Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778376

DETECTION OF CYBER CRIME ON SOCIAL MEDIA NETWORKS USING MACHINE LEARNING ALGORITHMS

Dr. R. Aravind
Assistant Professor, Department of Computer Science, Gobi Arts & Science College (Autonomous), Gobichettipalayam Tamilnadu,India.

Dr S Govindaraju
MCA MPhil PhD, Associate Professor, PG and Research Department of Computer Science
Sri Ramakrishna College of Arts & Science, Nava India Peelamedu, Tamilnadu,India.

Dr. P.E.Elango
Assistant Professor, Department of Computer Science, Gobi Arts & Science College (Autonomous), Gobichettipalayam Tamilnadu, India, Coimbatore 641006

Social Media Cyber bullying Detection using Machine Learning

Preprocessing

Preprocessing involves cleaning up the data by removing noise and extraneous text.

1.1 Feature Extraction

The features extraction stage is the second step. The textual input is changed in this step into a format that may be used to feed machine learning algorithms. In this step, TFIDF and sentiment analysis are applied.

1.2 Detection and Prevention measures for Cyberbullying and Online Grooming

In this system, individuals can post messages and photographs on a social media network similar to Facebook. The posting of adult photos, inappropriate comments, and other material is prohibited by this system.

The User Messages are categorised using the Bad Words Dataset and the Sensitive Words Dataset in this case, and the user's bad count is entered into the database. Any user who submits too many offensive or pornographic photographs will immediately be banned from this social networking site.

1.3 Adult Image Detection

Any user who submits an adult image will receive a warning. Before their account is blocked, each user has a limited number of opportunities. If the user is discovered to be submitting this type of stuff, there is a clause for the database item that determines whether or not the account may be kept open.

1.4 Irrelevant Posts Detection Algorithm

This algorithm extracts keywords from text files containing different categories of data and user messages are scanned to find whether they contain those keywords to classify messages into the Crime/Worst/Riots category and to find the sentiment of a message.

1.5 NLP Algorithm

A approximate idea of a user's social standing can be obtained by analysing comments, the percentage of positive or negative responses, and sentiment analysis using different text mining modules. User posts are processed into tree structures, and the words within those tree structures are subsequently analysed to determine the posts' sentiments.

2. MACHINE LEARNING TECHNIQUES

2.1 Naive Bayes

It is one of the classifiers that work based on the Bayes probability theorem. It predicts the associative probability of each class by determining if the given tweet belongs to a specific category of the threat class.

2.2 Decision Tree

It is a model that resembles a tree, with different nodes standing for different types of tweet messages. The dataset's input tweets are sorted from root node to terminal node.

2.3 Support vector Machine

It is a supervised machine learning approach that may be applied to both classification and regression issues. The hyperplane is initially created in an N-dimensional environment that clearly categorises the threat tweet data points. The current hyperplane is also updated to include the new data points.

2.4 Random Forest

The outcome of Random Forest is based on the prediction of the Decision Tree. The average of each decision tree-time bases the precision. Therefore, multiple decision trees are used to calculate the accuracy rate.

3. DETECTION ALGORITHMS USED IN MACHINE LEARNING

3.1 Adult Image Detection Algorithm

The Nudity Detection Algorithm is mostly based on observations that nude images typically contain a lot of skin, persons have varying skin tones, and skin Areas in naked pictures are really near to one another.

To classify skin and skin pixel identities in a picture is necessary for these findings. To determine whether skin pixels are connected or form continuous patches, the diagnosed skin pixels are analysed.

1. Detect skin tone pixels within the image.
2. Locate or shape skin regions based on the detected skin pixels.
3. Analyze skin regions for clues of nudity or nonnudity.
4. Classify the post as nude or not.

3.2 Skin Detection Techniques

This involves developing an effective mathematical model to capture the distribution of skin colour.

Range-based

- Transform an input pixel into a proper color space
- Skin detection classifier to label the pixel whether it is a skin or non-skin pixel.

Histogram back-projection

- The histogram is a spectrum of intensity repartition.
- A list that contains the number of pixels for each possible value of the pixel.

