



library@chuka.ac.ke; www.chuka.ac.ke

EFFECTIVENESS OF SOCIAL MEDIA ANALYTICS COUNTERTERRORISM TECHNOLOGY (SMACT) ON TERRORISM CONTAINMENT RATES IN LAMU COUNTY BEACH TOURISM DESTINATION, KENYA

Biwott G. K.¹, Muriuki L. M.², Too E. C.¹

*1*Department of Environmental Studies and Resources Development, Chuka University; P.O. Box 109-60400, Chuka
2 Department of Environmental Studies and Resources Development, Chuka University P.O. Box 109-60400, Chuka
 Department of Computer Science and ICT, Chuka University, P.O. Box 109-60400, Chuka

*biwotkiprotich@gmail.com , mmuriuki@chuka.ac.ke, echebet@chuka.ac.ke

Citation:

K. Biwott G , M.Muriuki L. and C. Too . (2024). Effectiveness of Social Media analytics counterterrorism Technology (smact) on Terrorism containment rates in Lamu county beach tourism destination, Kenya
In: Mutembei Henry, Nduru Gilbert, Munyiri Shelmith, Gathungu Geoffrey, Kiboro Christopher, Otiso Wycliffe, Rithaa Jafford, Miriti Gilbert, Gichumbi Joel, Mwathi David, Gitonga Lucy, Nanua Jackin, Kahindi Roseline, Jonathan Kathenge & Muthui Zipporah (Eds.). Proceedings of the Chuka University Tenth Annual International Research Conference held in Chuka University, Chuka, Kenya from 5th to 6th October, 2023.314-321 pp.

ABSTRACT

Fear of terrorism has led to social and economic decline particularly in beach tourism destinations. The main approaches used in managing terrorism include hard and soft strategies such as military and counter-radicalization. Previous studies have reported the capabilities of social media analytics in detecting terror threats through media streams. However, the effectiveness of this technology has not been examined in beach tourism destinations. This study examines the effectiveness of social media analytics counterterrorism technology (SMACT) in identifying terror threats in tourism destinations. The aim of the research is to determine the effectiveness of SMACT technology on terrorism containment rates in Lamu County beach tourism destination. Descriptive research and machine learning is used to process Twitter dataset using Python. A dataset of 9,572 tweets is preprocessed. Naive Bayes and Recurrent Neural Network (RNN) sentiment analysis models are implemented and evaluated to categorize terrorism-related tweets as positive or negative. A dataset of 5840 tweets is processed after preprocessing and split 80:20 into train and test sets models are developed and trained. The trained models are used to predict sentiment on the 20% test set. A total of 1168 tweets counts are predicted on the test set for each model. Naive Bayes model predicts 719 positive and 449 negative tweets. The RNN model predicted 829 positive and 339 negative tweets. The Naive Bayes and RNN models demonstrate highly accurate detection of extremist sentiment in tweets, though the Naive Bayes classifier outperformed the RNN model. The Naive Bayes model predicted 61.6% of tweets as positive sentiment and 38.4% as negative. In contrast, the RNN model predicted a 71:29 split between positive and negative tweets. Frequently occurring terrorism-related terms include 'attack', 'kill', 'bomb' among others. Twitter terrorism and counterterrorism tweets sentiments are successfully analyzed, giving important insights into the prevalent opinions on the platform. The sentiment distribution and correlations between positive and negative feelings are clustered. The results help researchers, policy makers and

other stakeholders in counterterrorism efforts gain a better grasp of public opinion on Twitter.

Keywords: sentiment analysis, Twitter, terrorism, counterterrorism, social media, dataset, and data preprocessing.

INTRODUCTION

This report presents findings on a research conducted on sentiment analysis on a dataset of Twitter tweets related to terrorism and counterterrorism. The aim of the research is to analyze the sentiment distribution and gain insights into the prevailing attitudes expressed on Twitter regarding these topics. The analysis involves data preparation, cleaning and sentiment analysis. Naive Bayes and Recurrent Neural Network (RNN) sentiment analysis models are implemented and evaluated to categorize terrorism-related tweets as positive or negative.

