European Journal of Molecular & Clinical Medicine
ISSN: 2515-8260, Volume 10, Issue 02, 2023

CYBER CRIME DETECTION USING MACHINE LEARNING APPROACHES

Dr.M.Rajaiah[1], Dean Academics & HOD, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr D. SUREDNRA[2], Assistant Professor ,Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr.K. LOKESH[3], UG Scholar, Dept of CSE, Audisankara College ofEngineering and Technology, Gudur.

Ms.A. DIVANYA[4], UG Scholar, Dept of CSE, Audisankara College ofEngineering and Technology, Gudur

Ms.K. JANSI[5], UG Scholar , Dept of CSE, Audisankara College ofEngineering and Technology, Gudur

Mr.A. HEMANTH[6], UG Scholar, Dept of CSE, Audisankara College ofEngineering and Technology, Gudur.

ABSTRACT

Now a days the use of social media has grown exponentially over time with the growth of the Internet and has become the most powerful networking platform in the 21st century. However, theimporvement of social connectivity often creates negative impacts on society that contribute to a couple of bad phenomena such as online abuse, harassment, cybercrime and online trolling. Cyber crime leads to serious mental and physical distress, particularly for women and children, and even sometimes force them to attempt suicide. Some kind of fake message can impact women to consider as suicide. Online harassment attracts attention due to its strong negative social impact. Many incidents have recently occurred worldwide due to online harassment, such as sharing private chats, rumours, and sexual remarks. Therefore, the identification of bullying text or message on social media has gained a growing amount of attention among researchers. The purpose of this research is to design and develop an effective technique to detect online abusive and bullying messages.

Two distinct freatures, namely Bag-of Words (BoW) and term frequency-inverse text frequency (TFIDF), are used to analyse the accuracy level of four distinct machine learning algorithms

1.INTRODUCTION

With the huge uasge of the social apps like Twitter, Facebook,instgarm, whatsappcybercrimehas become normal in the life, especially in the life of students. Most of the youngsters in America are effected by the cybercrime. This tormenting intellectually affects the casualty. The casualties pick reckless behaves like self-destruction in light of the fact that the injury of cybercrimewhich is difficult to be suffered. Subsequently, the identifying and avoidance of cybercrimeis essential to secure youngsters.According to situation, we recommend a cybercrimerecognition system in view of AI to recognize whether or not a text connects with cyberbullying. We have explored a few AI algorithms in our research to find out the best one among them which can be used to detect cybercrime. We direct examinations with datasets from twitter comments and remarks. In execution investigation, we utilize two distinctive component vectors BOW and TF-IDF. The outcomes show that TF-IDF highlight gives preferable exactness over BOW where SVM gives preferred execution over some other AI calculations used for our research. Rest of the research is coordinated in the following pattern. Section 2 outlines the connected works. Section 3 presents the subtleties of the given AI comparison.

2.CONNECTED WORKS: -

There are a few deals with AI based digital tormenting identification. A regulated AI calculation was proposed utilizing a sack of words way to deal with identifying the context and intention of the writerof the text . This calculation shows scarcely 67.9% of exactness. SVM to detect cybercrimeof Twitter remarks. The scientist joined location with rational thinking by adding social parameters. The after effect of this undertaking was improved to 69.9% precision for applying probabilistic displaying. Reynolds et al. discover an even more effective cyber bullying technique with an increased accuracyof 78.5%. The decision tree and occasion-based mentor is utilized by creator to accomplish this accuracy. To improve online harassment recognition, the creator of research has utilized characters, feeling and opinion of element.

