

**VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF
TECHNOLOGY**

Department of Computer Engineering



Project Report on

**Cyberbully and Fake Account Detection in Social
Media**

In partial fulfillment of the Fourth Year, Bachelor of Engineering (B.E.) Degree in
Computer Engineering at the University of Mumbai Academic Year 2020-21

Submitted by

Jayesh Samtani (D17 - A , Roll no - 57)

Sagar Sidhwa (D17 - A , Roll no - 62)

Somesh Tiwari (D17 - A , Roll no - 71)

Riya Wadhwani (D17 - A , Roll no - 74)

Project Mentor

Mr. Richard Joseph

(2020-21)

**VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF
TECHNOLOGY**

Department of Computer Engineering



Certificate

This is to certify that ***Jayesh Samtani, Sagar Sidhwa, Somesh Tiwari, Riya Wadhwani*** of Fourth Year Computer Engineering studying under the University of Mumbai have satisfactorily completed the project on “***CYBERBULLY AND FAKE ACCOUNT DETECTION IN SOCIAL MEDIA***” as a part of their coursework of PROJECT-II for Semester-VIII under the guidance of their mentor ***Prof. Richard Joseph*** in the year 2020-21.

This project report entitled “***Cyberbully and Fake Account Detection in Social Media***” by ***Jayesh Samtani, Sagar Sidhwa, Somesh Tiwari, Riya Wadhwani*** is approved for the degree of ***Bachelor of Engineering (B.E.) Degree in Computer Engineering at the University of Mumbai.***

Programme Outcomes	Grade
PO1,PO2,PO3,PO4,PO5,PO6,PO7,PO8, PO9, PO10, PO11, PO12,PSO1, PSO2	

Date: 15 May 2021

Project Guide:

Project Report Approval For B. E (Computer Engineering)

This project report entitled “*Cyberbully and Fake Account Detection in Social Media*” by *Jayesh Samtani, Sagar Sidhwa, Somesh Tiwari, Riya Wadhwani* is approved for the degree of *Bachelor of Engineering (B.E.) Degree in Computer Engineering at the University of Mumbai.*

Internal Examiner

External Examiner

Head of the Department

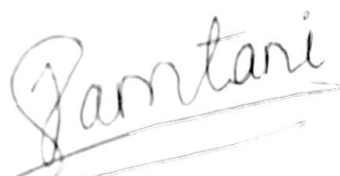
Principal

Date: 15 May 2021

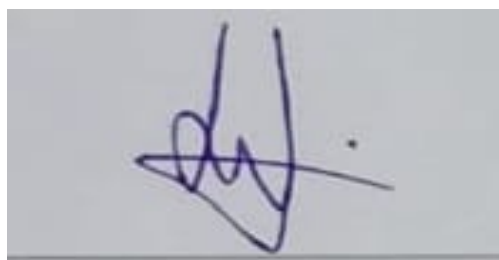
Place:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.



(Jayesh Samtani D17A-57)



(Sagar Sidhwa D17A-62)



(Somesh Tiwari D17A-71)



(Riya Wadhwani D17A-74)

Date: 15 May 2021

ACKNOWLEDGEMENT

We are thankful to our college Vivekanand Education Society's Institute of Technology for considering our project and extending help at all stages needed during our work of collecting information regarding the project.

It gives us immense pleasure to express our deep and sincere gratitude to Assistant Professor **Mrs. Priya R.L** (Project Guide) for her kind help and valuable advice during the development of project synopsis and for her guidance and suggestions.

We are deeply indebted to Head of the Computer Department **Dr.(Mrs.) Nupur Giri** and our Principal **Dr. (Mrs.) J.M. Nair** , for giving us this valuable opportunity to do this project.

We express our hearty thanks to them for their assistance without which it would have been difficult in finishing this project synopsis and project review successfully.

We convey our deep sense of gratitude to all teaching and non-teaching staff for their constant encouragement, support and selfless help throughout the project work. It is a great pleasure to acknowledge the help and suggestion, which we received from the Department of Computer Engineering.

We wish to express our profound thanks to all those who helped us in gathering information about the project. Our families too have provided moral support and encouragement several times.

Computer Engineering Department
COURSE OUTCOMES FOR B.E PROJECT

Learners will be to,

Course Outcome	Description of the Course Outcome
CO 1	Able to apply the relevant engineering concepts, knowledge and skills towards the project.
CO2	Able to identify, formulate and interpret the various relevant research papers and to determine the problem.
CO 3	Able to apply the engineering concepts towards designing solutions for the problem.
CO 4	Able to interpret the data and datasets to be utilized.
CO 5	Able to create, select and apply appropriate technologies, techniques, resources and tools for the project.
CO 6	Able to apply ethical, professional policies and principles towards societal, environmental, safety and cultural benefit.
CO 7	Able to function effectively as an individual, and as a member of a team, allocating roles with clear lines of responsibility and accountability.
CO 8	Able to write effective reports, design documents and make effective presentations.
CO 9	Able to apply engineering and management principles to the project as a team member.
CO 10	Able to apply the project domain knowledge to sharpen one's competency.
CO 11	Able to develop professional, presentational, balanced and structured approach towards project development.
CO 12	Able to adopt skills, languages, environment and platforms for creating innovative solutions for the project.

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 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.

INDEX

Chapter No	Title	Page No.
1	Introduction	13-16
	1.1 Introduction	13
	1.2 Motivation	14
	1.3 Problem Definition	14
	1.4 Existing Systems	15
	1.5 Lacuna of the existing systems	15
	1.6 Relevance of the Project	15
2	Literature Survey	17-21
	A. Brief Overview of Literature Survey	17
	B. Related Works	17
	2.1 Research Papers Referred (Mentioned in IEEE format) a. Abstract of the research paper (in your own word) b. Inference drawn	17
	2.2. Inference drawn	20
3	Requirement Gathering for the Proposed System	22-23
	3.1 Introduction to requirement gathering	22
	3.2 Functional Requirements	23
	3.3. Non-Functional Requirements	23
	3.4. Hardware, Software , Technology and tools utilized	23
	3.5. Constraints	23
4	Proposed Design	24-30
	4.1 Block diagram representation of the system	24
	4.2 Modular design of the system	25

	4.3 Detailed Design (DFD - level 0,1,2, State Transition Diagram, ER Diagram, Use case diagram)	26
	a.DFD - Level 0,1,2	26
	c. Use Case diagram	27
	d. ER Diagram	28
	4.4. Project Scheduling & Tracking using Timeline / Gantt Chart	30
5	Implementation of the Proposed System	31-34
	5.1. Methodology employed for development	31
	5.2 Algorithms and flowcharts for the respective modules developed	32
	5.3 Datasets source and utilization	34
6	Testing of the Proposed System	35-38
	6.1 . Introduction to testing	35
	6.2. Types of tests Considered	35
	6.3 Various test case scenarios considered	38
	6.4. Inference drawn from the test cases	38
7	Results and Discussions	39-49
	7.1. Screenshots of User Interface (UI) for the respective module	39
	7.2. Performance Evaluation measures	43
	7.3. Input Parameters / Features considered	45
	7.4. Graphical and statistical output	47
	7.5. Comparison of results with existing systems	49
	7.6. Inference drawn	49
8	Conclusion	50-51
	8.1 Limitations	50
	8.2 Conclusion	50

	8.3 Future Scope	50
9	References	52
10	Appendix	53

Table of Figures

Sr No.	Title	Page No
1	Graph showing the increase in the rate of CyberBullying in the recent years	13
2	Graph showing the increase in the number of fake accounts	14
3	Rumor detection Results(R: Rumor, N: Non-Rumor)	20
4	Block Diagram	24
5	Modular Design for Cyberbully and fake account detection	25
6	DFD Level-0 Diagram	26
7	DFD Level-1 Diagram	26
8	DFD Level-2 Diagram	27
9	Use Case Diagram	28
10	ER Diagram	29
11	Task Usage Of Project	30
12	Gantt Chart	30
13	SVM Model	34
14	Integration Testing	37
15	Home Page	39
16	Login Page	39
17	Register Page	40
18	New Post Page	40

19	Details Page	41
20	Admin Page	41
21	Post Details Page	42
22	Fake Account Page	43
23	Comparison of F1 Score of the different Algorithm in graph form	44
24	Cyberbully Dataset	46
25	Fake Account Dataset	47
26	Exploratory Data Analysis of comments based on different categories	48
27	Comparison of F1 Score of the different Algorithms	48
28	Accuracy Comparison For Fake Account	49
29	IEEE Paper	53
30	ICAST Conference Certificate	56
31	Plagiarism Report	59
32	Project Review Sheet	61

CHAPTER – 1

INTRODUCTION

1.1 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 young adults, are finding new ways to bully one another over the Internet. Close to 25% of parents in a study conducted by Symantec reported that, to their knowledge, their child has been involved in a cyberbullying incident.

Other than cyberbullying, Spreading False information is increasingly at a rapid pace. The number of users in social media is increasing exponentially. Instagram has recently gained immense popularity among social media users.

The major source of the fake news are the 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.