A significant amount of data is generated as well as being made available to internet users with recognized development and growth of online technologies. Internet has evolved into platform for online education, idea sharing, and exchange social networking platforms, such as Facebook, Twitter, Google+ are quickly becoming more popular since they enable users to engage in discussion, exchange ideas, and other forms of discourse with other communities, or send messages over the globe. Numerous studies have been conducted in the area of sentiment analysis of data on twitter (Kharde and Sonawane, 2016).

Sentiment analysis is a procedure that uses Natural Language Processing (NLP) to automatically mine attitudes, opinions, perspectives, and emotions from text, speech, tweets, and database sources. In a sentiment analysis, opinions in a text are categorized into "positive," "negative," and "neutral" categories (Kharde and Sonawane, 2016).

Various scholars have reported the capabilities of SMACT as an approach to manage terrorism through media streaming. Adwan *et al.* (2020) investigates the capabilities of twitter sentiment analysis approaches and algorithms that have been use for sentiment analysis in Twitter. The authors surveys various articles resulting from studies

conducted by various scholars. Over 40 articles are reviewed and categorized as machine learning, lexicon-based, hybrid-based and graph-based. According to Adwan *et al.*, (2020), machine learning approaches which utilize machine learning classifiers include Support Vector Machine (SVM) LibLinear model.

According to (Jain & Vaidya, 2020), social media is ubiquitously present in all spheres of life including education, health care, business, disaster management, politics, tourism industry, as well as, the use of media sharing and entertainment. Apart from all such conveniences provided by the social media, it does have a darker side to cast. Misuse of social media also needs to be accounted for. On one hand, this may seem to abridge the communication gap and faster news delivery among people; on the other hand, it is being heavily misused by many; misuse on a level of genocide, murders, bombings and conspiracies. Social media platforms have provided terrorists with an enhanced capacity to distribute their propaganda selectively to specific audiences, innovate novel and interactive user-generated forms of propaganda, and enable these groups to engage in advanced brand-building efforts (Droogan *et al.*, 2018). In a study conducted by Medina, the author states that about 90% of terrorist activities online are conducted via social media platforms while 76% of U.K. terrorists engage in the internet to research and strategize their actions.

Jain & Vaidya (2021) provides an overview of research conducted by different authors over the past decade regarding the utilization of social media in response to terrorist attacks. The authors explore the ways in which social media can be employed for public communication with emergency agencies, military, or law enforcement during such incidents. Additionally, the study examines into the post-attack analysis of social media data and the identification of acts related to terrorism, civil unrest, and hate through social media analytics. The authors believe that there is an urgent necessity to expand the scope of data analysis significantly, both in terms of scale and frequency. This expansion is crucial not only for identifying acts of terrorism on social media but also for enhancing safety measures, taking preventive actions, and conducting post-attack investigations.

Trabelsi *et al.* (2023), conducts an extensive exploration of a variety of machine and deep learning techniques utilized in the analysis of sentiment within Twitter content. Their primary objective is to investigate the impact of malicious activities on human security and safety within the context of social networks. They systematically evaluate the strengths, weaknesses, and recent trends within this field, conducting a comprehensive survey that encompass a broad spectrum of sentiment classification methods and algorithms. These approaches are rigorously tested on diverse datasets by various researchers. The study advances understanding of Twitter Sentiment Analysis, with a particular focus on lexicon-based strategies, including dictionary-based, corpus-based, and machine learning-based methods such as SVM, Bayesian Networks, Maximum Entropy, Naive Bayes, and Neural Networks. Notably, the analysis indicated that machine learning-based techniques are the most widely adopted by researchers, with Support Vector Machine and Naïve Bayes being the prevailing choices, although the highest level of accuracy was attained using the AdaBoost classifier.

Droogan *et al.* (2018) employed machine learning techniques to analyze sentiment on Twitter in Asia Pacific. They utilized the Twitter streaming API to collect a dataset comprising 10,332 tweets containing keywords related to terrorism. Subsequently, the authors conducted data cleaning and preparation, consolidating 10,322 tweets into a single corpus. To categorize synonyms and antonyms associated with words containing "terrorism" in their titles, they developed a dictionary that segregated these terms into positive and negative categories. This lexicon comprised 3,824 negative terms and 1,900 positive ones. The proposed methodology, which relies on feature extraction using the "Bag-of-Words" approach, calculated the cumulative score for each tweet's text by summing the scores of words present in the training data. Naive Bayes classifiers were then utilized to assign classifications to each tweet based on the training data.