3.3 Natural Language Processing

A user's social standing may be roughly estimated by analysing comments, the percentage of positive or negative responses, and sentiment analysis using various text mining modules. User messages or comments are processed into a tree structure before their words are examined in the tree structure to determine their emotion.

To increase classification accuracy, text analysis of the linguistic content of shared photos might be useful in addition to image analysis. The distinction between child pornographic and adult pornographic imagery, as well as between legal and criminal content, is another issue analysts must deal with. Accessing postings from a user's account is the system's primary viewpoint.

3.4 User Behavior Detection

It is utilised to study user behaviour for security considerations. When a significant shift in user behaviour is noticed, it initiates or executes an action. It keeps a record of the user's typical performance in a journal. When a user deviates from their typical behaviour or patterns, the system in turn recognises any aberrant behaviour for that user.

For instance, if a person hasn't logged in for three months but then all of a sudden increases their social media activity, it is referred to as a pattern shift or behaviour change.

4. CONCLUSION

This method created a thorough product in this article and are aiming to put up a mechanism to safeguard the next generation against cyberbullying attacks. The majority of the features outlined in this article were able to be designed for our own social media platform, which we have already deployed. If guidelines are

broken, actions are also taken on social media. We made an effort to illustrate a real-world scenario for each feature described in this article.

Cybercrime offences are occurring at an alarming rate in the modern world. Making use of this in our work is crucial to the development of a model that can support analytics regarding the identification, discovery, and bracketing of the integrated cybercrime offences (struct attacks that take advantage of the security ways). This is because the use of the Internet is attracting more and more criminals. The intended outcome is that the constructed frame will offer the necessary broad knowledge of society and enable them to think about the geographical context of comparable crimes.

REFERENCES

[1]. Ghankutkar S, Sarkar N, Gajbhiye P, Yadav S, Kalbande D, Bakereywala N. 2019. Modelling machine learning for analysing crime news. In: 2019 International Conference on Advances in Computing, Communication and Control (ICAC3). 1–5.

[2]. Feng M, Zheng J, Han Y, Ren J, Liu Q. 2018. Big data analytics and mining for crime data analysis, visualization and prediction. In: International Conference on Brain Inspired Cognitive Systems. Cham:
Springer, 605–614

[3]. Kim S, Joshi P, Kalsi PS, Taheri P. 2018. Crime analysis through machine learning. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Piscataway: IEEE, 415–420.

[4] S. J. Stolfo, KDD Cup 1999 Data Set, University of California Irvine, KDD repository [Online].
Available: http://kdd.ics.uci.edu, accessed on Jun. 2014

[5] Afrah Almansoori, Mohammed Alshamsi, Sherief Abdallah, and Said A. Salloum, “Analysis of Cybercrime on Social Media Platforms and Its Challenges” under exclusive licence to Springer Nature Switzerland AG 2021.

[6] Kazi Saeed Alam, Shovan Bhowmik, Priyo Ranjan Kundu Prosun- “Cyberbullying Detection: An Ensemble Based Machine Learning Approach," Published: July 2021

[7] John Hani, Mohamed Nashaat, Mostafa Ahmed, Zeyad Emad, and Eslam Amer. “Social Media Cyberbullying Detection using Machine Learning International Journal of Advanced Computer Science and Applications, (IJACSA) Vol. 10, No. 5, 2019

[8] Nureni Ayofe Azeez, Sunday O. Idiakose, Chinazo Juliet Onyema and Charles Van Der Vyver, “Cyberbullying Detection in Social Networks: Artificial Intelligence Approach” Publication 18 June 2021.

[9] Department of Translation, Interpreting, and Communication - Faculty of Arts and Philosophy, Ghent University, Ghent, Belgium, “Automatic detection of cyberbullying in a social media text.” Published online 2018 Oct 8.

[10]. J. Agarwal, R. Nagpal, and R. Sehgal, “Crime analysis using k-means clustering”, International Journal of Computer Applications, Vol. 83 – No4, December 2013.