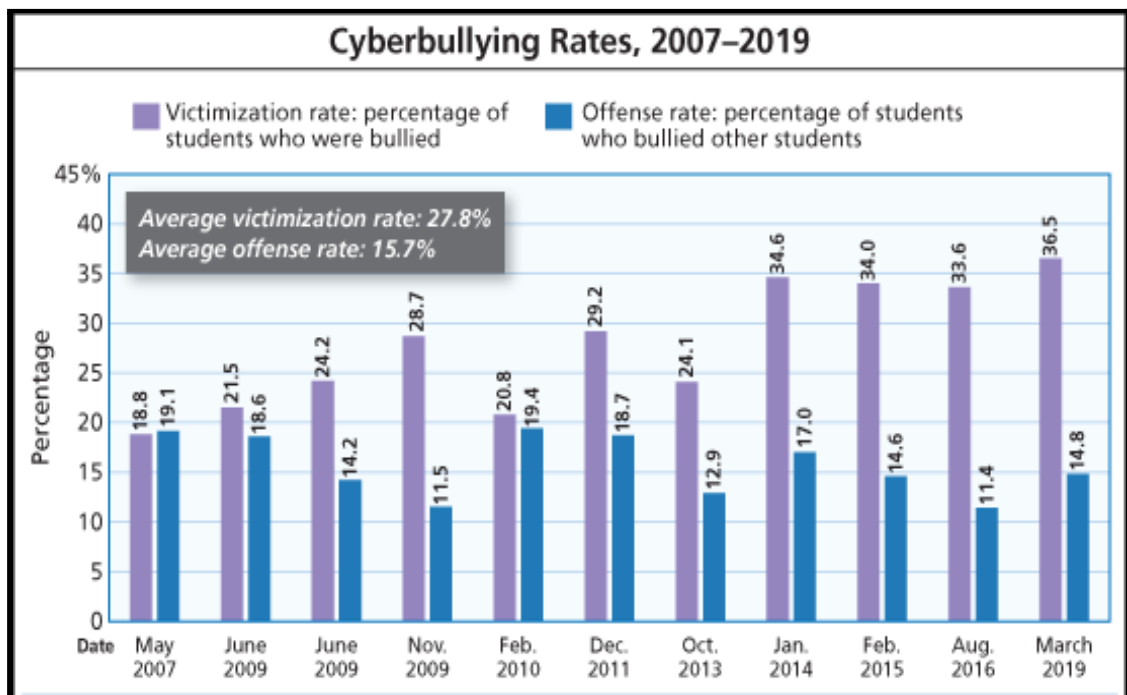


Fig 1.1.1-Graph showing the increase in the rate of CyberBullying in the recent years

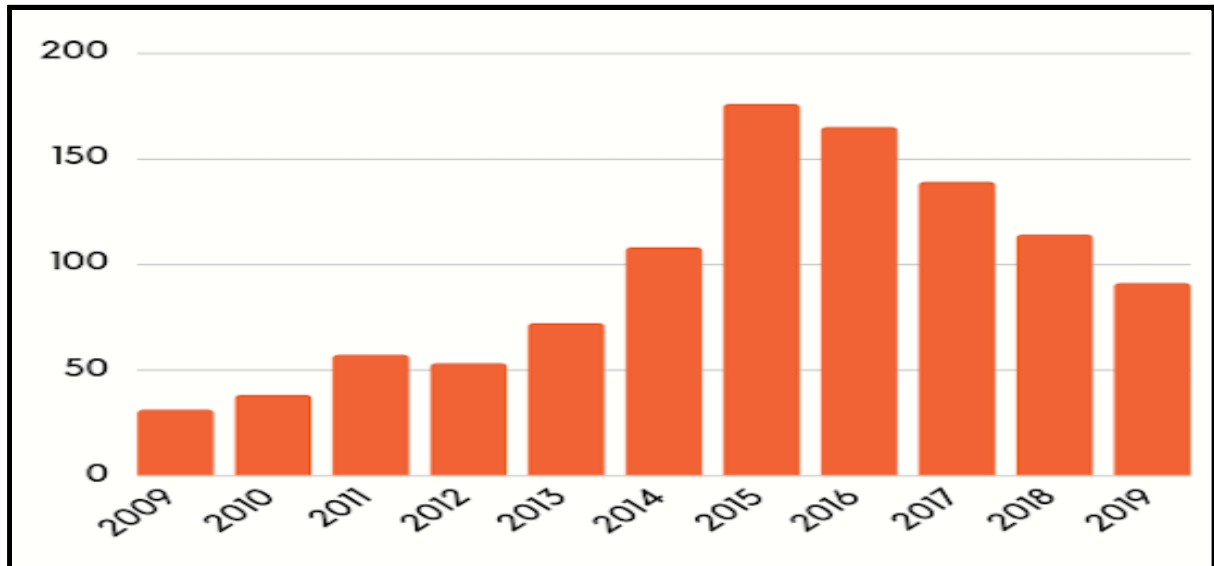


Fig 1.1.2-Graph showing the increase in the number of fake accounts

1.2 Motivation

The use of social networks such as Facebook, Twitter, Google+, Instagram, and LinkedIn is on the rise. Individuals and organizations use social networks to express their views, advertise their products, and express future policies of their companies and organizations. By expanding the use of social networks, malicious users seek to violate the privacy of other users and abuse their names and credentials by creating fake accounts, which has become a concern for users. Hence, social networks providers are trying to detect malicious users and fake accounts in order to eliminate them from social networking environments. Creating fake accounts in social networks causes more damage than any other cybercrime .

Removing fake accounts has attracted the attention of many researchers thus, extensive research has been carried out on the identification of fake accounts in social networks. Different approaches are proposed to find fake accounts based on attribute similarity hence this generates an awareness in the field of social technology era to remove cyberbullying and eliminate the fake accounts from social media.

1.3 Problem Definition

One of the common issues everyone is facing and it is impacting the people, in which some are long period of sadness, anger, irritability, loss of interest in activities, being restless, anxious and worried, even in some cases they go into depression and take steps to scarify their life. It is unfortunate that there are no special Anti-Cyberbullying Laws in India yet. There are some common types of cyberbullying that is Flaming, Harassment, Denigration, Impersonation, Trickery. So to detect cyberbullying we have to make some software that will detect it and then report it to www.cybercrime.gov.in. Similarly, we will detect fake accounts.

1.4 Existing Systems

Other systems use the algorithm first which gives the message a value and then based on our pre trained data, it decides if the comment is harsh enough to be transformed or not. If it is indeed harsh, then the system will look through our complex network of users and find how this user talks to people on average and how they talk to the end user on average.

Other systems detect cyberbullying attacks in both English and Arabic languages, including Arabish (or Arabizi). Arabizi is the use of Latin letters in writing Arabic text . Sometimes it is referred to as the Arabic chat alphabet. This system uses ML techniques for feature selection/extraction and classification. In a later stage ML will be used for transliteration from Arabic and Arabizi to English characters.

1.5 Lacuna of the existing systems

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.

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] 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.

1.6 Relevance of the Project

Most people who are bullied online are also bullied in person. However, while offline bullying allows one the chance to avoid areas and situations that will put them in direct contact with a bully, cyberbullying offers no such reprieve.

Cyberbullying can follow victims wherever they go, whether they are in a crowd or alone. Cyberbullies can reach their victims, 24 hours a day, 7 days a week, 365 days a year. They often post hurtful content online, anonymously, so that they cannot be traced or stopped.

Given the nature of social media, such content is quick to go viral, and reaches a large audience in the blink of an eye, making it difficult, even impossible, for authorities to delete the harmful content before it wrecks damage.

The all-pervasive nature of cyberbullying, as well as the amount of time it takes to trace cyberbullies, makes the growth of cyberbullying an alarming trend across the globe.

Because cyberbullying is difficult to track, many victims feel helpless and unable to cope with it, especially if the bullying is personal and long-drawn. It is no surprise, therefore, that this form of bullying has been known to trigger depression and anxiety in its victims. In many instances, it has also resulted in victims developing suicidal tendencies.

Hence, social networks providers are trying to detect malicious users and fake accounts in order to eliminate them from social networking environments. Creating fake accounts in social networks causes more damage than any other cybercrime.

CHAPTER – 2

LITERATURE SURVEY

In this chapter we are going to see all the literature surveys associated with our project. We have studied all of the below mentioned papers from which we have drawn some inferences and conclusions. We got to know a lot about the work which we have to do and the way in which we should proceed so that we can get the best classification model that will help to classify the posts on social platforms as toxic, sever_toxic , threat, insult etc. For the fake account also we got to know which are all parameters that we should take into consideration so that the model will give accurate results.

There is really lots of work being done in this field to identify the cyberbully and also the fake account detection in twitter, instagram and facebook is using some techniques to overcome this problem and provide overall good experience to its users.