The importance of sentiment analysis has grown significantly due to the rise of social media platforms. It allows both businesses and researchers to track real-time discussions and reactions to various events. Sentiment analysis algorithms assess text through diverse techniques, including machine learning, deep learning, and natural language processing (Nirbhik, 2023).

According to Nirbhik (2023), sentiment analysis, particularly opinion mining, has become a crucial tool for detecting and monitoring extremist actions on social media. Deep learning model, which utilizes the Distil BERT algorithm, seeks to enhance classification accuracy by incorporating both text and emoticons for sentiment analysis. This model effectively captures sentiment conveyed in both textual content and emoticons, underscoring the importance of

considering emoticons in sentiment analysis. Utilizing sentiment analysis has the capacity to significantly aid in monitoring social media, ultimately supporting the endeavors to counteract terrorism.

Kenya is widely recognized as a symbol of stability and tranquility within the Horn of Africa, the broader Eastern Africa region, and indeed, across the African continent. It plays a pivotal role as an economic and commercial center, attracting both domestic and international investors. Nevertheless, the specter of terrorism has posed a significant threat to Kenya's peace and stability. This menace has eroded citizens' freedom of association and movement while instilling a pervasive sense of fear and intimidation. These adverse effects have hindered the spiritual, economic, and social progress of individuals. Sentiment analysis and mapping offer valuable tools for the timely and effective identification, detection, and tracking of terrorist activities in Kenya. This can enable actionable responses to safeguard its security and well-being (Ngoge & Otero, 2017).

Social Media Analytics for Combating Terrorism Model (SMACT)

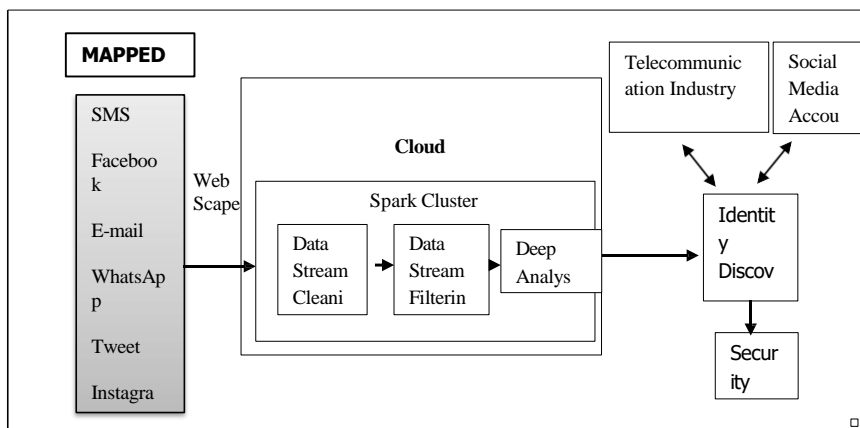


Figure 2: Social Media Analytics for Combating Terrorism (SMACT) Model, (Kolajo and Daramola, 2017)

METHODOLOGY

The researcher utilized supervised machine learning techniques particularly focusing on processing a Twitter dataset using Python and descriptive study to examine the efficacy of social media analytics counterterrorism technology (SMACT).

Twitter dataset containing 9752 terrorism and counterterrorism tweets which was treated as population of the study.

Terrorism and counterterrorism tweets were sampled using stratified sampling with the use of multicriteria decision making approach using excel. Data was divided into strata and sample of specified size taken from each stratum.

The researcher chose 20 themes to sample the dataset based on the type of tweet communicated on twitter. These included the following terms; terror (30%), attack (14%), kill (12%), war (11%), milit (8%), target (5%), bomb (4%), death (4%), die (4%), murder (2), crime (2), explo (1), injur (1), shoot (1), recruit (1), capture (1), fear (0%), shot (0), kidnap (0) and grenade (0). Total sample size was 5840 tweets which was considered as sample population. This is illustrated in the graph below: -

