



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 3, March 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

A Framework for Analyzing Real-Time Tweets to Detect Terrorist Activities

Prof Aparna Patil¹, Vaishali Nachan², Jagruti bagul², Pranjli Pisal², Mansi Bansode²

Professor, Department Computer Engineering, Genba Sopanrao Moze College of Engineering, Balewadi, Pune, India¹

Student, Department Computer Engineering, Genba Sopanrao Moze College of Engineering, Balewadi, Pune, India²

ABSTRACT: Social media are interactive computer mediated technology that facilitates the sharing of information via virtual communities and networks. And Twitter is one of the most popular social media for social interaction and microblogging. This paper introduces an improved system model to analyze twitter data and detect terrorist attack event. In this model, a ternary search is used to find the weights of predefined keywords and the Aho-Corasick algorithm is applied to perform pattern matching and assign the weight which is the main contribution of this paper. Weights are categorized into three categories: Terror attack, Severe Terror Attack and Normal Data and the weights are used as attributes for classification. K-Nearest Neighbor (KNN) and Support Vector Machine (SVM) are two machine learning algorithms used to predict whether a terror attack happened or not. We compare the accuracy with our actual data by using confusion matrix and measure whether our result is right or wrong and the achieved result shows that the proposed model performs better..

KEYWORDS: K-Nearest Neighbor (KNN) and Support Vector Machine (SVM)

I. INTRODUCTION

Detecting and removing terrorist related content on the Internet is an important and difficult task for law enforcement agencies all over the world. Jihadist groups, and specifically ISIS, have been able to maintain a persistent online presence by sharing content through a broad network of "mediamujahideen". The internet has been identified by senior Sunni extremists as a "battlefield for jihad, a place for missionary work, a field of confronting the enemies of God". This was further encouraged by a "Twitter Guide" (dalil Twitter) posted on the Shumukh al-Islam forum which outlined reasons for using Twitter as an important arena of the electronic front (ribat). Since 2011 the Syrian conflict, recognized as the most "socially mediated" in history, has developed into the new focal point for jihadi media culture

II. LITERATURE SURVEY

Paper Title	Author	Methodology
Tweeting for the caliphate: Twitter as the new frontier for jihadist propaganda.	A. Fisher and N. Prucha	Comparison of different machine algorithms
The call-up: The roots of a resilient and persistent jihadist presence on twitter	M. Lynch, F. Deen, and S. Aday,	SVM and Random forest algorithm
"Online territories of terror: how jihadist movements project influence on the internet and why it matters offline,	A. Zelin	Tweets are detected using LSTM

III. PROBLEM DEFINATION

This work is aiming at detecting tweets that are involved in terrorist activity - the supporters of terrorist groups who disseminate propaganda content online.

To do this we use a machine learning approach where we make use of two sets of features: data dependent features and data independent features.

The data dependent features are features that are heavily influenced by the specific dataset while the data independent features are independent of the dataset and can be used on other datasets with similar result

IV. PROPOSED SYSTEM

Extract Twitter Data :

We extracted social data using Twitter 4j API in JAVA based on Hashtags.

Pre-processing the Dataset:

Pattern Matching and Weight Assigning (PMWA) is introduced to find the weights of filtered words. Weights help us to find the words which having harsh language.

Classifying the data:

For classifying these data, we use a machine learning algorithm that is SVM to predict the different phases and also use confusion matrix for calculating the accuracy

SVM Algorithm:

1. Import the dataset.
2. Explore the data to figure out what they look like.
3. Pre-process the data.
4. Split the data into attributes and labels.
5. Divide the data into training and testing sets.
6. Train the SVM algorithm.
7. Make some predictions.