2.1 Research Papers Referred

1. Fake Twitter accounts: Profile characteristics obtained using an activity-based pattern detection approach[1]:

Abstract : In this paper analysis 62 millions of publicly available Twitter user profiles was conducted and a strategy to retroactively identify automatically generated fake profiles was established. As recently as 2010, when the maximum number of Twitter user IDs was estimated to be less than 800 million , it was feasible to crawl over the entire Twitter user ID space. Spam accounts constitute as much as 93% of all new accounts, 68% of which are detected and automatically suspended or deleted by Twitter. To overcome these issues, they performed a Breadth First Search (BFS) over a given set of seed users. As the social graph is crawled, and eventually the user profiles for these IDs are acquired. This ensures that all user profile requests we make to Twitter include only valid Twitter user IDs.

Inference : From this paper we got the information about the fake account dataset quantity, because due to the low number of false positives of fake account data accuracy of model decreased even if the twitter profile database was approx 60 million.

2. Detection of Behavior Patterns through Social Networks likeTwitter, using Data Mining techniques as a method to detect Cyberbullying[2] :

Abstract : Social networks such as Twitter or Facebook have revolutionized the communication mechanism between human beings, but have also generated a negative impact due to inappropriate use, this fact is perpetuated by cybercriminals to hurt other people psychologically, these bad practices are called cyberbullying. This research focuses on the detection and analysis of cyberbullying on pages and with pejorative terms in Spanish, taking advantage of the power of classification of feelings through specialized tools. For the detection of cyberbullying, first the efficiency of classification of each tool is measured, through a set of pejorative terms commonly used to hurt other people.

Inference : In the analysis stage we use data mining techniques to generate a dictionary of pejorative terms that are related to cyberbullying and thus be able to generate behavior patterns of these terms. And in this way provide better tools so that psychology specialists can optimize their work. The results show which platform is more flexible, and also shows which is best suited to the search of incidences of cyberbullying on Twitter.

3. Classification of Cyberbullying in Facebook Using Selenium and SVM[3]:

Abstract : Cyberbullying is one of the emerging problems over the past few years especially to teenagers. Approximately 24% of teens go online constantly, facilitated by the widespread availability of smartphones. Almost 21% of teens said the main reason they checked social media always was to make sure nobody was saying mean or bad things to them. Cyberbullying related Facebook posts were harvested by a customized web scraper tool.

Inference : In this paper facebook data were used for classification using Support Vector Machines (SVM) models. A total of 2263 data was used for training data, Facebook posts. Based on these posts, the study achieved the precision of 88% and the recall is 87%. So it is quite a good algorithm for cyberbully detection.

4. Identifying Fake News from the Variables that Governs the Spread of Fake News[4]:

Abstract : Several researchers have attempted to investigate the processes that govern and support the spread of fake news. This paper collates and identifies these variables. This paper then categorised these variables based on three key players that are involved in the process: Users, Content, and Social Networks. The authors conducted an extensive review of the literature and a reflection on the key variables that are involved in the process. The paper has identified a total of twenty-seven variables. Then the paper presents a series of tasks to mitigate or eliminate these variables in a holistic process that could be automated to reduce or eliminate fake news propagation. Finally, the paper suggests further research into testing the method in lab conditions.

Inference: In paper has reviewed a variety of variables identified by researchers in the field of understanding the factors that influence fake news. The variables show a significant overlap in views but also concentration on different players. As such, the paper collated all these variables and redistributed them based on the key players. This has helped build a holistic and bigger picture of the environment in which Fake News thrives. The variables identified pinpointed some areas where one can see how different social media platforms have attempted to combat fake news and failed.

5. Detecting Rumors from Microblogs with Recurrent Neural Networks[5]:

Abstract : Microblogging platforms are an ideal place for spreading rumors and automatically debunking rumors is a crucial problem. To detect rumors, existing approaches have relied on hand-crafted features for employing machine learning algorithms that require daunting manual effort. Upon facing a dubious claim, people dispute its truthfulness by posting various cues over time, which generates long-distance dependencies of evidence. This paper presents a novel method that learns continuous representations of microblog events for identifying rumors. The proposed model is based on recurrent neural networks (RNN) for learning the hidden representations that capture the variation of contextual information of relevant posts over time. Experimental results on datasets from two real-world microblog platforms demonstrate that (1) the RNN method outperforms state-of-the-art rumor detection models that use hand-crafted features; (2) performance of the RNN-based algorithm is further improved via sophisticated recurrent units and extra hidden layers; (3) RNN-based method detects rumors more quickly and accurately than existing techniques, including the leading online rumor debunking services.

Inference : In this research, we propose a deep learning framework for rumor debunking. Our method learns RNN models by utilizing the variation of aggregated information across different time intervals related to each event. We empirically evaluate our RNN-based method with three widely used recurrent units, tanh, LSTM and GRU, which perform significantly better than the state-of-the-art.

(a) Twitter dataset					
Method	Class	Accuracy	Precision	Recall	F_1
DT-Rank	R	0.644	0.638	0.675	0.656
	N		0.652	0.613	0.632
SVM-RBF	R	0.722	0.856	0.526	0.651
	N		0.663	0.914	0.769
DTC	R	0.731	0.724	0.757	0.740
	N		0.739	0.704	0.721
RFC	R	0.772	0.717	0.908	0.801
	N		0.870	0.634	0.734
SVM-TS	R	0.808	0.735	0.963	0.834
	N		0.947	0.652	0.772
tanh-RNN	R	0.827	0.847	0.833	0.840
	N		0.804	0.820	0.812
LSTM-1	R	0.855	0.855	0.883	0.869
	N		0.854	0.820	0.837
GRU-1	R	0.864	0.857	0.900	0.878
	N		0.872	0.820	0.845
GRU-2	R	0.881	0.851	0.950	0.898
	N		0.930	0.800	0.860

Fig 2.1.5 Rumor detection Results(R: Rumor, N: Non-Rumor)

6. Automatic detection of cyberbullying in social media text[6]:

Abstract : The focus of this paper is on automatic cyberbullying detection in social media text by modelling posts written by bullies, victims, and bystanders of online bullying. We describe the collection and fine grained annotation of a cyberbullying corpus for English and Dutch and perform a series of binary classification experiments to determine the feasibility of automatic cyberbullying detection. We make use of linear support vector machines exploiting a rich feature set and investigate which information sources contribute the most for the task. Experiments on a hold-out test set reveal promising results for the detection of cyberbullying-related posts. After optimisation of the hyperparameters, the classifier yields an F1 score of 64% and 61% for English and Dutch respectively, and considerably outperforms baseline systems .

Inference :A set of binary classification experiments were conducted to explore the feasibility of automatic cyberbullying detection on social media. In addition, we sought to determine which information sources contribute most to the task. Two classifiers were trained on an English and Dutch ASKfm corpus and evaluated on a hold-out test of the same genre. Overview of the most related cyberbullying detection approaches.After feature and hyperparameter optimisation of our models, a maximum F1 score of 64.32% and 58.72% was obtained for English and Dutch.

2.2. Inference drawn

The very first point is most of them haven't used the NLP for their classification of the text they just trained it on their model and founded the results and the second point we got is that they had trained it only one models and different projects in the literature have different models with varying accuracy, So, to overcome the first point we had used the NLP for cleaning and for the second problem we will train and test our prediction on the different models (for e.g Random Forest, Logistic

Regression , Decision Tree etc.) and find the best models with best accuracy for the toxicity type, so that each and every type of offensive language will be identified and classified accurately.

Overall Inference from all the above papers is that the use of ML algorithm varies with different types of dataset so we will have to use some of the algorithms which are used as per the literature survey, for the testing and after comparison we can use the best model based on countvectorizer and F1 score value. From the above literature survey we got to know that the Random forest and SVM is giving best results for classification, so we will focus more on these algorithms only so that we'll save a lot of time.

CHAPTER – 3

REQUIREMENT GATHERING

3.1 Introduction to requirement gathering

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.

3.2 Functional Requirements

- **Social Media-**

The government uses social media technologies to extract opinion from people regarding a specific issue , these social media technologies have now been seen as the most extensively used platforms to conduct electronic participation activities. According to smallbiztrends.com, Facebook, Twitter and Instagram are one of the famous social networking sites that a lot of people are using including establishments and organizations .With high online activity using these sites, teens can be a victim or a perpetrator of cyberbullying

- User authentication module should detect and reject malicious authentication attempts.
- The system should decide whether a suspicious content should be checked for malicious behaviour or for fake identity or activity.
- Each time a malicious behaviour is detected, an account should be added in the appropriate malicious behaviour reputation list.
- **Admin-** It can view and block all the malicious accounts

3.3 Non-Functional Requirements

- **Availability** - The system is available all the time, no time constraint

3.4 Hardware, Software , Technology and tools utilized

- Intel Pentium Processor
- RAM > 4GB
- Django
- Machine Learning Algorithms
- Anaconda

3.5 Constraints

- Continuous Internet Connection
- Risk Management
- System Failure

CHAPTER – 4

PROPOSED DESIGN

This chapter describes the block diagram, modular design and detailed design of the system. Detailed design consists of a data flow diagram(DFD level-0,1,2) , State transition diagram, ER diagram and Use Case Diagram. Project scheduling and tracking using timeline/ gantt chart is also mentioned in this chapter. These all diagrams and designs give us the overall working of the project.

