International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 8, Issue 8, August 2019 **ISSN 2319 - 4847**

Prediction of Cyberbulling Using Random Forest Classifier

Lakhdeep Kaur[1] Dr. Sonia Vatta[2]

[1] M.tech CSE , Rayat Bahra University, Mohali India
[2] Head of Department (CSE), Rayat Bahra University, Mohali, India

Abstract

The people who already know each other through any source like from schools or colleges can bully each other which is the pervasive as well as constant. In this type of bully, the person who is bullying the person will follow every time through internet and creates problem to him. The bully person can be very intelligent, he knows all the schemes to create problem to victim and can easily hides his identity. There are enormous types of applications developed and still developing by which the data can be easily generated. It gives rise to a term known as Data Mining. It is the process by which useful information and patterns are extracted from the large amount of data beings stored in the databases. Data Mining is also known as knowledge discovery process as knowledge is being extracted or patterns are analyzed which is very useful to collect data. Many classifiers are being used in the prediction of cyberbulling such as Naïve Bayes, SVM, KNN etc. In this work, Random Forest Classifier is implemented and results are analyzed in terms of accuracy, precision, f-measure and recall.

Keywords*:* Cyberbulling, Data Mining, Naïve Bayes, Random Forest

1.INTRODUCTION

The expansion of technology has generated the requirement of increasing the dimension of databases or folders for the storage of enormous information being produced on every day. This information is generated with the help of huge quantity of applications. The proper storage and manipulation of produced information is extremely significant according to the necessity. Up to now, large number of databases has been developed [1]. Numerous investigations have been performed for ensuring the appropriate management of these databases. The procedure used for the extraction of valuable information and prototypes from enormous folders is identified as data mining. This approach is also recognized as Knowledge discovery procedure as the information retrieval or prototype scrutiny is utilized for the collection of valuable information.

A number of data mining mechanisms are implemented in this research works for proficient investigation. This tool is utilized in numerous fields like medical management, decision taking, client preservation, and manufacturing management and so on. Predictive Analysis is an area of observation used for the management of extracted information [2]. Predictive analysis approach uses this information for the prediction of prototypes and designs. Commonly the ambiguous instance of deception occurs afterward, but prophetic assessment can be linked to a vague and it can be past, present or future. For example, recognition of suspect after the submission of a bad behavior and accuse card falsification. The midpoint of analytical analysis relies on catching links amid rational parameters and the predictable parameters from precedent proceedings, and mistreating them to predict the ambiguous outcome. It is essential to identify that in any situation, the precision and accessibility of outcome will rely on the particular data study level and the character of uncertainties [3]. Prediction analytics is commonly distinguished as prediction at an additional fundamental level of granularity, i.e., generating prophetic scores (probabilities) for every single hierarchical constituent. This distinguishes it from prediction. For example, "Prediction analytics technique that grow for a fact (information) to predict the future behavior of people by keeping in mind the target to make improved decisions." In prospect automatic structures, the assessment of prophetic inspection will be done to predict and shun possible concerns for achieving approximately zero separate and further included into authoritarian test for preference optimization. Also, the transformed data can be used for close circle item life cycle development which is the visualization of Industrial

Internet Consortium. Maltreatment actions towards others by means of digital devices like smart phones, internet or emails are known as cyber bullying [7]. The individuals who know each other

through school or good friends of sometime can intimidate each other which are enveloping and stable. In cyber bullying, intimidate can follow the prey all the time using internet and causes issues for him. The other benefit to cyber bullies is insight of vagueness. Though, in most of the cases, the individual who is bullying mainly identifies the prey. Cyber bullying is mostly a civic form of disgrace. Cyber bullying is damaging. The other clients can see what is being placed in micro blogging sites. The elimination of already posted trace is extremely difficult. Bullying is a societal problem being experienced from various years on a huge level. Because of bullying, the problems raise either in straight or roundabout way. The complete elimination of this problem has become extremely complex in the present scenario. These days, in the technical period, youth remains busy in social media sites and does not take part in outside physical activities [5]. The youngsters utilize online services to hook up with old friends. They also make new friends by exchanging their private information with them. However most of the micro blogging sites have made some guiding principles for the protection of personal data. But youngsters are not aware about the privacy rules. By using privacy guidelines, the atmosphere of online surfing can be protected through the enhancement of client communication. In the present scenario, the effects of bullying can be observed in genuine world structure. This has turn out to be a challenging situation for online surfing [9]. A number of investigations have been carried out in accordance with the content mining prototype for analyzing different issues related to the discovery of cyber bullying. But, only few researches have been presented in the significance of technological elucidations because of which appropriate preparation data suites are not accessible. Additionally, cyber bullying can be explained in the form of some causes like seclusion problems and indistinctness. Thus the designing of an effectual system is required for the inclusion of word-level traits and client based traits to detect and prevent the unpleasant text. The evaluation of client's unpleasantness level is imperative as well beside the discovery of rudeness statement intensity inside a memo [11]. The exploitation of this kind of method in concurrent relevance should be checked properly for implementing a real time application.