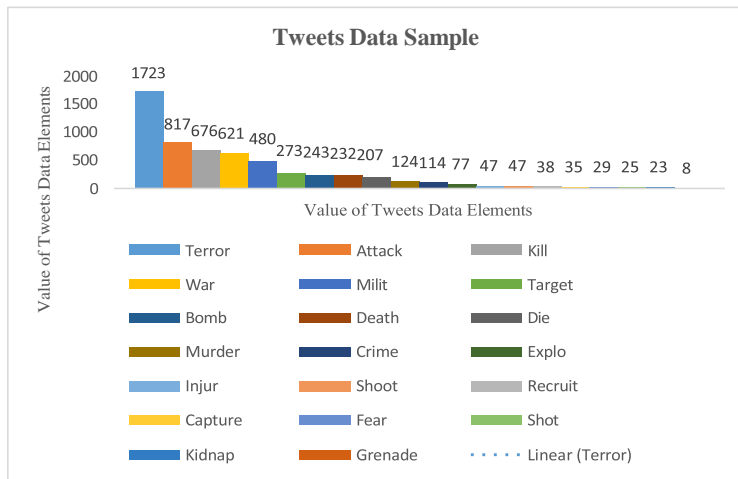


Figure 3: Stratified sample population of Terrorism and Counterterrorism Tweets Dataset

Total sample size = 5840 tweets

A dataset containing tweets related to terrorism and counterterrorism was collected from <https://www.kaggle.com/datasets/shaileshkankarej2001/dataset-of-terrorism-and-anti-terrorism-tweets> by the researcher in form of csv excel file. The dataset includes information such as the tweet content and associated labels.

Python programming language was used to upload and process the downloaded dataset. Python is a modern programming language that supports object-oriented, functional, and imperative programming styles. It can be used for machine learning to analyze data (Kelly & Kelly, 2019). Its versatility and user friendly, making it one of the most popular programming languages available.

The researcher started by importing the necessary libraries, including pandas, numpy, nltk, and sklearn. The pandas library was used to handle the data in tabular format, numpy for numerical computations, nltk for text processing, and sklearn for data visualization. The researcher then loaded the dataset, "tweets.csv," using the pandas library's `read_csv` function. Encoding was specified as 'ISO-8859-1' to handle any encoding issues. The dataset contained columns such as "Tweet" and "label," which represented the tweet content and its associated label (terrorism or counterterrorism).

The initial dataset of 5840 tweets is preprocessed, involving tasks like cleaning, tokenization, and removing noise from the tweets. To ensure reliability of analysis, the researcher performed data cleaning. He focused on two columns, "Tweet" and "label." For each column, he checked if it was of object type (string). If so, he removed special characters like '@' and '#' using the `str.replace` function. Additionally, he removed URLs from the tweets using a regular expression pattern. Null values were dropped from the dataset, and duplicate rows were removed.

Sentiment Analysis of Twitter Terrorism and Counterterrorism Tweets

The research employs Naive Bayes and Recurrent Neural Network (RNN) sentiment analysis models to categorize terrorism-related tweets as either positive or negative sentiment. These models are developed and trained on a dataset of 5,840 preprocessed tweets. After preprocessing, the subset of 5,840 terrorism and anti-terrorism tweets are divided into a training set (80%) and a test set (20%). The trained models are then employed to predict sentiment on the test set.

RESULTS AND DISCUSSIONS

Model Performance and Evaluation

The predictions from each model on the test set were compared to the true labels to evaluate performance using accuracy, precision, recall, F1 score, and confusion matrices. Naive Bayes model achieved 99% accuracy on the test set while RNN model gained 77% test accuracy as shown in Table 1. Both models performed very well in predicting positive and negative tweets.

Metric	Naive Bayes	RNN
Accuracy	0.99	0.77
Positive Precision	0.98	0.76
Positive Recall	1.00	0.93
Negative Precision	1.00	0.82
Negative Recall	0.98	0.51
Positive F1	0.99	0.84
Negative F1	0.99	0.63

Table 1: Model Evaluation Metrics on Test Set

Confusion Matrices

The visualization of the models' performance is facilitated through confusion matrices, which provide a clear depiction of the correct and incorrect predictions. The matrices presented in Figure 1 and Figure 2 reveal that very few errors were made by both models on the test set, emphasizing their robustness and efficacy in sentiment classification.