4.1 Block diagram of the system

A block diagram is a specialized, high-level flowchart. It is used to design new systems or to describe and improve existing ones. Its structure provides a high-level overview of major system components, key process participants, and important working relationships.

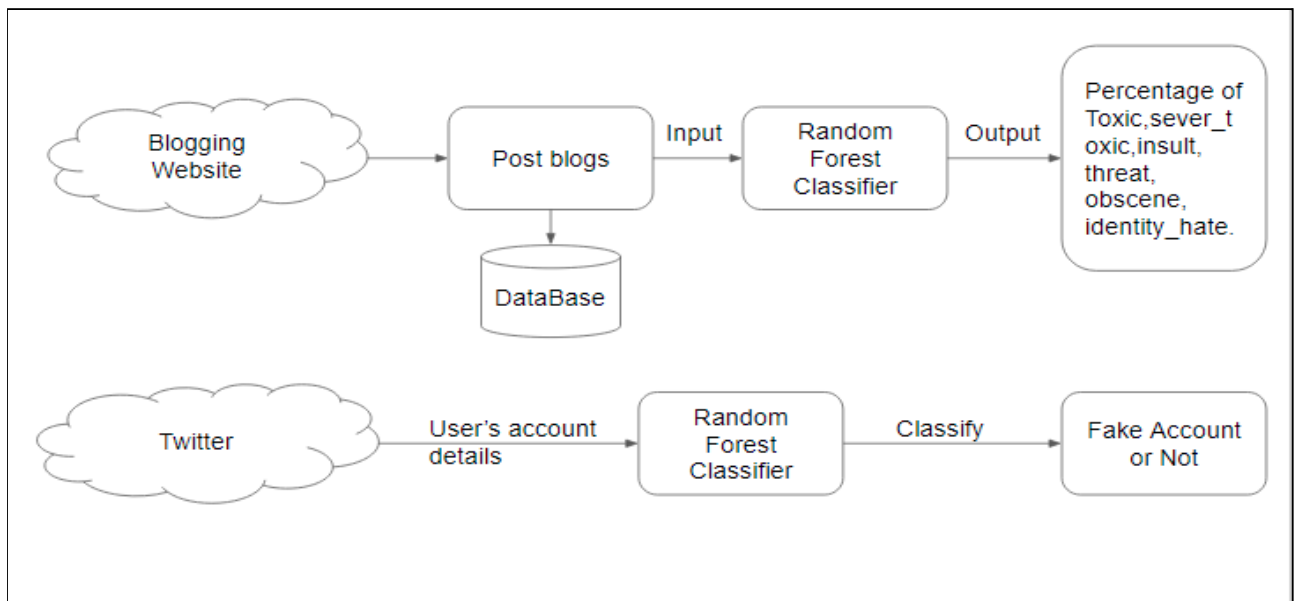


Fig 4.1.1 Block Diagram

The user will first login in to our portal with his/her credentials or can sign up on our portal for new registration. The portal can work as a simple blog where users can post their views and can read other people's views. on posting the views it will undergo certain machine learning algorithm processing where it will determine whether the following post is cyberbullying or not . If found that the post is vulnerable the system will further check that if the account is fake or not. if found fake it will block the account and if the account is not fake the system will report the tweet.

4.2 Modular design of the system

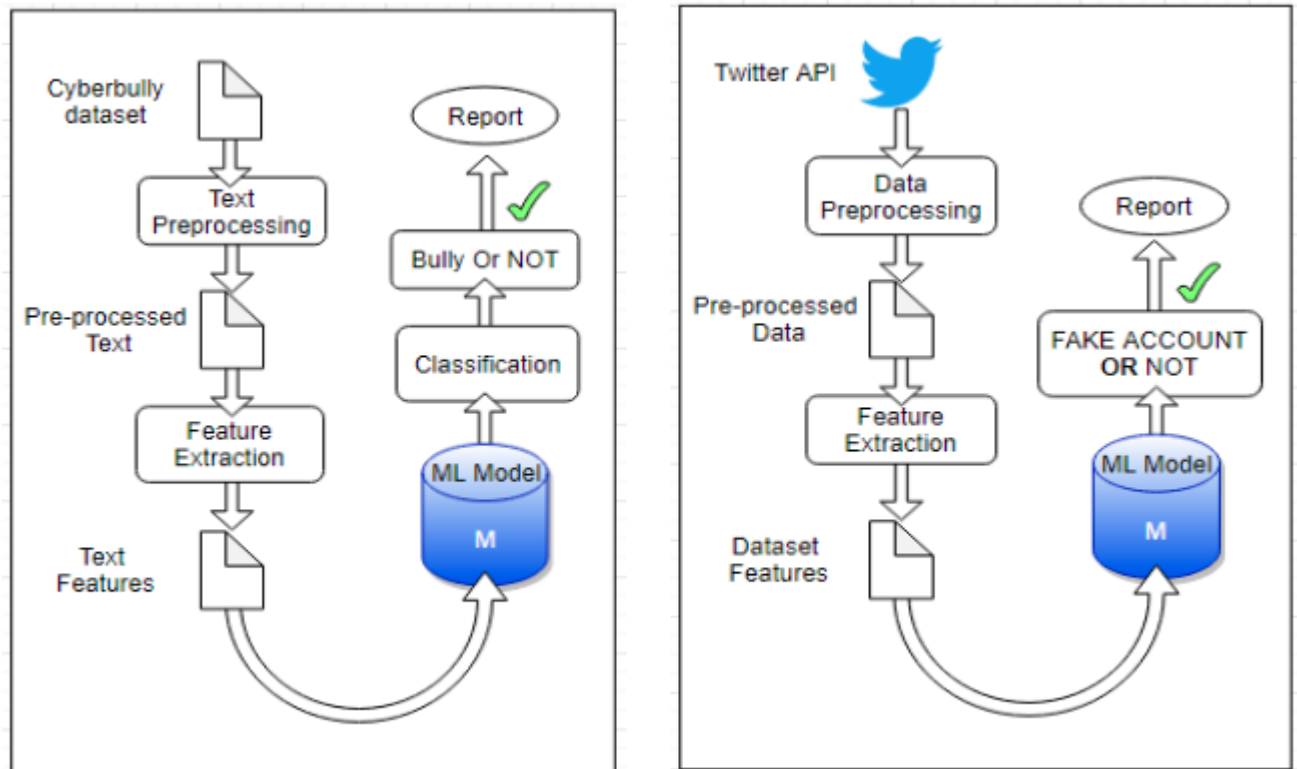


Fig 4.2.1 Modular Design for Cyberbully and fake account detection

As we can see here initially we have taken dataset for cyberbully and did some preprocessing (like tokenization, lowering text, then stop word removal), after this we have extracted the features like we have separated all the categories of text and then created balanced training and testing dataset so that model will not be overfit. After this we trained different models like (Logistic Regression, SVM, Random Forest, KNNB, BernoulliNB, Multinomial DB). Then we created a TFIDF Vectorizer and calculated F1 score of each model and from that we selected RandomForest classifier is best for each type of comment type. And then we tested and finally we did Pickling for trained RandomForest models for all categories, so that we can easily use those models.

4.3 Detailed Design (DFD - level 0,1,2, State Transition Diagram, ER Diagram, Use case diagram)

a. Data Flow Diagram

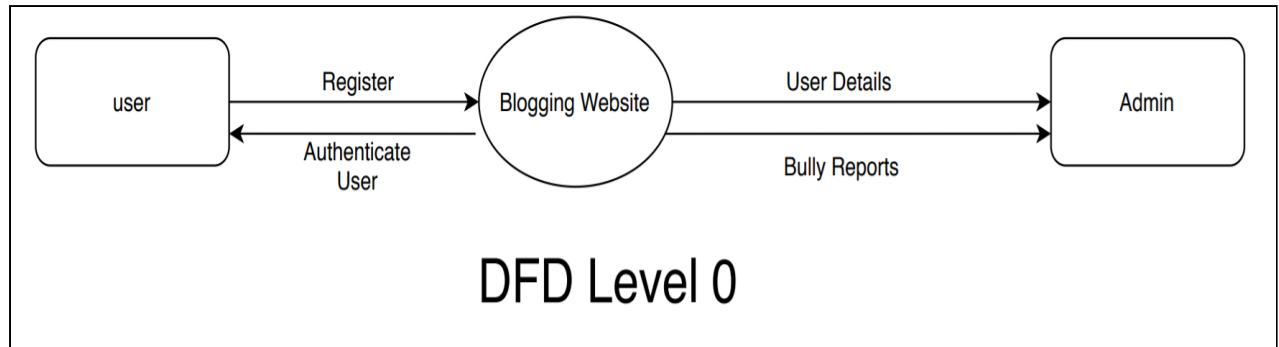


Fig 4.3.1 DFD Level-0 Diagram

As shown above the DFD Level-0 diagram which shows that the user first needs to register to the portal then the user details will be forwarded to the admin where if the user posts something abusive at the website then the bully reports will be send to the admin and the admin can authenticate the user.