2.LITERATURE REVIEW

One of the research is done by the noviantho et.al (2017). The author presented the misuse of the technology, in order to bully and torture a person called as the Cyberbully. There is increase in the number of cases worldwide and its impact on others is negative as it bullies a user for doing wrong favors. Therefore, it is very essential to detect this major issue as the present online information is large in size due to which it is not possible to track the each and every human [14]. The construction of a classification model is the main objective of this paper with optimal accuracy using which cyberbully conversation can be identifies easily. For this purpose, they utilized the Naive Bayes method and Support Vector Machine (SVM) in which they implemented the n-gram 1 to 5 for the number of class 2, 4, and 11 for each method. The average accuracy of 92.81% is provided by the Naive Bayes while the average accuracy of 93% is given by the SVM with a poly kernel. On the basis of performed experiments, it is concluded that high accuracy is provided by the proposed SVM with poly kernel method as compared to other kernels, Naive Bayes, and Kelly Reynolds research method of decision tree (J48) and k-NNc.

In 2015, Cynthia Van Hee, et.al presented the production and explanation of a corpus of Dutch social media posts annotated with fine-grained cyberbullying-related text categories, such as insults and threats. The authors presented with the advent in the technology, there is development in the social media due to which major challenges has been faced. In order to analyze the online interactions between the people there is various researchers have been done by the researchers so far. For establishing the connection with others, the great opportunities have been provided by the social networking sites but due to this young people are more vulnerable to attacks such as cyber victimization. As per the recent reports the average, 20% to 40% of all teenagers have been victimized online [16]. They focused on the cyberbullying in this paper for the cyber victimization. The detection of the potentially harmful messages is the successful prevention. It is required to have an intelligent system to identify potential risks automatically due to the presence of large amount of information on the web. In order to enhance the analysis of human interactions involving cyberbullying, they identified the specific participants that are involved in the cyberbullying conversation. They presented proof-of-concept experiments in this paper for the identification of cyberbullying events and the categories the fine-grained cyberbullying.

Another research is done by the Nektaria Potha, et.al (2014). The researchers elaborated with the advent in the technologies, there is increase in the use of internet, cell phones and Personal Digital Assistants that result in the major issue of Cyberbullying. Therefore, in the new era it is considered as the major challenge of bullying problem. It is hard to trace the Online bullying due to its anonymous nature that damaged and upsetting the youth. They proposed a

method in this paper that utilized the dataset of real world conversations in which question is manually put by each predator in terms of sternness

using a numeric label. The representation of Singular Value Decomposition was used for the formulation of the predator's questions are, they show this issue as a sequential data modelling approach. Therefore, studying the accuracy of predicting the level of cyberbullying attack using classification methods is the main objective of this paper. In order to examine the potential patterns between the linguistic styles of each predator this approach has been utilized. They developed the whole question set model it as a signal instead of considering a fixed window of a cyber-predator's questions within a dialogue as done in the previously mentioned methods. This approach magnitude depends on the degree of bullying content [18]. The neural network has been utilized to parse each signal in which feature weighting and dimensionality reduction techniques are used. This network forecasts the level of insult within a question given a window between two and three previous questions. They made an interesting discovery using the time series modeling experiments. They implemented the SVD on the time series data and examined the second dimensions. They observed from the obtained results implemented approach is very similar to the plot of the class attribute. They implemented a Dynamic Time Warping algorithm and concluded that there is existence of the above mentioned signals. It is provided an immediate indicator for the severity of cyberbullying within a given dialogue.