A few profound learning-based models were additionally acquainted with identify the

cyberbullying. Profound Neural Networkbased model is used for detecting online bullying by utilizing genuine information. The creators first investigate cybercrimemethodically then used that data to learn the AI about automatic detection of bullying. Badjatiyaet al. has introduced a technique involving profound Neural organization models for identifying disdain discourse. A convolutional neural organization- based model is used to identify online bullying. The creators utilized word inserting where comparative words have comparative installing. In a multi-modular setting. paper the original study of online bullying identification by cooperatively taking advantage of web-based media information. This test, nonetheless, is difficult because of the intricate blend of both cross-modular relationship among numerous strategies and underlying connections between different web-based interactive conversations, arrangement of various complex models and modes of conversations. They propose Bully, online harassment detection framework to come out of the difficulties, which first change multi- modes of social apps information as a diverse organization and afterward attempts to do hub implanting portrayals onto that information. Numerous writings about online harassment focused on examination of what is written throughout recent many years. But Cyber crime, be that as it may, is now changing now it not only present in the form of text only.

The assortment of tormenting information of friendly stages can't be achieved only by text detecting algorithms only. Wang et al. recommended a multi-modes detection framework that coordinates multiple types of data, for example, gif, images, vulgar comments, time via online media to adapt to the most recent kind of harassment. Specifically, they remove printed attributes, yet additionally apply progressive consideration organizations to catch the informal organization meeting capacity and encode various types of data including gifs, pictures. The creators model the multi-modes harassment discovery structure to for addressing these new kind of online bullying ways other than text.

Utilizing Neural Networks to work with the identification of web-based harassing become a common norm today. These Neural Networks originally founded exclusive for or related to other types of Layers by use of Long-Short-Term-Memory layers. presented another model for the Neural Network that can be used in words-based media to identify whether there is online bullying or not. The idea is based upon current models that combine the strength of Long-Short-Term-Memory layers with Coevolutionary layers. Along with this, the design includes the use of stacked center layers, which shows that their review improves the Neural Network's performance. A different type of enactment strategy is also remembered for our

plan, that is classified" SVM like initiation" By involving the weight L2 regularization of a straight actuation work in the actuation layer along with utilizing a misfortune work, the" SVM like accuracy" is achieved.

Making an AI framework with three unmistakable highlights, by Raisi et al. solves the issue of computation connected with badgering identification in interpersonal organizations. (1)In this type the key expressions which is given by expert which distinguish bullying from non-bullying, with minimal supervision required. (2) A total no. of two students who co-train each other, in which one student study the content of the language of text and the second student looks at social construction aspect. (3) On preparing nonlinear profound models, this coordinate decentralized word and chart hub portrayals. Upgrading a genuine capacity that consolidates co-preparing along with weak supervision, and the model is trained.

3.METHODOLOGY: -

We will develop this project with the help of python and web technology. Using html and CSS, we will design and develop the web interfaces for the project. Then after preparing the web interfaces, we will search and download the dataset that we need to classify. After downloading the dataset, we will pre- process the data and then transfer to Tf-Idf. Then we will generate codes for the machine learning algorithms (Naive Bayes, Decision Tree, Random Forest, SVM, DNN Model) using python. So here, we are using python as backend and for frontend html, CSS etc. The real-world posts or text contain number of unnecessary symbols or texts. For instance, emojis and symbols are not needed to detect cyber bullying. Hence, first they are removed and then machine learning algorithms are applied for the identification of bullying text. In this phase, the task is to remove unnecessary characters like symbols, emojis, numbers, links etc. And after those two important features of the text is prepared:

• **Bag-of-Word:** The machine learning algorithms are not going to work directly with texts. So, we have to convert them into some other form like numbers or vectors before applying machine learning algorithm to them. In this way the data is converted by Bag-of-Words (BOW) so that it can be ready to use in next round.

• **TF-IDF:** One of the important features to be considered is this. TF-IDF (Term Frequency-InverseDocument Frequency) is a statistical measure to know the importance that a word carries in a document. **Machine Learning:**

In this model we will apply five efficient algorithms used in machine learning namely- Random Forest, Decision tree, Naive Bayes, SVM and Deep Neural Networks Model (DNN) to compare them and find the most accurate algorithm among them. The algorithm having highest accuracy is discovered among the five algorithms using public datasets.

Decision Tree:

This tree classifier can be utilized in both arrangement and relapse. It can assist with addressing the choice and choose both. Decision tree has a design which resembles a tree like structure in which the parent/root hub is a condition, and descending parent hub is leaf/branch hub which is a choice of the condition. For ex. If the root hub is the coin than its branch hub will be the outcome of the coin i.e., head and tail. A relapse tree yields the anticipated incentive for a tended to enter.