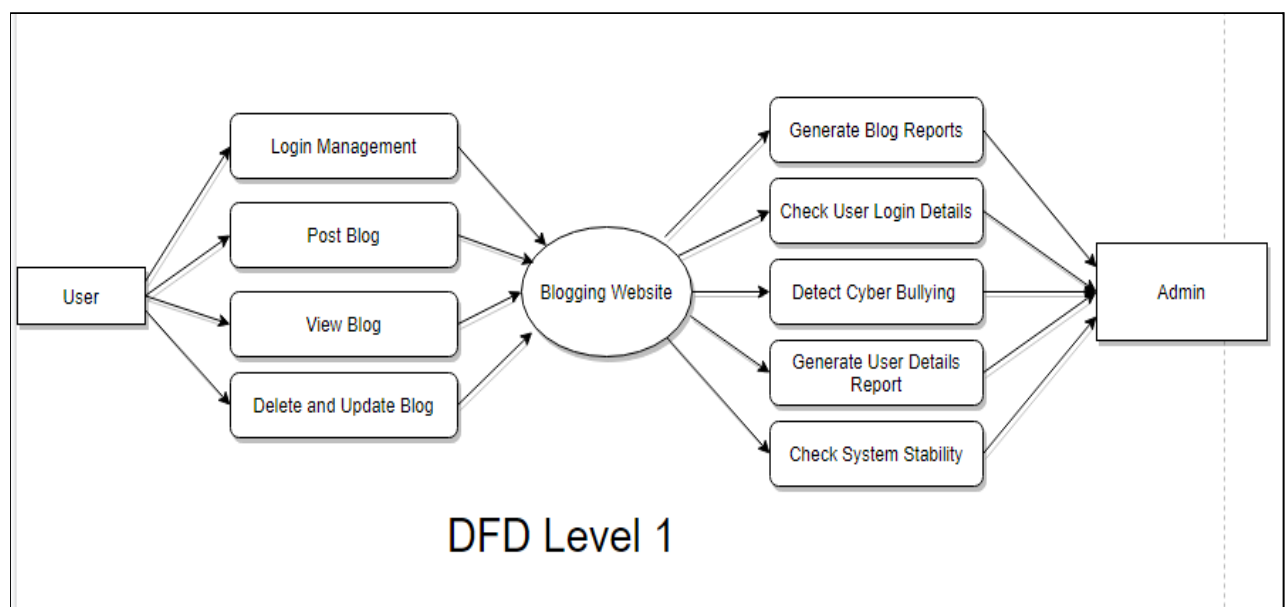


Fig 4.3.2 DFD Level-1 Diagram

In the DFD Level-1 Figure the user can perform the functionality like it can do login, post blog, view its blog and delete or update its blog on the blogging website and from the admin side. It can generate blog reports, check user login details, detect cyberbullying, generate user details reports, check system stability.

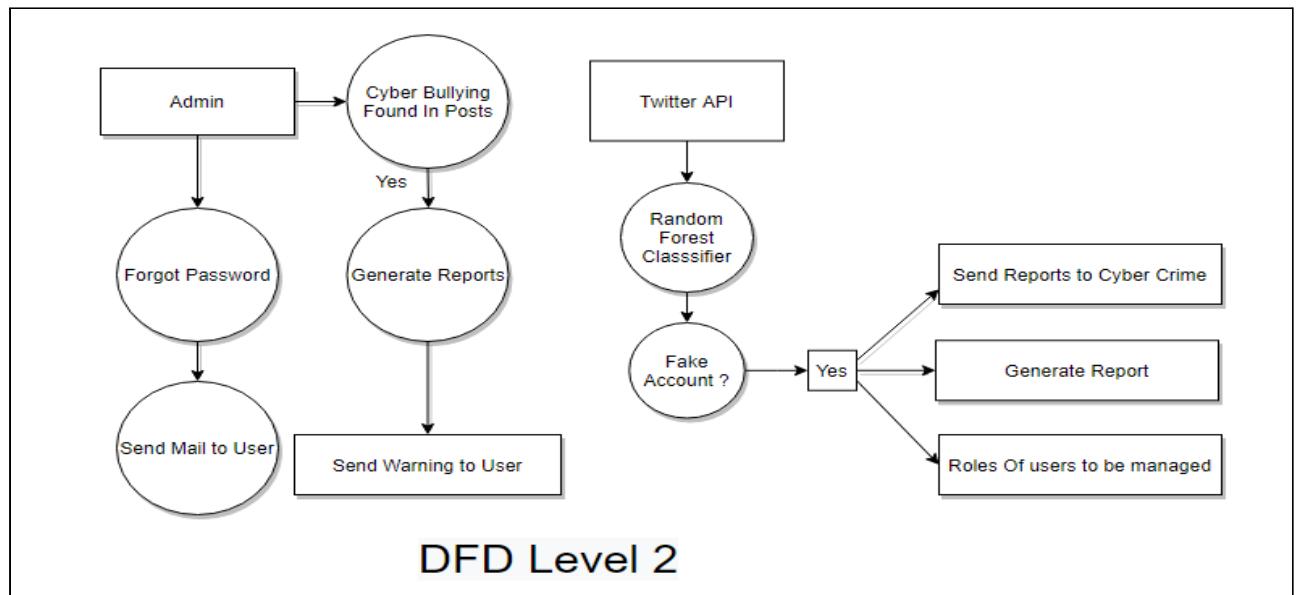


Fig 4.3.3 DFD Level-2 Diagram

In DFD Level 2 Diagram, as shown above the flow is like User will Register and then he/she will log into the blogging Website where he/she will post some blogs and can view other users blogs also. If he/she has posted some offensive or bully content then that will be detected and then Account verification will be also done if the account is fake or not valid then a report will be generated and that will be sent to the Cyber Crime and Users Account will be blocked.

b. USE CASE DIAGRAM

A use case diagram is a dynamic or behavior diagram in UML. Use case diagrams model the functionality of a system using actors and use cases. ... In this context, a "system" is something being developed or operated, such as a web site. The "actors" are people or entities operating under defined roles within the system.

This is the sample Use Case Diagram representing the Cyberbullying and fake Account detection model. If we look into diagram we can see the Use Cases as Follows:

Manage Account, Manage Blog, Add Post, View Blogs, Manage application, Manage Users, Account and Blog. We have two Actors as we can see in the diagram User and Admin.

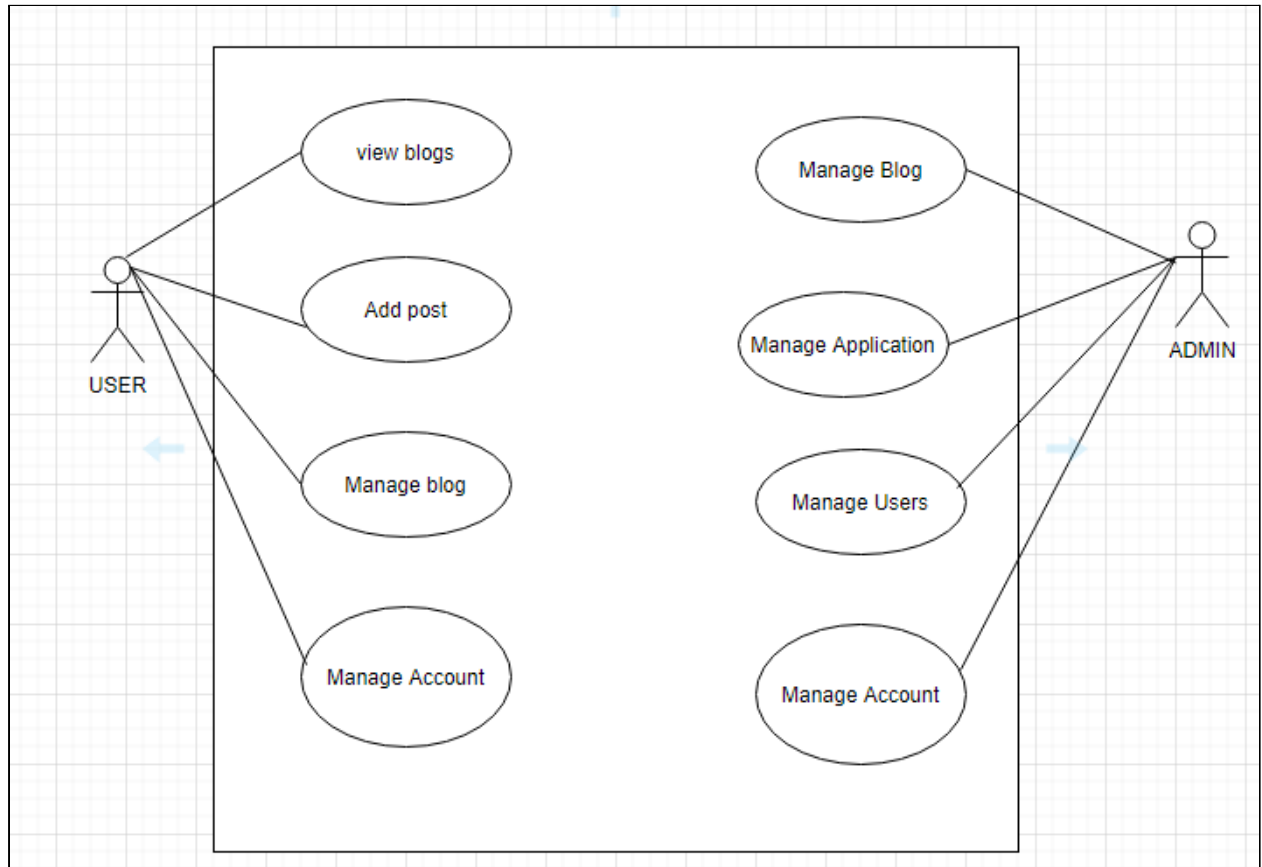


Fig 4.3.4 Use Case Diagram

c. ER Diagram

An Entity Relationship (ER) Diagram is a type of flowchart that illustrates how “entities” such as people, objects or concepts relate to each other within a system. ER Diagrams are most often used to design or debug relational databases in the fields of software engineering, business information systems, education and research. Also known as ERDs or ER Models, they use a defined set of symbols such as rectangles, diamonds, ovals and connecting lines to depict the interconnectedness of entities, relationships and their attributes.