Qianjia Huang, et.al (2014) presented the negative impact left on the victim by this major issue of cyberbullying which is increasing day by day among adolescents due to the wider use of internet. The main focused of the experts in social science is on the following attributes such as personality, social relationships and psychological factors including the both the bully and victim in order to understand the fundamental of cyber bullying [19]. There is development of automated methods by the computer science researchers that helps in identifying the cyber bullying messages for which all the bullying-related keywords in cyber conversations are identified. However, the textual features based methods having the limited accuracy. They investigated the proposed work in this paper and also analyzed the social network features weather they are improving the accuracy of cyber bullying detection. There is significant improvement in the detection of cyber bullying after analyzing the social network structure between users and deriving features such as number of friends, network embeddedness, and relationship centrality. The integration of the textual features with social network features leads to increase in all these issues.

3. ISSUES OF EARLIER RESEARCH WORK

Many classifiers are being used to predict the cyberbullying such as Naïve bayes, SVM, KNN and so on. The SVM classifier takes long training time on large data set. In the case of cyberbulling, large data set is required [13]. Furthermore, SVM suffers from the overfitting problem in the case of cyberbullying. In KNN algorithm, Distance-based learning is not very clear because it doesn't know what type of training data or distance it should use and which type of attribute is best for the excellent results [9]. It has been found that in related work that while using Naïve Bayes Classifier. The Naïve Bayes classifier is based on the probability and assumptions. Assumptions are not correct in every time. So, the percentage of accuracy and precision-recall were affected from this classifier. The probability works on possibilities which sometimes vary from original results. It doesn't classify the whole problem as it is. Moreover, manual classification is best for classification. But the manual classification is time consuming and not accurate [21][6].

4. SOLUTION

To tackle the previous problems, The Random Forest Classifier is used in the current work. The Random Forest Classifier gives the best results to analyze the complex and large data. It also maintains the accuracy even when a large proportion of data are missing words [23]. Random Forest creates multiple decision trees and combines them together to get a more accurate and stable prediction. To perform the prediction using the trained random forest algorithm, it need to pass the test features through the rules of each randomly created trees. For large data sets the major memory requirement is the storage of the data itself, and three integer arrays with the same dimensions as the data. If proximities are calculated, storage requirements increase as the number of cases times the number of trees. It doesn't over-fitting [24].

5. OBJECTIVES

To apply Random forest classifier to classify the text data i.e. offensive and non-offensive.
To compare performance parameters of Random Forest and Naïve Bayes on the basis of accuracy, precision, f-measure and recall.

6.RESEARCH METHODOLOGY

The projected method is relied on the clascification of the key information into offensive or non-offensive case. For the classification of offensive or non-offensive cases following phases are utilized:

In first step, data sets are prepared.

In the second step, information suites are grouped into two classes of sets in form of offensive and non-offensive messages. The contents of information suites are recognized, on the basis of Naïve Bayes classification model which carry out categorization on university information. Naïve Bayes classifier supposes the existence of a specific characteristic in a class not related to other traits.

In third step, information suites are classified with the help of classification method named as Random forest classifier. This approach is utilized for categorization, deterioration and other tasks that function by developing a mass of decision trees during preparation time and outputting the class that is the form of the classes or mean prophecy of the single trees. A non-parametric supervised learning technique identified as Decision Tree is presented for performing the categorization and regression of obtained information. The major aim of this study is to forecast the level of the destined variable. For predicting its value, this scheme utilizes information characteristics from which the uncomplicated decision regulations are gathered. In this study, the decision tree supports in providing the erudite capability which supplementary offers the estimation of distinct-valued destined purposes. The illustrations are classified by categorizing it from the root to any leaf nodule. Every node represents an analysis of a few qualities inside a tree. Every branch downward from the exacting nodule is connected to any of the values that may be probable in connection to the exacting quality. The classification of the occurrence starts in the staring of the root node of the tree. Every node stipulates a quality which is to be experienced in this study. Additionally, the tree branch connected to the value of characteristic is experienced further on and this process continues in the similar way. This technique plays an significant role inside the data mining approach as it supports to predict the value for any destined variable with regard to some of the key variables granted for it. Every key variable is connected to the interior node existing inside the tree. Any quantity of probable values for that key variable is identified as its kids who are symbolized by boundaries.

In the last step, the outcomes of Naïve Bayes classification model and random forest are compared by means of Accuracy, Precision, Recall and F-measure.

