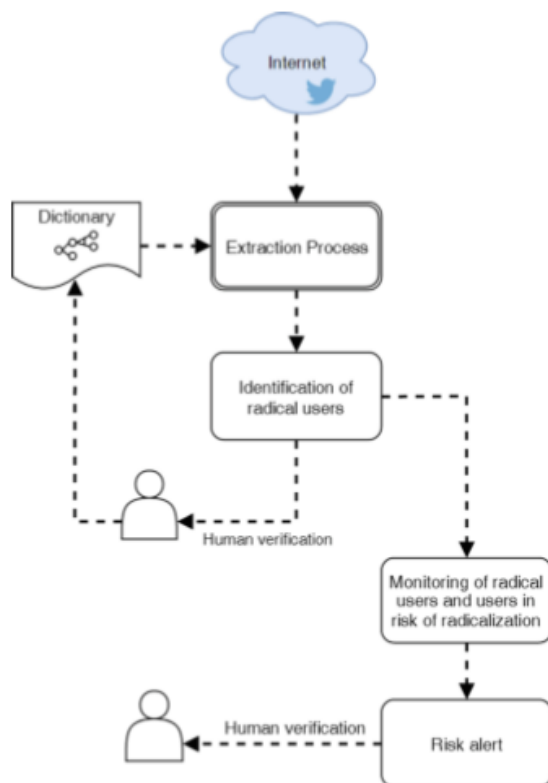


Fig.2 The Operational Schema for Opinion Mining

## 2. ARTIFICIAL NEURAL NETWORKS

Artificial Intelligence and Machine learning have become an increasingly sought after domain in this recent time. Its popularity and dependence can be attributed to the fact that it is very advanced and strong approach. Below are some of the associated concepts of artificial intelligence. Artificial Neural Networks are the mechanism of artificial intelligence that implements it:

**Computational Intelligence:** This refers to the intelligent machines and using machines for high computational work that usually requires huge amounts of human efforts. Here the machine can perform such high end tasks better and more accurately.

**Artificial Intelligence:** It can be defined as the design of computational systems which can perform tasks generally needing human intervention.

**Machine Learning:** This is a branch of computer science that involves making the machine learn akin to humans for problem solving and performing variety of advanced and complex tasks.

**Neural Networks:** Neural Networks can be described as the neuron connection counterpart of the human brain. It has the ability to replicate the functions of human intelligence. The main features of machine learning are given below:-

- The ANN is type of self learning network that can be trained to perform tasks accurately.
- There consists of millions of neurons that are connected to each other. This aids the brain to perform complex tasks and process lots of information. But with ANN, the ANN has the feature of saving the previous input data.
- And this way ANN trains itself based on the data and information that input to it previously.
- This way ANN learns and adapts according to the previously fed data. This is achieved through training and testing of the neural network. This is a crucial aspect as the accuracy of the classification depends on this process.

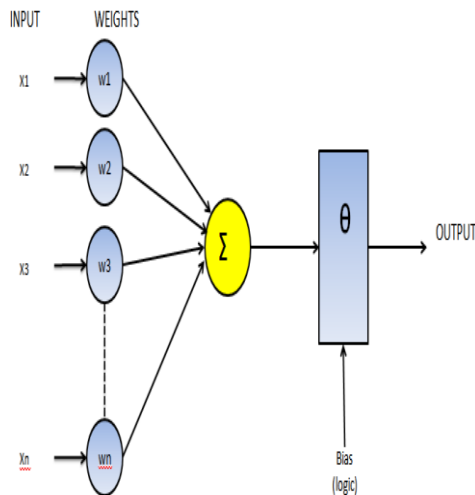


Fig.3 Mathematical Model of ANN

Artificial neural networks are effective in the following problems:

- Forecasting problems
- Classification Problems
- Optimization Problems

In this present case, the ANN is used as a classifier for a classification problem in which the ANN has to decide whether the image is forged or not. The mathematical formulation for the output of the neural network is given by:

$$Y = \sum_{i=1}^n X_i W_i + \theta \quad (1)$$

Here,

X is the parallel input stream fed to the neural network

W is the weights updated as per the changing inputs

Y is the final output or decision of the neural network

θ is the bias.

Training of ANN is of major importance before it can be used to predict the outcome of the data inputs. Neural Networks can be used for a variety of different purposes such as pattern recognition in large and complex data pattern sets wherein the computation of parameters would be extremely daunting for conventional statistical techniques. The weights or the equivalents of experiences are evaluated and updated based on the data patterns which are fed to the neural networks for training.

### 3. PREVIOUS WORK

In this section, the previous approaches used to identify terrorist and radical content on the web has been explained along with its salient features.

In [1], **Kapitonov et al.** showed that terrorist and radical groups of people use instant messengers and accounts on social networks to publish propaganda messages. Blocking such accounts is one of the most effective methods of countering them. To do this, analysts need to read and process a huge amount of information. In this paper authors propose an approach based on machine learning that will automate the process of processing and classifying messages into radical and non-radical messages.

