Cyberbullying and Fake Account Detection in Social Media

Richard Joseph
Asst. Professor, Department of Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, Maharashtra, India
richard.joseph@ves.ac.in

Jayesh Samtani
Student, Department of Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, Maharashtra, India
2017.jayesh.samtani@ves.ac.in

Sagar Sidhwa
Student, Department of Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, Maharashtra, India
2017.sagar.sidhwa@ves.ac.in

Somesh Tiwari
Student, Department of Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, Maharashtra, India
2017.somesh.tiwari@ves.ac.in

Riya Wadhwani
Student, Department of Computer Engineering
Vivekanand Education Society's Institute of Technology
Mumbai, Maharashtra, India
2017.riya.wadhwani@ves.ac.in

***Abstract*—Enhancement in the technology trend of using social networking is increasing day by day as of now there are more than 50 crores active users are using different social media platforms for the interaction which had affected their life so just like a coin has two face in a similar way misuse of these platforms is going which cause the the rapid rise of cybercrime and exploitation eg harassing someone by sending malicious messages, spreading abusive messages through fake accounts on the social media etc.. In this new era insulting a person physically or emotionally is done by cyberbullying and by using fake accounts, so as a preventive measure to ensure the above things should not happen there is a need of detecting cyberbullying and the fake accounts. In our study to stop cyberbullying and fake accounts we'll use different Machine Learning algorithms for detecting the cybercrime and fake accounts so as to report these issues to the system immediately and to stop the crimes to increase in future and develop a secure online environment.**

***Keywords*—Automated, Time-Saving, Efficient, Fool-Proof, Cybercrime , Secure, Fake Accounts.**

I. Introduction

Social networking sites have connected us to different parts of the world however, people are finding illegal and unethical ways to use these communities. We see that people, especially teens and adults, are finding new ways to bully one another over the internet. About 25% of parents in a study conducted by Semantic reported that their child had been involved in a cyberbullying incident as shown in Fig 1.1. Other than cyberbullying, the spread of false information is increasing at an alarming rate. The number of users in social media is increasing exponentially. Instagram, Twitter has recently gained immense popularity among social media users. The major sources of fake news are fake accounts. Business organizations that invest a huge sum of money on social media influencers must know whether the following gained by that account is organic or not. Hence there is a huge need for the detection of these fake accounts which are increasing as shown in Fig 1.2.

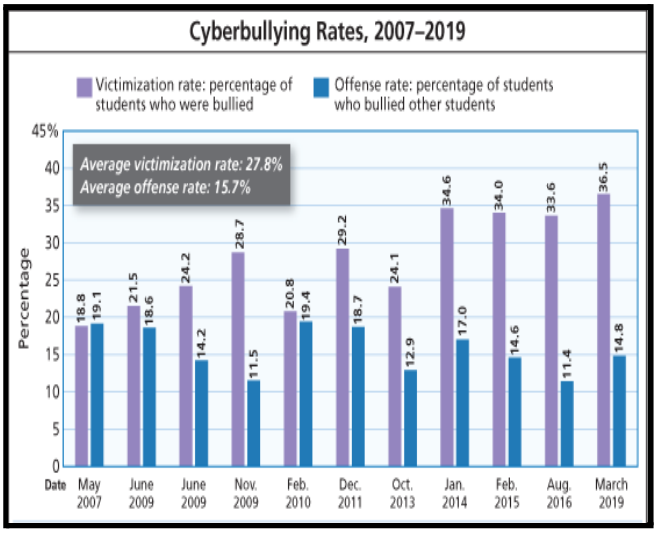

Fig 1.1-Graph showing the increase in the rate of CyberBullying in the recent years

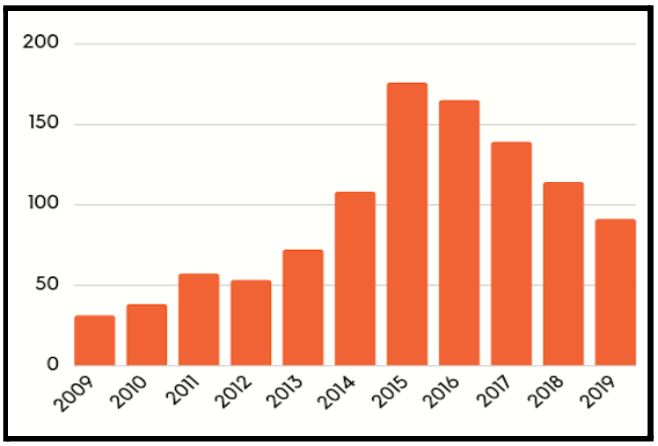

Fig 1.2-Graph showing the increase in the number of fake account

II. Proposed System

The applied technique consists of the following points namely re-processing, mining required parameters, and a separate phase is listed below.