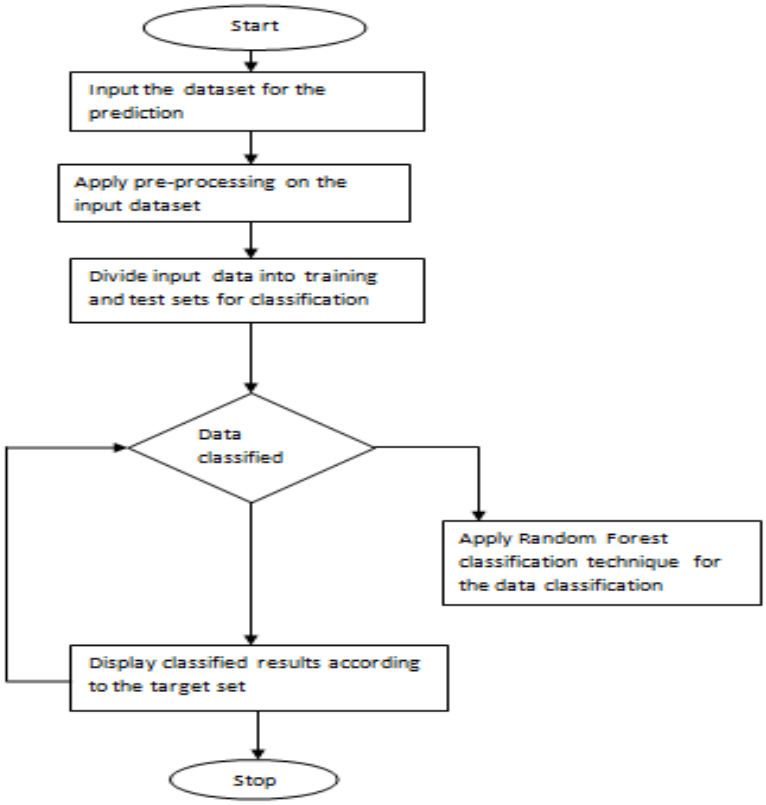


Figure 1: Flowchart

7. TOOLS AND TECHNIQUES

Python

Python is one of most flexible languages and can be used for various purposes. Python's straightforward, simple to learn language structure underscores decipherability and along these lines lessens the cost of program support [4]. Its abnormal state worked in information structures, joined with dynamic composing and dynamic authoritative, make it extremely appealing for Rapid Application Development, and also for use as a scripting or paste dialect to associate existing parts together. Python is used for web development, data analyisis, artificial intelligence, and scientific computing. It has different code libraries and different syntax. It contains special libraries for machine learning namely scipy and numpy which great for linear algebra and getting to know kernel methods of machine learning. It consists lot of code libraries for ease of use [10].

Anaconda Platform

Anaconda is a free and open-source distribution of the Python and R programming languages for scientific computing (data science, machine learning applications, large-scale data processing, predictive analytics, etc.), that aims to simplify package management and deployment [17]. Anaconda is a great option for installing python, specially for data science. Anaconda makes it easy to install python on to a windows system and if you work on different platforms it gives consistency as well. For me, it's definitely the best way of using python [10].

8. EXPERIMENTAL RESULTS

The results of Naïve Bayes and Random Forest Classifier are compared on the basis of accuracy, precision, recall and f-measure.

Accuracy Analysis

It defined as a freedom from error (correctness), or closeness to truth or fact. Accuracy depends on the how the data is collected and is usually judge by comparing several measurements from the same or different sources [15].

Table 1: Accuracy Analysis

Parameters	Naïve Bayes	Random Forest
Accuracy (%)	92	97

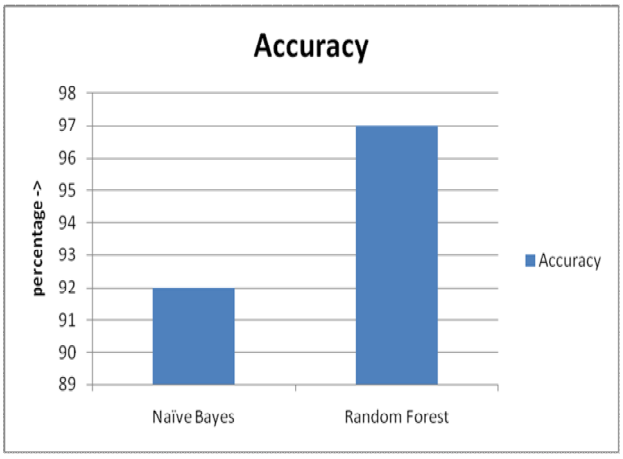


Fig.2 Accuracy Analysis

In the fig. 2, the accuracy of Naïve Bayes Classifier is 92% and Random Forest is 97%. The Random Forest Classifier performs well as compared to Naïve Bayes Classifier in terms of accuracy.