In [2], **Lopez et al.** proposed a novel framework to enable the automatic detection and monitoring of radicalization processes that occur in Twitter. In particular, our system performs two different tasks: Detects influential users with a radicalization agenda, suggesting relevant profiles to human supervisors; and Monitors the interactions of confirmed radical users, estimating the risk of radicalization for vulnerable users that interact with them. Finally, authors present a case study on the monitoring of “Hogar Social Madrid”, a far-right extremist group that operates in Spain and makes an intensive use of social networks. In this case study, authors show how our platform enabled us to identify several profiles immersed in a process of radicalization, which corresponded to young individuals that recently adopted the radical messages and ideas of “Hogar Social Madrid”.

In [3], **Bobashev et al.** proposed an approach where narrative data from the trial of the 1995 Paris Metro and RER bombings was used to extract actors, places, groups and actions that led to the formation of the radical group. This data was dynamically visualized and allowed one to follow the process of terrorist group formation. An important part of the approach is the inclusion of the individuals who were parts of the social network of the radicalized individuals but who did not get radicalized (e.g. members of a soccer team). Authors emphasize the importance of the Natural Language Processing (NLP) in timely information extraction followed by dynamic visualization.

In [4], **Sun et al.** proposed that predicting terrorist attacks by group networks is an important but difficult issue in intelligence and security informatics.

Effective prediction of the behavior not only facilitates the understanding of the dynamics of organizational behaviors but also supports homeland security's missions in prevention, preparedness, and response to terrorist acts. There are certain dynamic characteristics of terrorist groups, such as periodic features and correlations between the behavior and the network. In this paper, authors propose a comprehensive framework that combines social network analysis, wavelet transform, and the pattern recognition approach to investigate the dynamics and eventually predict the attack behavior of terrorist group. The main ideas rely on social network analysis to model the terrorist group and extract relevant features for group behaviors. Next, based on wavelet transform, the group networks (features) are predicted and mutually checked from two aspects. Finally, based on the predicted network, the behavior of the group is recognized based on the correlation between the network and behavior.

In [5], Tundis et al. showed that adoption of a computer-based approach represents a viable solution. In particular, this paper aims at supporting the automatic identification process of potential online suspicious users, who act on social media. A methodological process, centered on the combination of well-known text analysis techniques by considering multi-language aspects, is proposed. In addition, an evaluation approach, based on the exploitation of different qualitative evaluation criteria, is employed to assess the level of suspiciousness of the identified users.

In [6], Zevairi et al. put forth the focus on radical Islamism and hypothesize that Islamist radicals have identifiable information and behavioral traits that could be utilized to identify their ideological motive uniquely amongst other radicals. Four different supervised machine learning algorithms are applied to validate this hypothesis using the "profiles of individual radicalization in the United States" dataset and their performance is compared and discussed. The evaluation results support the authors' hypothesis and show that profiling religious extremists can be achieved with high recall and precision using machine learning models.

In [7], Johnston et al. proposed explored that Sunni extremism poses a significant danger to society, yet it is relatively easy for these extremist

organizations to spread jihadist propaganda and recruit new members via the Internet, Darknet, and social media. The sheer volume of these sites make them very difficult to police. This paper discusses an approach that can assist with this problem, by automatically identifying a subset of web pages and social media content (or any text) that contains extremist content. The approach utilizes machine learning, specifically neural networks and deep learning, to classify text as containing "extremist" or "benign" (i.e., not extremist) content. This method is robust and can effectively learn to classify extremist multilingual text of varying length. This study also involved the construction of a high quality dataset for training and testing, put together by a team of 40 people (some with fluency in Arabic) who expended 9,500 hours of combined effort.

In [8], Ishitaki et al. proposed that due to the amount of anonymity afforded to users of the Tor infrastructure, Tor has become a useful tool for malicious users. With Tor, the users are able to compromise the non-repudiation principle of computer security. Also, the potentially hackers may launch attacks such as DDoS or identity theft behind Tor. For this reason, there are needed new systems and models to detect the intrusion in Tor networks. In this paper, authors present the application of Deep Recurrent Neural Networks (DRNNs) for prediction of user behavior in Tor networks. Authors constructed a Tor server and a Deep Web browser (Tor client) in our laboratory. Then, the client sends the data browsing to the Tor server using the Tor network. Authors use the Wireshark Network Analyzer to get the data and then used the DRNNs to make the prediction. The simulation results show that proposed simulation system has a good prediction of user behavior in Tor networks.

In [9], Lourentzou et al. showed that Inferring the location of a user has been a valuable step for many applications that leverage social media, such as marketing, security monitoring and recommendation systems. Motivated by the recent success of Deep Learning techniques for many other tasks such as computer vision, speech recognition, and natural language processing, we study the application of neural networks to the problem of geolocation prediction and experiment with multiple techniques to improve neural networks for geolocation inference

based solely on text. Experimental results on three Twitter datasets suggest that choosing appropriate network architecture, activation function, and performing Batch Normalization, can all increase performance on this task.