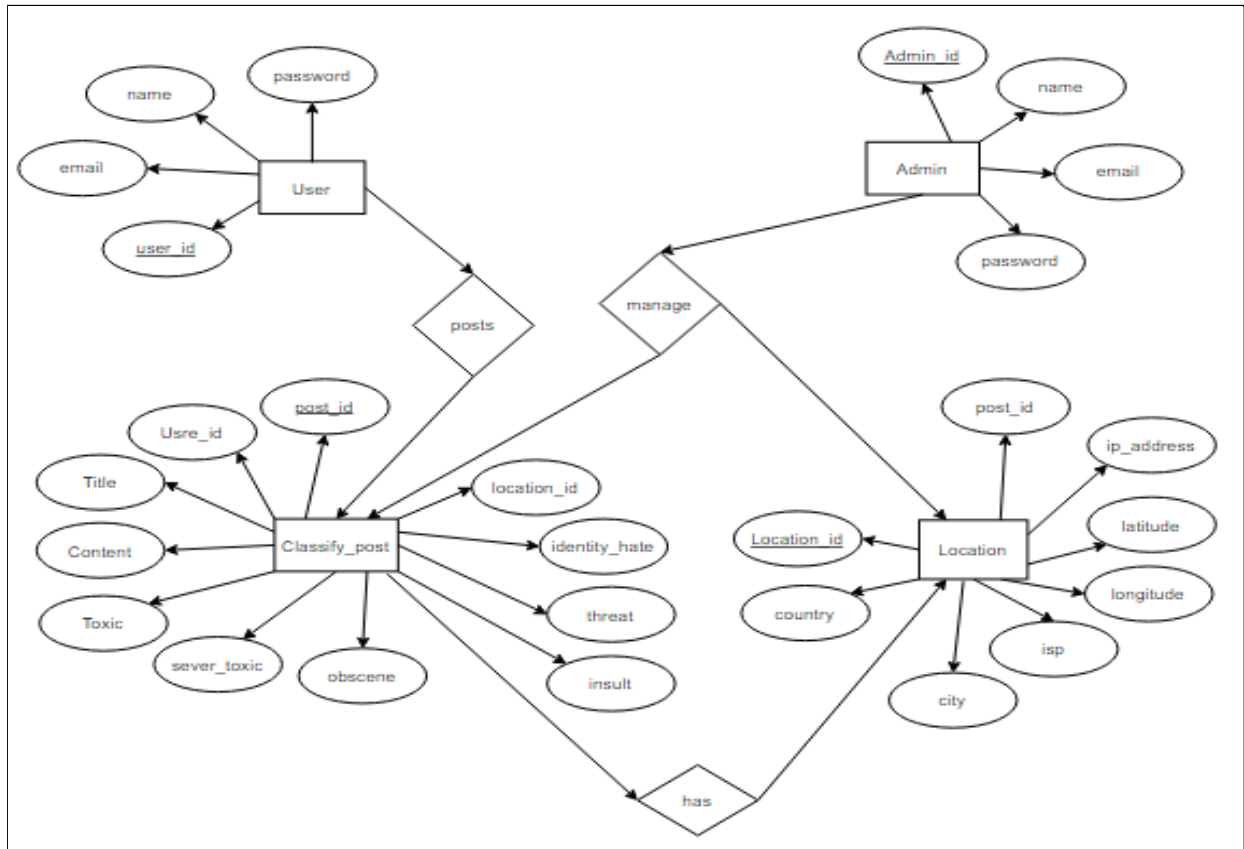


Fig 4.3.5 ER Diagram

As we can see that there are four tables (user table, classify_post table, location table and admin table). User table consists of four attributes such as user_id(primary key), name, email and password. Classify posts consist of eleven attributes such as post_id(primary key), user_id(foreign key), title, content, toxic, sever_toxic, obscene, threat, insult, identity_hate and location_id(foreign key). Location table consists of 8 attributes and it shows the location of users with longitude and latitude and Internet Service Provider(ISP).

4.4 Project Scheduling & Tracking using Timeline / Gantt Chart

1. Table













	Task Mode ▾	Task Name ▾	Duration ▾	Start ▾	Finish ▾	Predecessors ▾
		Requirements Details	3 days	Tue 31-03-20	Thu 02-04-20	
		Interactive Requirements	5 days	Fri 03-04-20	Thu 09-04-20	1
		Retail Requirements	2 days	Fri 10-04-20	Mon 13-04-20	2
		Business System Requirements	1 day	Tue 14-04-20	Tue 14-04-20	3
		Development	12 days	Wed 15-04-20	Thu 30-04-20	4
		Unit test	3 days	Fri 01-05-20	Tue 05-05-20	5
		Handover to test	2 days	Wed 06-05-20	Thu 07-05-20	6
		Test Planning	3 days	Fri 08-05-20	Tue 12-05-20	7
		Test Analysis and Design	1 day	Wed 13-05-20	Wed 13-05-20	8
		Test execution and Recording	2 days	Thu 14-05-20	Fri 15-05-20	9
		Test Completion	4 days	Mon 18-05-20	Thu 21-05-20	10

Fig 4.4.1 Task Usage Of Project

2. Gantt Chart

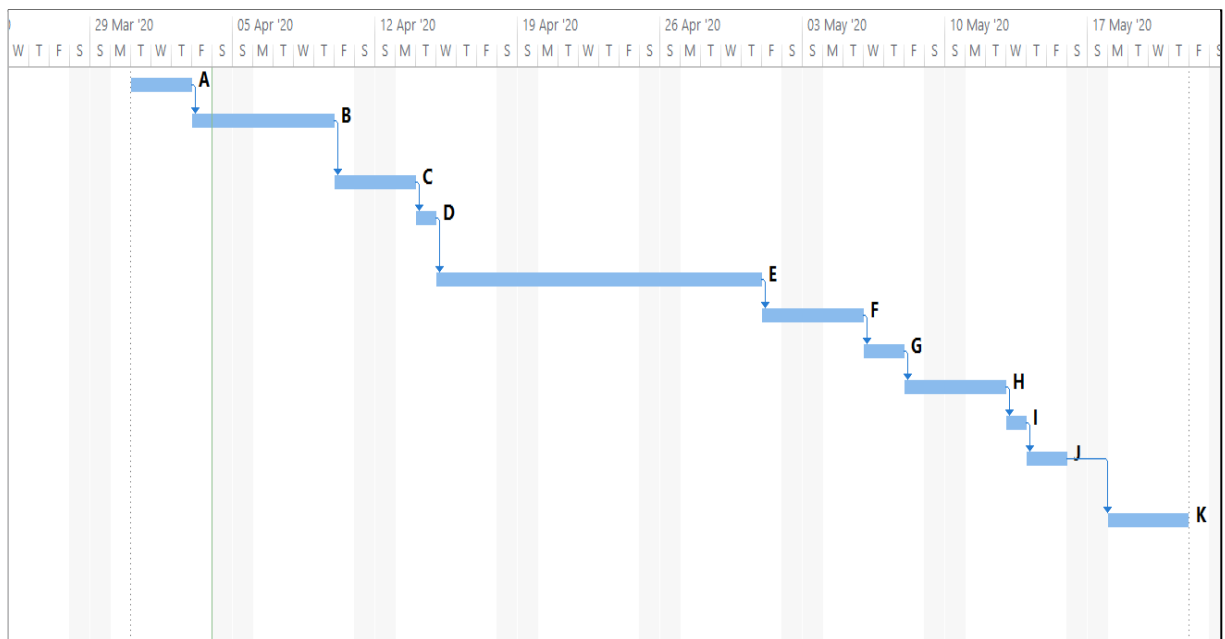


Fig 4.4.2 Gantt Chart

CHAPTER – 5

IMPLEMENTATION OF PROPOSED DESIGN

5.1. Methodology employed for development

The proposed approach contains three main steps namely Preprocessing, features extraction and classification step. In the preprocessing step we clean the data by removing the noise and unnecessary text.

The preprocessing step is done in the following.