Precision Analysis

Precision defined as the percentage of your result which are relevant. Precision refers to the closeness of two or more measurements to each other [18].

Table 2: Precision Analysis

Parameters	Naïve Bayes	Random Forest
Precision (%)	86	87

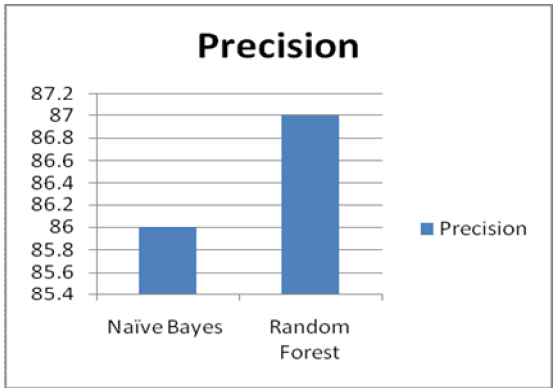


Fig. 3 Precision analysis

In the fig. 3, Random Forest Classifier gives 87% précised data and Naïve Bayes Classifier gives 86% précised data. The performance of Random Forest classifier is better than Naïve Bayes in the case of precision analysis.

Recall Analysis

Recall refers to the percentage of total relevant results correctly Identified. It is also known as sensitivity [20].

Parameters	Naïve Bayes	Random Forest
Recall (%)	84	93

Table 3: Recall Analysis

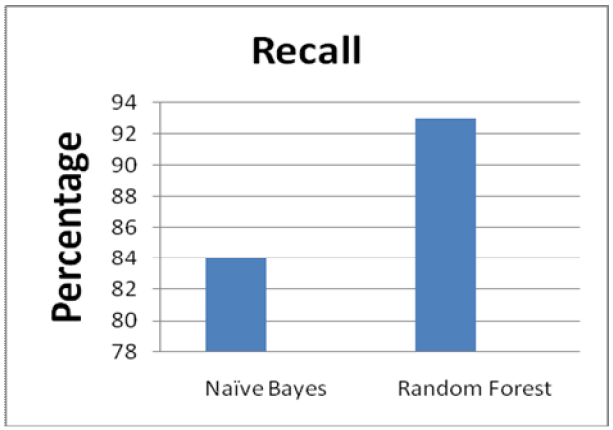


Fig. 4 Recall Analysis

In terms of recall analysis, the Random Forest Classifier shows 93% and Naïve Bayes Classifier shows 84%. The Random Forest Classifier works better than the Naïve Bayes Classifier in the terms of recall

F1-Measure Analysis

The **F score** is defined as the weighted harmonic mean of the test's precision and recall [22].

Table 4: F1-Measure Analysis

Parameters	Naïve Bayes	Random Forest
F1 measure (%)	86	89

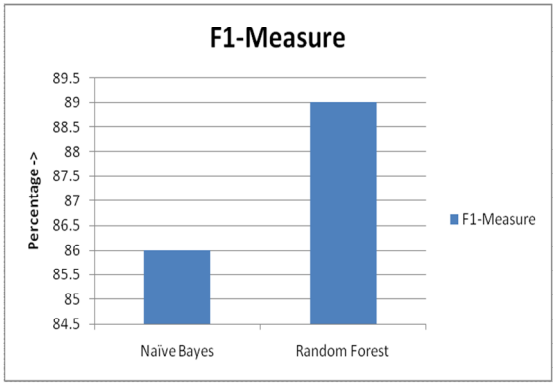


Fig 5. F1-Measure Analysis

In the F1-Measure, the Random Forest Classifier predicts 89% and the Naïve Bayes Classifier predicts 86% .
The performance of the Naïve Bayes and Random Forest algorithm is compared on the basis of accuracy, precision, recall and f-measure value is demonstrated by the fig 2, 3, 4 and 5. It is examined that Random Forest shows better performance than Naïve Bayes classifier by means of entire factors.