In [10], Lara-Cabrera et al. showed that Social networks (SNs) have become essential communication tools in recent years, generating a large amount of information about its users that can be analysed with data processing algorithms. Recently, a new type of SN user has emerged: jihadists that use SNs as a tool to recruit new militants and share their propaganda. In this paper, we study a set of indicators to assess the risk of radicalisation of a social network user. These radicalisation indicators help law-enforcement agencies, prosecutors and organizations devoted to fight terrorism to detect vulnerable targets even before the radicalisation process is completed. Moreover, these indicators are the first steps towards a software tool to gather, represent, pre-process and analyze behavioral indicators of radicalisation in terrorism.

#### 4. EVALUATION PARAMETERS

The performance of the approaches are accuracy and sensitivity since it's a classification problem that is being dealt with. The performance metrics are discussed below:

$$Se = \frac{TP}{TP+FN} \quad (2)$$

$$Ac = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

Here,

Se indicates sensitivity

Ac indicates accuracy

TP indicates true positive

TN indicates true negative

FP indicates false positive

FN indicates false negative

#### 5. CONCLUSION

It can be concluded from the previous discussions that radial and terrorist activities have infiltrated the cyberspace. Hence it is necessary to identify such activities and report them. However the complexity and the largeness of the data makes it challenging to say the least. Hence it becomes mandatory to use artificial intelligence and artificial neural networks for

the purpose. The present work cites the fundamental work done in the domain along with its salient features. Moreover, the fundamentals of neural networks and its applicability to classification problems has also been explained.

#### 6. REFERENCES

- [1] Andrey I. Kapitanov, Ilona I. Kapitanova, Vladimir M. Troyanovskiy, Vladimir F. Shangin, Nikolay O. Krylikov, "Approach to Automatic Identification of Terrorist and Radical Content in Social Networks Message". IEEE 2018
- [2] D López-Sánchez, J Revuelta, F de la Prieta, "Towards the Automatic Identification and Monitoring of Radicalization Activities in Twitter," IEEE 2018
- [3] G Bobashev, M Sageman, AL Evans, "Turning Narrative Descriptions of Individual Behavior into Network Visualization and Analysis: Example of Terrorist Group Dynamics, IEEE 2018.
- [4] Z Li, D Sun, B Li, Z Li, A Li, "Terrorist group behavior prediction by wavelet transform-based pattern recognition", hindawi 2018.
- [5] A Tundis, G Bhatia, A Jain, "Supporting the identification and the assessment of suspicious users on Twitter social media", IEEE 2018.
- [6] M Al-Zewairi, G Naymat, "Spotting the Islamist Radical within: Religious Extremists Profiling in the United State", Elsevier 2017
- [7] AH Johnston, GM Weiss, "Identifying sunni extremist propaganda with deep learning", IEEE 2017
- [8] T Ishitaki, R Obukata, T Oda, "Application of deep recurrent neural networks for prediction of user behavior in tor networks", IEEE 2017
- [9] I Lourentzou, A Morales, CX Zhai "Text-based geolocation prediction of social media users with neural networks", IEEE 2017
- [10] R Lara-Cabrera, A Gonzalez-Pardo, "Extracting radicalisation behavioural patterns from social network data" IEEE 2017
- [11] L Ball, "Automating social network analysis: A power tool for counter-terrorism", Springer 2016.
- [12] T Ishitaki, T Oda, L Barolli, "A neural network based user identification for Tor networks: Data analysis using Friedman test", IEEE 2016
- [13] T Oda, R Obukata, M Yamada, "A Neural Network Based User Identification for Tor Networks: Comparison Analysis of Different Activation Functions Using Friedman Test", IEEE 2016

[14] T Sabbah, A Selamat, MH Selamat, R Ibrahim, H Fujita, "Hybridized term-weighting method for dark web classification", Elsevier 2016  
[15] R Scrivens, R Frank, "Sentiment-based Classification of Radical Text on the Web", IEEE 2016  
[16] T Sabbah, A Selamat, "Hybridized Feature Set for Accurate Arabic Dark Web Pages Classification", Springer 2015  
[17] T Ishitaki, T Oda, L Barolli, "Application of Neural Networks and Friedman Test for User Identification in Tor Networks" IEEE 2015

[18] R Frank, M Bouchard, G Davies, J Mei, "Spreading the message digitally: A look into extremist organizations' use of the internet", Springer 2015  
[19] T Sabbah, A Selamat, "Hybridized Feature Set for Accurate Content Arabic Dark Web Pages Classification", researchgate, 2015  
[20] Basant Agarwal, Soujanya Poria, Namita Mittal, Alexander Gelbukh, Amir Hussain, "Concept-Level Sentiment Analysis with Dependency-Based Semantic Parsing: A Novel Approach", Springer 2015

**ijournals**