Bayes Naive:

This is a productive AI calculation in view of Bayes hypothesis. It predicts about the probability of occurring of an event based upon the event which already occurred previously. And when we add naïve assumption into it became the Naïve Bayes classifier. In naïve bayes assumption we consider that each event is independent of each other and is going to make an equal contribution to final result. The best useof it is the classification of text which required a high dimensional training dataset. As stated earlier it consider that each event is independent so it cannot be used for events having relationship between them.

Random Forest:

It is a classifier which comprises of different choice tree classifiers. It is created by using subset of data

and the final output of that data is based on majority ranking means the higher votes. It is slower than thedecision tree which we have discussed earlier as it contains not only one but a large number of decision tree which comes together to form a forest and hence the name random forest. The greater number of decision tree are going to be present in random forest the more precise the output is going to be. Unlike decision tree it doesn't use any set of rules or formulas to show the output.

Support Vector Machine:

Support Vector Machine (SVM) is a regulated AI calculation which can be applied in both order and relapse the same a choice tree. It can recognize the classes extraordinarily in n-layered space. Along these lines, SVM produces a more precise outcome than different calculations significantly quicker. By

and by, SVM develops set an of hyper planes in a limitless layered space and SVM is executed with part which changes an information space into the necessary structure. For instance, Linear Kernel involves the ordinary spot result of any two examples as follows:

K (y, yi) = aggregate (y ∗yi)

4.EXPERIMENT AND RESULT: -

The dataset used for this study is downloaded from website called kaggle.com [27]. The dataset contains two types of set which are bullying text and non-bullying text. The goal is to identify all the bullying text.

- **Non-bullying Text**: The text which is not demeaning or hurtful but is a legit compliment or respectful criticism of the work of an individual. For example, comments such as “This girl is cute” are somewhat humane and demeaning.
- **Bullying text:** The comments which is hurtful and abusive in nature or are promoting racism, body shaming, casteism, slut shaming etc. comes in the category of bullying text. For example, "This bitch isugly", “you should die” are the text which is straight up bullying someone which can affect their mental health severely. So, with the use of python machine learning packages algorithms known as troubleshooting algorithm is implemented.

Accuracy of different algorithms :

In the given graph shown. We are comparing all the five algorithms with each other to find out which algorithm is best among all five. This graph has been plotted with the help of Mat plot library. We observed that among the five machine learning algorithms, DNN Model outperforms the others while Random Forest comes second, Decision Tree- third, Naïve Bayes comes second last and SVM is the least accurate. So according to this result we can safely say that it is better to use DNN Model for detecting the cyber crimethan any other algorithm.

5.RESULT ANALYSIS: -

the input processing and prediction result that we performed during our testing. We used a tweet from Twitter with the trace of bullying and applied it to our model. The classification report based on our testing data. Here labels 0 and 1 represent Bullying and Non-Bullying respectively. the confusion matrix based on the result of our testing data. the accuracy of the SVM and Naive Bayes that is 71.25% and 52.70% respectively, when applied on the same dataset from. The result shows better accuracy when using the BERT model for sentiment analysis on the Twitter dataset. Our proposed model gave a better accuracy of 91.90% when

applied to the Twitter dataset for the sentimental analysis which can be considered as a greater result when compared to the traditional machine learning models used on similar datasets.

6.CONCLUSION: -

As the users of social media is increasing day by day along with-it cyber bullying related cases is also increasing on social media with its growing popularity and the increasing usage of social media by young people. It is necessary to devise an automated method of detecting cyber crimein order to avoid the harmful effects of cyber crimebefore it's too late. As sometimes the consequences of cyber crimecan be as bad as the suicide by the person that is bullied. So, keeping in mind the importance of a system which can detect the cyber crimeand online harassment, we are going to study different ML algorithms and their effectiveness in comparison with each other to predict their accuracy on a given data set to find out the best among them. After studying all the five algorithms and their results we come to a conclusionthat DNN model perform best in detecting cyber crimewith an accuracy of 0.990145 and along with the second-best performing algorithm comes out to be random forest algorithm with an accuracy of 0.986897. So, we can use any of these two algorithms to detect the cyber crimeand online harassment to get the highest accuracy while SVM is the least accurate among all of them.