9. CONCLUSION

The data mining is a process used for the retrieval of captivating knowledge to study data. The data mining approach uses different data mining mechanisms to scrutinize different kinds of information. Several applications of data mining are decision creation, market basket observation, manufacturing control; client preservation, technical discoveries and learning systems. These applications are used to scrutinize the gathered data. Predictive Analysis is an area of observation used for the management of extracted information. Predictive analysis approach uses this information for the prediction of prototypes and designs. This investigative study is based on the forecasting of the cyber harassment cases. The method of Naïve Bayes and Random Forest is implemented for the classification of key information into offensive or non-offensive. The Random Forest classification model demonstrates better performance in comparison with Naïve Bayes on the basis of accuracy, precision, recall and f-measure.

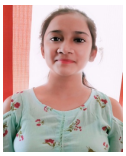
REFERENCES

[1] RasimAlguliyev, RamizAliguliyev, NijatIsazade, “A Sentence Selection Model and HLO Algorithm for Extractive Text Summarization”,2016, IEEE.
[2] NarendraAndhale, L.A. Bewoor, “An Overview of Text Summarization Techniques”,2016, IEEE.
[3] RupalBhargava ,Yashvardhan Sharma, “MSATS: Multilingual Sentiment Analysis via Text Summarization”, 2017, IEEE.
[4] What is python https://www.python.org/doc/essays/blurb/
[5] ArchanaN.Gulati, Dr.S.D.Sawarkar, “A novel technique for multi-document Hindi text summarization”,2017 International Conference on Nascent Technologies in the Engineering Field (ICNTE-2017).

[6] Naïve bayes classifier http://www.statsoft.com/textbook/naive-bayes-classifier

[7] Manisha Gupta, Dr.Naresh Kumar Garg, "Text Summarization of Hindi Documents using Rule Based Approach", 2016 International Conference on Micro-Electronics and Telecommunication Engineering.
[8] What is precision analysis https://en.wikipedia.org/wiki/Accuracy_and_precision
[9] Akshi Kumar, Aditi Sharma, Sidhant Sharma,ShashwatKashyap, "Performance Analysis of Keyword Extraction Algorithms Assessing Extractive Text Summarization", International Conference on Computer, Communication, and Electronics (Comptelix), 2017
[10] What is Anaconda https://www.anaconda.com/
[11] Tsaousis, I. "The relationship of self-esteem to bullying perpetration and peer victimization among schoolchildren and adolescents: A meta-analytic review". Aggress. Violent Behav. 2016, 31, 186–199
[12] Divyashree, Vinutha H, Deepashree N S, "International Journal of Innovative Research in Computer and Communication Engineering", Vol. 4, Issue 4, April 2016.
[13] SVM https://statinfer.com/204-6-8-svm-advantages-disadvantages-applications/
[14] Noviantho, Sani Muhamad Isa, Livia Ashianti, "Cyberbullying Classification using Text Mining", 2017 1st International Conference on Informatics and Computational Sciences (ICICoS)
[15] What is accuracy analysis https://ellistat.com/en/accuracy-analysis/
[16] Cynthia Van Hee∗ , Els Lefever∗ , Ben Verhoeven† , Julie Mennes∗ , Bart Desme, "Automatic Detection and Prevention of Cyberbullying", 2015.
[17] What is Anaconda(Python) https://en.wikipedia.org/wiki/Anaconda_(Python_distribution)
[18] Nektaria Potha, Manolis Maragoudakis, "Cyberbullying Detection using Time Series Modeling", 2014 IEEE International Conference on Data Mining Workshop
[19] Qianjia Huang, Vivek K. Singh, Pradeep K. Atrey, "Cyber Bullying Detection Using Social and Textual Analysis", IEEE, 2014
[20] What is recall analysis https://towardsdatascience.com/precision-vs-recall-386cf9f89488
[21] Kyriakos Charalampous, Constantina Demetriou, Loukia Tricha, Myria Ioannou, Stelios Georgiou, Militsa Nikiforou, Panayiotis Stavrinides, "The effect of parental style on bullying and cyber bullying behaviors and the mediating role of peer attachment relationships:A longitudinal study"
[22] What is F1-Measure https://en.wikipedia.org/wiki/F1_score
[23] Sebastian Raschka, Vahid Mirjalili, "Python Machine Learning: Machine Learning and Deep Learning with Python, scikit-learn, and TensorFlow"
[24] Gilles Louppe, "Understanding Random Forests: From Theory to Practice.

Author's Profile



Lakhdeep Kaur, Student of M.Tech (CSE), Rayat & Bahra University

Sonia Vatta, Head of Department (CSE), Rayat & Bahra University