1] Tokenization: In this part we take the text as sentences or whole paragraphs and then output the entered text as separated words in a list.

2] Lowering text: This takes the list of words that got out of the tokenization and then lower all the letters Like: 'THIS IS AWESOME' is going to be 'this is awesome'.

3] Stop words and encoding cleaning: This is an essential part of the preprocessing where we clean the text from those stop words and encoding characters like \n or \t which do not provide meaningful information to the classifiers.

4] The second step of the proposed Model is the features extraction step. In this step the textual data is transformed into a suitable format applicable to feed into machine learning algorithms.

5] The last step in the proposed approach is the classification step where the extracted features are fed into a classification algorithm to train, and test the classifier and hence use it in the prediction phase. We will use classifiers, namely, SVM (Support Vector Machine), Naive Bayes, Random Forest, Decision Tree, Logistic Regression.

6] Accuracy of different algorithms will be Compared to get the best possible result. For the 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.

FOR FAKE PROFILE:

Each profile (or account) in a social network contains lots of information such as gender, no. of friends, no. of comments, education, work, etc. Some of this information is private and some are public. Since private information is not accessible, we have used only the information that is public to determine the fake profiles in the social network. We have considered this information as features

of a profile for the classification of fake and real profiles. The steps that we have followed for the identification of fake profiles are as follows.

1. First, all the features are selected on which the classification algorithm is applied.
2. After proper selection of attributes, the dataset of previously identified fake and real profiles are needed for the training purpose of the classification algorithm.
3. After this data preprocessing is done, in the preprocessing step we clean the data by removing the noise and unnecessary text.
4. After Preprocessing this cleaned data is fed to various machine learning classifiers such as SVM, Decision Trees, Random Forest Gradient Descent, Naive Bayes.
5. Accuracy of all these algorithms is compared and the one with best efficiency is selected.
6. For testing real time data is fetched via twitter api is fetched and is given as input to our machine learning model.

5.2 Algorithms and flowcharts for the respective modules developed

5.2.1 Logistic Regression

Logistic regression is one of the well-known techniques introduced from the field of statistics by machine learning. Logistic regression is an algorithm that constructs a separate hyper-plane between two datasets utilizing the logistic function. The logistic regression algorithm takes features (inputs) and produces a forecast according to the probability of a class suitable for the input. For instance, if the likelihood is ≥ 0.5 , the instance classification will be a positive class; otherwise, the prediction will be for the other class (negative class), as given in Equation. logistic regression was used in the implementation of predictive cyberbullying models. $h_{\theta}(x) = \frac{1}{1 + e^{-\theta^T x}}$, (1) if $h_{\theta}(x) \geq 0.5$, $y = 1$ (Positive class) and if $h_{\theta}(x) \leq 0.5$, $y = 0$ (Negative class)

5.2.2 Random Forest algorithm

The Random Forest Algorithm is composed of different decision trees, each with the same nodes, but using different data that leads to different leaves. It merges the decisions of multiple decision trees in order to find an answer, which represents the average of all these decision trees

The random forest algorithm is a supervised learning model; it uses labeled data to “learn” how to classify unlabeled data. This is the opposite of the K-means Cluster algorithm, which is an unsupervised learning model. The Random Forest Algorithm is used to solve both regression and classification problems, making it a diverse model that is widely used by engineers.

When performing Random Forests based on classification data, you should know that you are often using the Gini index, or the formula used to decide how nodes on a decision tree branch

$$Gini = 1 - \sum_{i=1}^c (p_i)^2$$

This formula uses the class and probability to determine the Gini of each branch on a node, determining which of the branches is more likely to occur. Here, p_i represents the relative frequency of the class you are observing in the dataset and c represents the number of classes.

5.2.3 Naives bayes classifier

Naives bayes classifiers are a group of machine learning algorithms that all use the Bayes' Theorem to classify data points. The Bayes' Theorem is named after Reverend Thomas Bayes, a man who studied probability and binomial distributions in the 18th century. The mathematics behind Naive Bayes The algorithm completely depends upon Bayes theorem since the classifiers simply apply the formula to sets of data. This theorem consists of a formula assessing probabilities of different events occurring. The formula below is the simplest version of it, with only two events — Event A

$$P(B|A) = \frac{p(A|B)p(B)}{p(A)}$$

and B.

5.2.4 Support Vector Machine (SVM)

Support Vector Machine (SVM) is a supervised machine learning classifier widely utilized in text classification . SVM turns the original feature space into a user-defined kernel-based higher-dimensional space and then seeks support vectors for optimizing the distance (margin) between two categories. SVM originally approximates a hyperplane separating the two categories. SVM accordingly selects samples from both categories, which are nearest to the hyperplane, referred to as support vectors.

SVM seeks to efficiently distinguish the two categories (e.g., positive and negative). If the dataset is separable by nonlinear boundaries, specific kernels are implemented in the SVM to turn the function space appropriately. Soft margin is utilized to prevent overfitting by giving less weighting to classification errors along the decision boundaries for a dataset that is not easily separable [101]. In this research, we utilize SVM with a linear kernel for the basis function. Figure 2 shows the SVM classifier implementation for a dataset with two features and two categories where all samples for the training are depicted as circles or stars. Support vectors (referred to as stars) are for each of the two

categories from the training samples, meaning that they are nearest to the hyperplane among the other training samples.

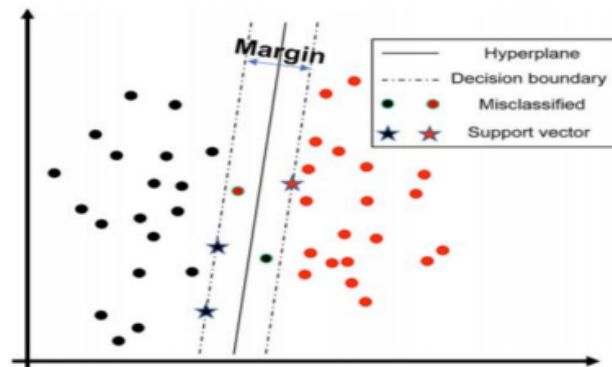


Fig-5.2.4 SVM Model

5.3 Datasets source and utilization

The dataset used for cyberbullying is obtained from kaggle.

Following are the parameters of the dataset: Text(comment),toxic , server toxic , insult , obscene , threat , identity threat. All these parameters are taken into consideration for the training of our model.

For Fake profile detection we have used a kaggle dataset as well as live data fetched from twitter .

The dataset comprises of following parameter : id , screen_name , statuses_count , friend_count , following_count , profile_url , location ,profile_backgroundcolor , favourites , listed_count, language , The parameters taken into consideration are statuses_count , friend_count , following_count, favourites , listed_count,time zone.

The model is tested on live data fetched via twitter api.

CHAPTER – 6

TESTING OF PROPOSED SYSTEM

6.1 . Introduction to testing

Definition: A TEST CASE is a set of conditions or variables under which a tester will determine whether a system under test satisfies requirements or works correctly.

The process of developing test cases can also help find problems in the requirements or design of an application. Testing plays an important role in quality assurance for the software. It is a dynamic method for the verification and validation, where the system to be tested is executed and the behavior of the system is observed

6.2. Types of tests Considered

Alpha Testing

It is the most common type of testing used in the Software industry. The objective of this testing is to identify all possible issues or defects before releasing it into the market or to the user. Alpha Testing is carried out at the end of the software development phase but before the Beta Testing. Still, minor design changes may be made as a result of such testing. Alpha Testing is conducted at the developer's site. In-house virtual user environments can be created for this type of testing.

Entry Criteria for Alpha testing:

- Software requirements document or Business requirements specification
- Test Cases for all the requirements
- Testing Team with good knowledge about the software application
- Test Lab environment setup
- QA Build ready for execution
- Test Management tool for uploading test cases and logging defects
- Traceability Matrix to ensure that each design requirement has at least one test case that verifies it

Exit Criteria for Alpha testing

- All the test cases have been executed and passed.
- All severity issues need to be fixed and closed
- Delivery of Test summary report

- Make sure that no more additional features can be included
- Sign off on Alpha testing

Black Box Testing

BLACK BOX TESTING, also known as Behavioral Testing, is a software testing method in which the internal structure/design/implementation of the item being tested is not known to the tester. These tests can be functional or non-functional, though usually functional. This method is named so because the software program, in the eyes of the tester, is like a black box; inside which one cannot see. This method attempts to find errors in the following categories:

- Incorrect or missing functions
- Interface errors
- Errors in data structures or external database access
- Behavior or performance errors
- Initialization and termination errors

White box testing

White box testing techniques analyze the internal structures, the used data structures, internal design, code structure and the working of the software rather than just the functionality as in black box testing. It is also called glass box testing or clear box testing or structural testing.

Working process of white box testing:

1.Input: Requirements, Functional specifications, design documents, source code.

2.Processing: Performing risk analysis for guiding through the entire process.

3.Proper test planning: Designing test cases so as to cover the entire code. Execute rinse-repeat until error-free software is reached. Also, the results are communicated.

Output: Preparing final report of the entire testing process.