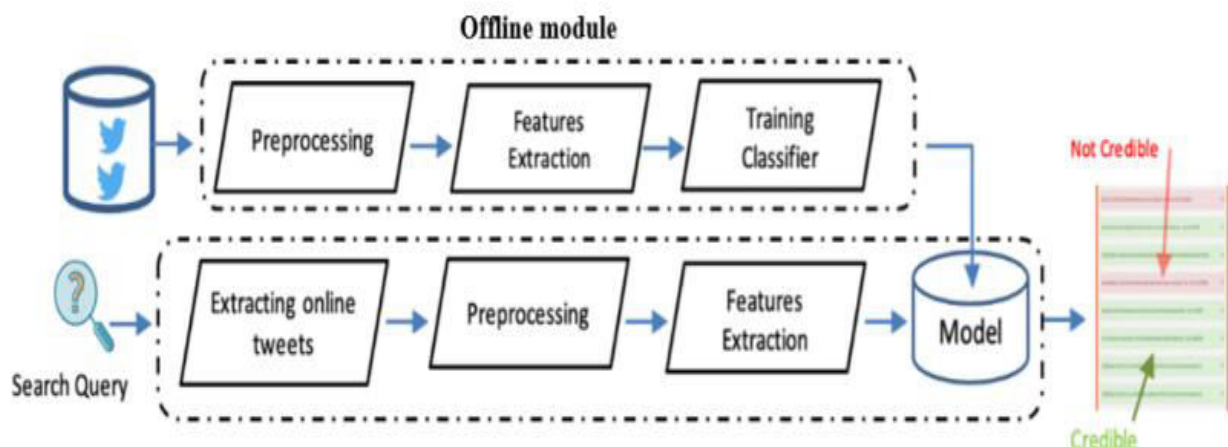


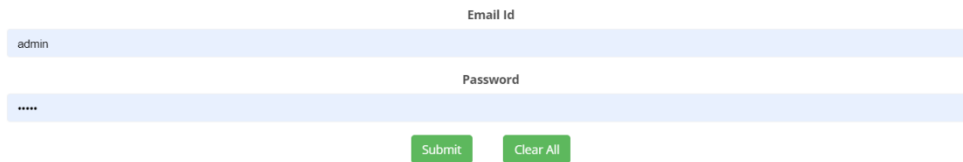
Fig 1. Architecture Diagram

V. PROPOSED SYSTEM

Login Page:

There are two type of user 1. Admin which can see if any of the post is the terror post. User after login can post the messages.

Login Form !

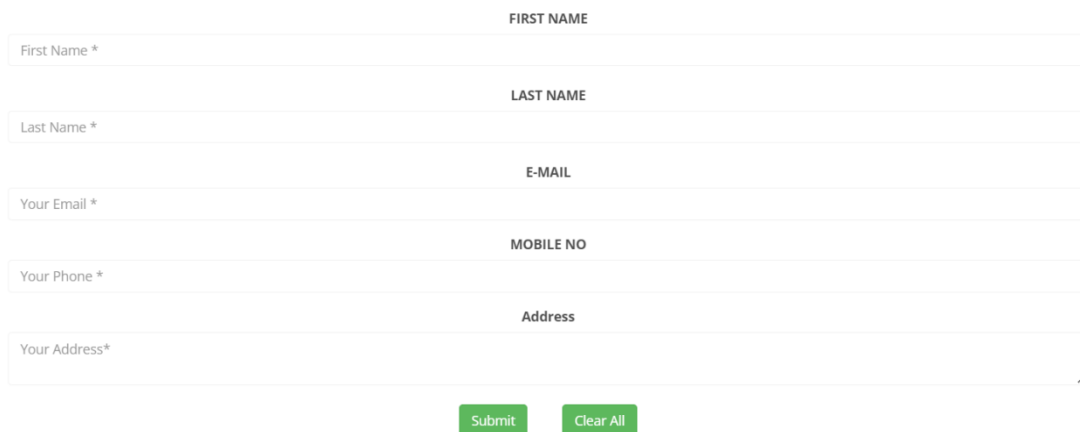


A screenshot of a login form. It has two input fields: 'Email Id' with the text 'admin' and 'Password' with masked characters '.....'. Below the fields are two green buttons: 'Submit' and 'Clear All'.

Login Screenshot

Registration Page: User need to fill personal details.Once fill it will send email to user to confirm the identity.

Registration Form !



A screenshot of a registration form with five input fields: 'First Name *', 'Last Name *', 'Your Email *', 'Your Phone *', and 'Your Address*'. Each field has a label above it: 'FIRST NAME', 'LAST NAME', 'E-MAIL', 'MOBILE NO', and 'Address'. Below the fields are two green buttons: 'Submit' and 'Clear All'.

Registration Screenshot

VI. CONCLUSIONS

In this paper we have used machine learning to classify tweeps and tweets as being multipliers of jihadism. When using machine learning there is always the risk that the models that are built only are applicable on the specific dataset.

REFERENCES

- [1] A. Fisher and N. Prucha, "Tweeting for the caliphate: Twitter as the new frontier for jihadist propaganda." in CTC Sentinel 6.6 19-23, 2013.
- [2] A.Fisher and N.Prucha, "The call-up: The roots of a resilient and persistent jihadist presence on twitter," in CTX Vol.4 No.3, 2014.
- [3] M. Lynch, F. Deen, and S. Aday, "Syria's socially mediated civil war." in United States Institute Of Peace 91.1 1-35, 2014.
- [4] N. Prucha, "Online territories of terror: how jihadist movements project influence on the internet and why it matters offline," in Dissertation, University of Vienna, 2015.
- [5] A. Zelin, "The state of global jihad online. a qualitative, quantitative, and cross-lingual analysis," in New America Foundation, 2013.
- [6] N. Prucha, Jihadist Innovation and Learning by Adapting to the New and Social Media Zeitgeist. Taylor & Francis, 2015. [Online]. Available: <https://books.google.se/books?id=Q2ShCAAQBAJ>
- [7] A. Abbasi, "Affect intensity analysis of dark web forums," in Intelligence and Security Informatics, 2007 IEEE, May 2007, pp. 282–288.



- [8] H. Chen, “Sentiment and affect analysis of dark web forums: Measuring radicalization on the internet.” in ISI. IEEE, 2008, pp. 104–109.
- [9] M. Yang, M. Kiang, Y. Ku, C. Chiu, and Y. Li, “Social media analytics for radical opinion mining in hate group web forums,” Journal of homeland security and emergency management, vol. 8, no. 1, 2011.
- [10] W. I. MagdyWalid, “#failedrevolutions: Using twitter to study the antecedents of isis support,” arXiv preprint arXiv:1503.02401, 2005. [



INNO  SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165


doi[®]
crossref

 INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA


निस्कयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details