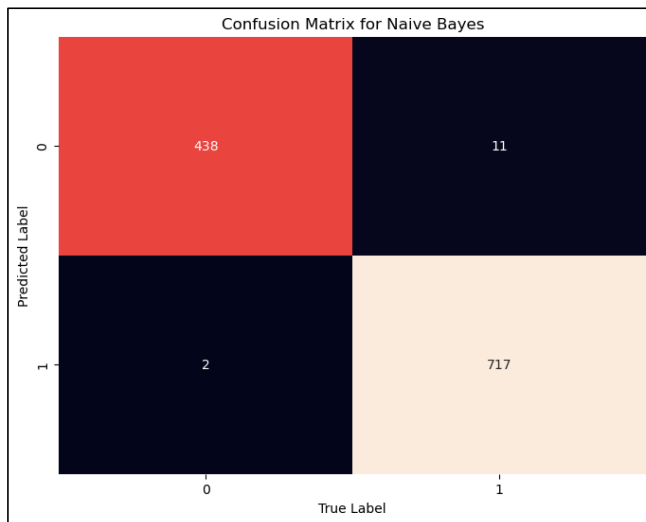


Figure 1: Confusion matrix for Naive Baye

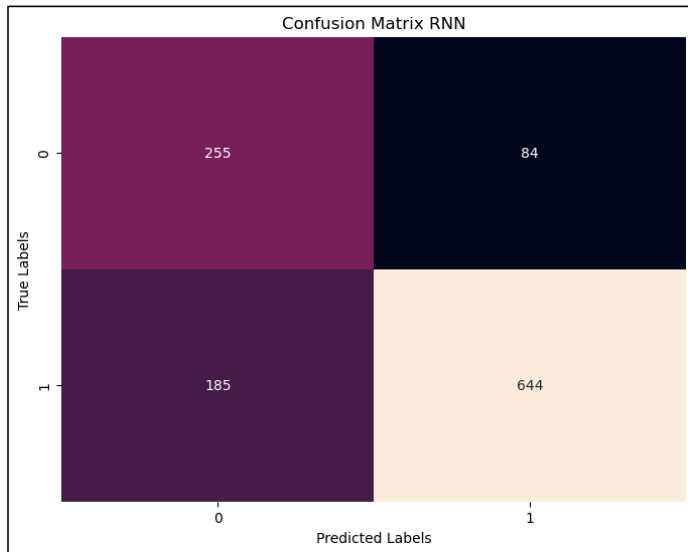


Figure 2: Confusion matrix for RNN

The Naive Bayes and RNN models demonstrate highly accurate detection of terrorism sentiment in tweets, though the Naive Bayes classifier outperformed the RNN model. The visualization in Figure 1 shows the Naive Bayes model predicted 61.6% of tweets as positive sentiment and 38.4% as negative. In contrast, the RNN model predicted a 71 % and 29 % split between positive and negative tweets as seen in Figure 2.

In total, 1168 tweet counts are predicted by each model on the test set. Impressively, both Naive Bayes and RNN models exhibit high accuracy in identifying extremist sentiment in tweets, with Naive Bayes outperforming RNN. Specifically, Naive Bayes achieves 99% accuracy on the test set compared to RNN's 77%.

The Naive Bayes model predicts 719 positive and 449 negative tweets, attributing 61.6% as positive sentiment and 38.4% as negative. Conversely, the RNN model predicts 829 positive and 339 negative tweets, resulting in a 71 % and 29% split. The sentiment predictions of each model on the test set were juxtaposed with the true labels to evaluate their performance.

Table 2: A summary of the findings

Model	Tweets Sentiments		Percentage		Probability Rank		Accuracy
	Positive	Negative	Positive	Negative	Positive	Negative	
Naive Bayes	719	449	61.6 %	38.4 %	0.6	0.4	99 % (0.9)
RNN	829	339	71	29	0.7	0.3	77 % (0.7)