ACKNOWLEDGEMENT: -

All the work and research done in this project is supported by M.I.E.T(Meerut Institute of Engineering and Technology), Meerut.

REFERENCES: -

[1] C. Fuchs, social media: A critical introduction. Sage, 2017.

[2] N. Selwyn, "Social media in higher education," The Europa world of learning,

[3] W. Akram and R. Kumar, "A study on positive and negative effects of social media on society," International Journal of Computer Sciences and Engineering,

[4] S. Bastiaensens, H. Vandebosch, K. Poels, K. Van Cleemput, A. Desmet, and I. De Bourdeaudhuij, "Cybercrimeon social network sites. an experimental study into bystanders' behavioral intentions to help the victim or reinforce the bully," Computers in Human Behavior,

[5] D. L. Hoff and S. N. Mitchell, "Cyberbullying: Causes, effects, and remedies," Journal of Educational Administration, 2009.

[6] S. Hinduja and J. W. Patchin, "Bullying, cyberbullying, and suicide," Archives of suicide research.

[7] D. Yin, Z. Xue, L. Hong, B. D. Davison, A. Kontostathis, and L. Edwards, "Detection of harassment on web 2.0," Proceedings of the Content Analysis in the WEB.

[8] K. Reynolds, A. Kontostathis, and L. Edwards, "Using machine learning to detect cyberbullying," in 2011 10th International Conference on Machine learning and applications and workshops,

[9] V. Balakrishnan, S. Khan, and H. R. Arabnia, "Improving cyber crimedetection using twitter users' psychological features and machine learning," Computers & Security,

[10] S. Agrawal and A. Awekar, "Deep learning for detecting cyber crimeacross multiple social media platforms," in European Conference on Information Retrieval. Springer,

[11] M. A. Al-Ajlan and M. Ykhlef, "Deep learning algorithm for cyber crimedetection," International Journal of Advanced Computer Science and Applications,

[12] K. Wang, Q. Xiong, C. Wu, M. Gao, and Y. Yu, "Multi-modal cyber crimedetection on social networks," in 2020 International Joint Conference on Neural Networks.

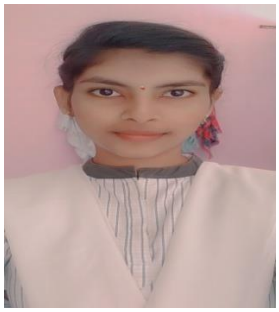
AUTHOR PROFILES

Dr.M.Rajaiah , Currently working as an Dean Academics & HOD in the department of CSE at ASCET (Autonomous), Gudur, Tirupathi(DT).He has published more than 35 papers in, Web of Science, Scopus Indexing, UGC Journals.

D.SURDNRA completed his Bachelor of Technology in Computer Science and Engineering.He completed his Masters of Technology in Computer Science and Engineering. He has published more than 6 papers in indexing Journals.Currently working as an Assistant Professor in the department of CSE at ASCET (Autonomous), Gudur, Tirupathi(DT). His areas of interest include, Data Mining, Cloud Computing and MachineLearning.

Mr.K. LOKESH as B.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. He is pursing Computer Science and Engineering from JNTUA. His areas of interests. Cyber crime detection using machine learning approches

Ms.A. DIVANYA, as B.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. She is pursing Computer Science and Engineering from JNTUA. His areas of interests. Cyber crime detection using machine learning approaches



Ms.K. JANSI, as B.Tech student in the department of CSE at Audisankara College of

Engineering and Technology, Gudur. She is pursing Computer Science and Engineering from JNTUA. His areas of interests. Cyber crime detection using machine learning approaches

Ms.A. HEMANTH, as B.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. He is pursing Computer Science and Engineering from JNTUA. His areas of interests. Cyber crime detection using machine learning approches