1] The very first part is to convert the jumbled or the impure information into pure information and to convert the strings into small tokens this process is known as tokenization.

2] In this part, we will convert the pure information collected from the first part to the smaller format that means converting the capital letters to small letters.

3] This is a very crucial part of this technique where we remove certain special characters such as '\b' or '\n' since we need meaningful characters and such characters don't provide any meaningful content.

4] The next part is to convert this data into Machine learning format so as to give input to our Models.

5] The final part of this technique is to provide input data to our machine learning algorithm so as to classify the data as toxic, sever_toxic, identity_hate, threat, obscene, insult.

6] The accuracy of different algorithms will be Compared to get the best possible result. For fake profile detection, this paper proposes the detection process starts with the selection of the profile that needs to be tested.

7] After selection of the profile the suitable attributes ie., features are selected on which the classification algorithm is being implemented, the attributes extracted are passed to the trained classifier. Different Classifier algorithms such as Gradient Booster, random forest Decision trees, Support Vector Machine, and Neural Networks such as RNN and CNN can be used. The model generated by the learning algorithm should both fit the input data correctly and also correctly predict the class labels of the learning algorithm to build the model with good generality capability.

8] The complete dataset of the fake account is used for the training purpose this data after preprocessing is fed to the different machine learning algorithms and the accuracy is compared and according to the results the Random Forest has given us the best results and for the testing purpose, the live data is fetched from the Twitter.

III. Existing System

As Compared to the existing System there are many Lacunas -

1] Lack of Security -There is a lack of Security in the existing systems but our system will deal with the proper security provision to the users. [1]

2] No Transparency- As the existing system doesn't provide the proper transparency in their system as they are not able to deal with the Sharing of their reports to the Cybercrime Department.[3]

3] One Feature is Implemented - Other systems deal with only one part but our System will provide different features to give the best solution.[5]

4] Costly to Produce Reports - The other systems will cost a lot to generate the reports but the system that we will develop will generate results and reports for free.[2]

IV. Working Of System

In this project, we aim to detect cyberbullying and fake account detection for the marginal number of attributes the proposed methodology consists of different steps.

1] The first step is the preprocessing and finding the proper set of attributes from the datasets i.e Cyberbullying and the fake account so in this step, we will separate a number of the attributes that will be used to identify these bullying, contains abusive words, etc from the second dataset we will preprocess and extract the attributes like name, followers count, the following count, listed count, timezone, screen name, favorite to identify that whether the account is fake or not. The data for the fake account will be fetched via Twitter API as shown in Fig 4.1.