CONCLUSION

The study successfully analyzes sentiments related to terrorism and counterterrorism tweets, providing insights into prevailing opinions on the Twitter platform. The sentiment distribution and correlations between positive and negative feelings are clustered. The study demonstrates the potential of using social media analytics and machine learning techniques to analyze sentiments and detect extremist content on Twitter, particularly in the context of beach tourism destinations and their counterterrorism efforts. The research findings offer a comprehensive blueprint for advancing security and counterterrorism efforts in beach tourism destinations. By embracing technological advancements, stakeholders can create an environment that is both secure and welcoming for tourists. This approach not only safeguards against threats but also ensures sustainable tourism growth, prioritizing the safety and well-being of all stakeholders involved

RECOMMENDATIONS

A continuous investment in upgrading and optimizing SMOACT technology is essential. This ensures that the system can perform real-time data analysis, allowing for the early detection of potential threats. Collaborative partnerships with relevant security agencies are crucial as well. These partnerships facilitate a swift response in the event of any detected threats, ensuring a coordinated approach to security management. It's important to foster regular training sessions for tourism stakeholders to familiarize them with SMOACT technology and emergency protocols, equipping them to respond effectively during crises.

WAY FORWARD

The research findings provide a clear path to enhance security and counterterrorism efforts in beach tourism destinations. The demonstrated effectiveness of Social Media Analytics Counterterrorism Technology (SMOACT) underscores the potential for a holistic approach. To capitalize on these findings, a strategic focus on technological advancements is essential. Continued research and development efforts should be directed towards refining SMOACT's capabilities. Incorporating advanced machine learning techniques and harnessing natural language processing can significantly improve the accuracy and predictive power of the technology, enabling authorities to stay ahead of evolving threats.

Equally important is the commitment to continuous training and skill development. Stakeholders, including security personnel and tourism professionals, should undergo regular training to ensure effective utilization of SMOACT tools. This proactive approach guarantees that the latest advancements are effectively employed to maintain security and manage potential crises.

Collaboration emerges as a key driver for success. Collaborative partnerships between government agencies, local authorities, tourism boards, and technology providers should be fostered. These partnerships facilitate the sharing of data, expertise, and resources, enabling comprehensive threat assessment efforts. Regular dialogues among stakeholders create a holistic and united approach to security and counterterrorism.

REFERENCES

- Adwan, O. M. A. R., Al-Tawil, M., Huneiti, A., Shahin, R., Zayed, A. A., & Al-Dibsi, R. (2020). Twitter sentiment analysis approaches: A survey. *International Journal of Emerging Technologies in Learning (IJET)*, 15(15), 79-93.
- Ali, G. A. (2016). Identifying terrorist affiliations through social network analysis using data mining techniques.
- Al-Shaibani, H. A., & Al-Augby, S. (2022, May). Terrorist Tweets Detection using Sentiment Analysis: Techniques and Approaches. In *2022 5th International Conference on Engineering Technology and its Applications (IICETA)* (pp. 585-590). IEEE.
- Droogan, J., Waldek, L., & Blackhall, R. (2018). Innovation and terror: An analysis of the use of social media by terror-related groups in the Asia Pacific. *Journal of Policing, Intelligence and Counter Terrorism*, 13(2), 170- 184.
- Ghanem, N. A., & Habeeb, H. M. (2021, July). Classifying Suspicious Content on Social Media Networks. In *2021 International Conference on Advanced Computer Applications (ACA)* (pp. 171-175). IEEE.
- Jain, P. N., & Vaidya, A. S. (2021). Analysis of social media based on terrorism—A review. *Vietnam Journal of Computer Science*, 8(01), 1-21.
- Kharde, V., & Sonawane, P. (2016). Sentiment analysis of twitter data: a survey of techniques. *arXiv preprint arXiv:1601.06971*.
- Medina, V. (2016). Terrorism Undermines the Credibility of Moral Relativism.
- Ngoge, L., & Orero, J. O. (2017). Mapping of terrorist activities in Kenya using sentiment analysis.
- Nirbhik, N. (2023). Integrating Text and Emoticons for Detecting Extremist Affiliations On Twitter Using Deep Learning (Doctoral dissertation).
- Thapa, B. (2022). Sentiment Analysis of cybersecurity content on Twitter and Reddit. *arXiv preprint arXiv:2204.12267*.
- Trabelsi, Z., Saidi, F., Thangaraj, E., & Veni, T. (2023). A survey of

extremism online content analysis and prediction techniques in twitter based on sentiment analysis. *Security Journal*, 36(2), 221-248.