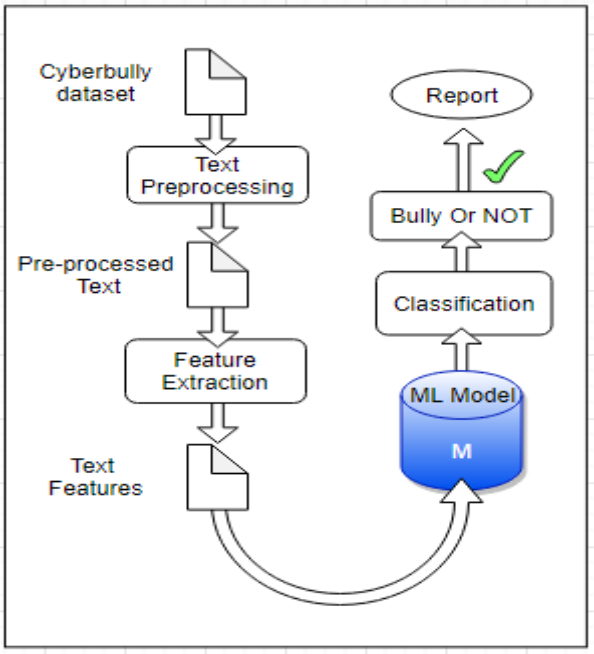

Fig 4.1 - Block diagram For Cyber Bullying

2] The second step is to create different Machine Learning Models like Support Vector Machine Classifier, Random Forest algorithm, Naïve Bayes, Logistic Regression, K-mean clustering, ADT and BFT tree and Neural Networks and NLP and applying the following algorithms on the datasets of cyberbullying and the fake account [4] by splitting the datasets into training and test approximately in the ratio of 75:25 or 80:20 to find the algorithm which best suits or fits for our system to achieve the highest accuracy.

3] The third step is to test the messages that are extracted from the chats or the blog which is posted on the blog by the user which causes bullying or use of abusive words to classify the post as toxic, severe toxic, obscene, threat, insult, identity hate and if found then the results will be saved in this step.

4] For Fake account Detection as shown in Fig 4.2 attributes fetched via Twitter API are given as input to the models and the model that will give us the best accuracy will be used that best fits our system and the results that we will get from the third step and the fourth step will be sent and a report will be generated which will help to identify whether the user has bullied anyone and this will help them to take any action on them.

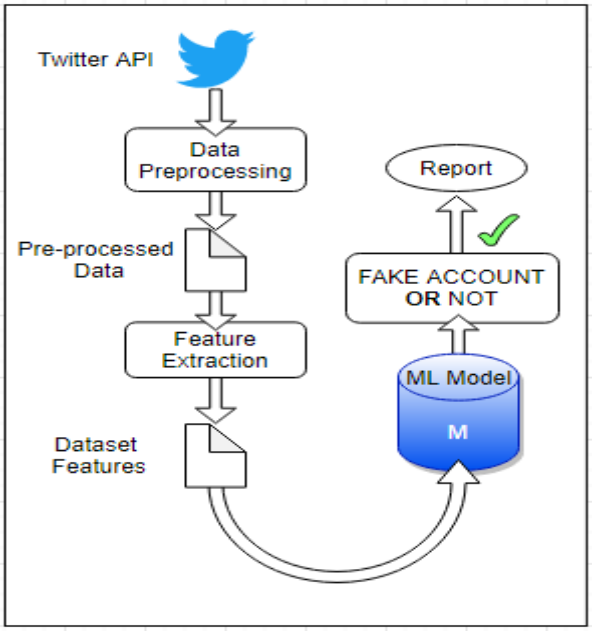

Fig 4.2 - Block diagram For Fake Account

V. Conclusion

In this paper, we have presented an idea to find cyberbullying using ML methods. We examined our model in the first cyberbully by comparing the authenticity of the different algorithms with which we can conclude that the SGD (Stochastic Gradient Descent) division gives us the best 92% accuracy and from the results of the model tested on the fake account we found that the most accurate algorithm is Decision Tree accuracy of ~ 98.5% by using fully automated learning algorithms, we have eliminated the need for personal accounting for a fake account, which requires a lot of resources and is a time-consuming process.

VI. Future Scope

1. Visual Cyberbullying is more harmful than the written ones thus we also plan to develop ML classifiers detecting cyberbullying from videos and images. This goal could be reached through the contribution of scholars from different fields, because of the technical (i.e., difficulty to create datasets containing this type of entries) and legal (i.e., privacy issues) issues raised by sharing multimedia content.

2. It is also necessary to understand which impact these detection systems could have on users' everyday life. Future works will be challenged to combine these technological systems with the implementation of psychosocial interventions.

3. We can Restrict the access of the fake account users to the authentication servers or the sites.

VII. References

[1] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, “SMOTE:synthetic minority over-sampling technique,” Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.

[2] I. Jolliffe, Principal Component Analysis, 2002.View at: MathSciNet.

[3] S. Sperandei, “Understanding logistic regression analysis,” Biochemia Medica, vol. 24, no. 1, pp. 12–18, 2014.

[4] R. Kohavi, “A study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection,” in Proceedings of the in 14th international joint conference on Artificial intelligence,pp. 20–25, 1995.

[5] N. E. Willard, “Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress”, Research Press, 2007.