UNIT TESTING

Unit testing is a type of software testing where individual units or components of a software are tested. The purpose is to validate that each unit of the software code performs as expected. Unit Testing is done during the development (coding phase) of an application by the developers. Unit

Tests isolate a section of code and verify its correctness. A unit may be an individual function, method, procedure, module, or object.

In SDLC, STLC, V Model, Unit testing is the first level of testing done before integration testing. Unit testing is a WhiteBox testing technique that is usually performed by the developer. Though, in a practical world due to time crunch or reluctance of developers to tests, QA engineers also do unit testing.

INTEGRATION TESTING

It is a level of software testing where individual units are combined and tested as a group. The purpose of this level of testing is to expose faults in the interaction between integrated units. Test drivers and test stubs are used to assist in Integration Testing.

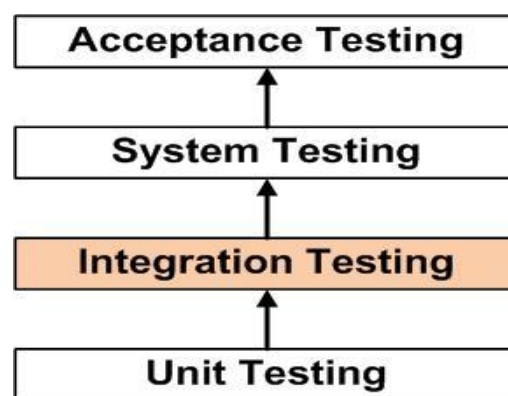


Fig 6.2.1 Integration Testing

SYSTEM TESTING

System Testing is a level of testing that validates the complete and fully integrated software product. The purpose of a system test is to evaluate the end-to-end system specifications. Usually, the software is only one element of a larger computer-based system. Ultimately, the software is interfaced with other software/hardware systems. System Testing is actually a series of different tests whose sole purpose is to exercise the full computer-based system.

System Testing involves testing the software code for following:

- Testing the fully integrated applications including external peripherals in order to check how components interact with one another and with the system as a whole. This is also called End to End testing scenario.
- Verify thorough testing of every input in the application to check for desired outputs.
- Testing of the user's experience with the application.

6.3 Various test case scenarios considered

Type of input	Example	Observations
1. Negative sentences	I will not kill you	This sentence has word kill but it is not toxic and has to be categorized as neutral.algorithm need not be heavily dependent on words it has to extract meaning of the sentence
2. Tricky input	I want to kill my time	There is talk about killing someone but it's time not a person or any living creature. so this comment has to be classified as neutral

6.4. Inference drawn from the test cases

We tested our system on various inputs and concluded that if certain inputs give at least 50% of probability on any category it will be categorized as the following type.

On testing we found that if sentences had more than 2 negation words our system does predict correctly but some sentences with no toxicity gives approx as 40% result which is less than 50% but it can be further reduced to around 20%.

CHAPTER – 7

RESULTS AND DISCUSSION

7.1. Screenshots of User Interface (UI) for the respective module

7.1.1 Home Page

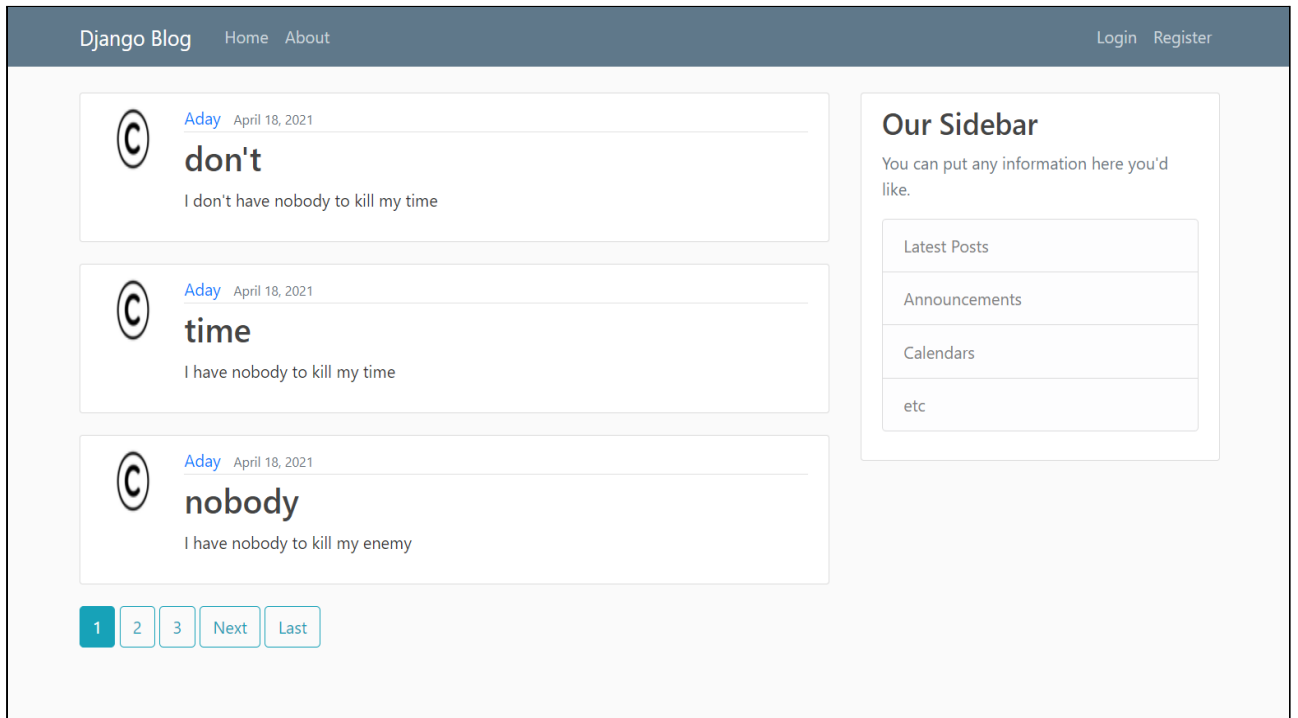


Fig 7.1.1 Home Page

7.1.2 Login Page

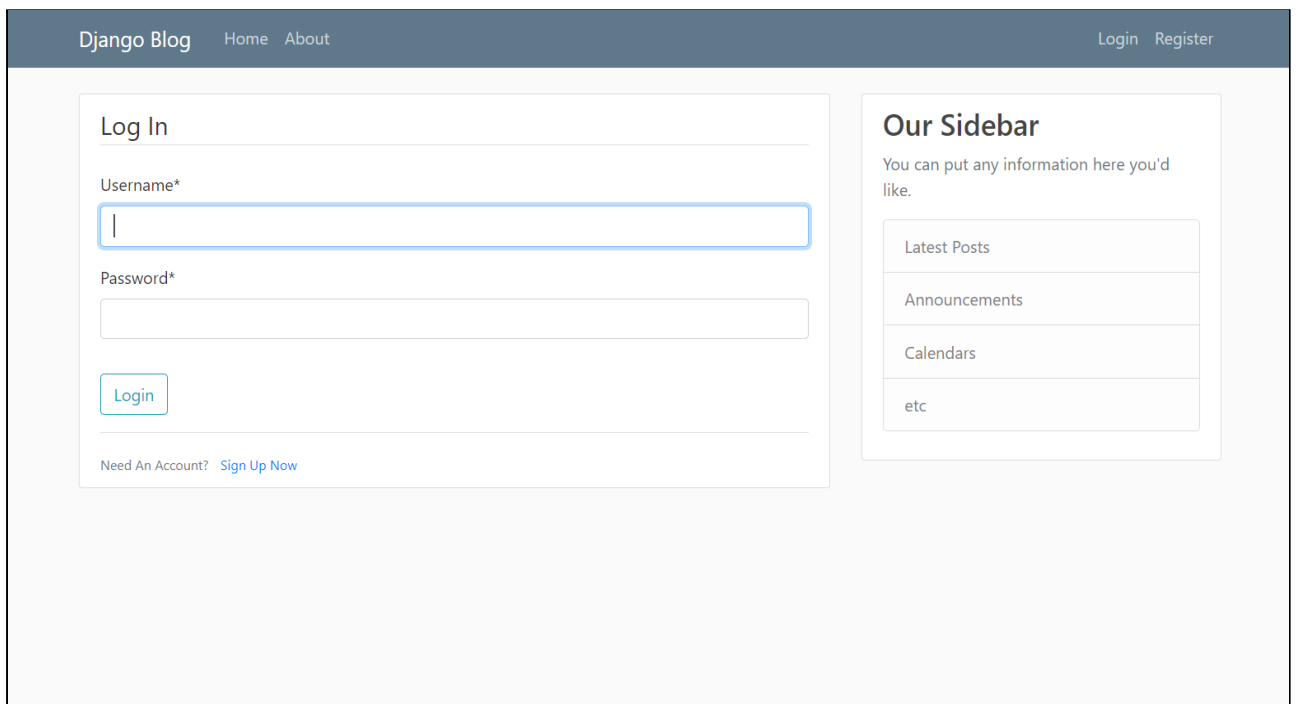
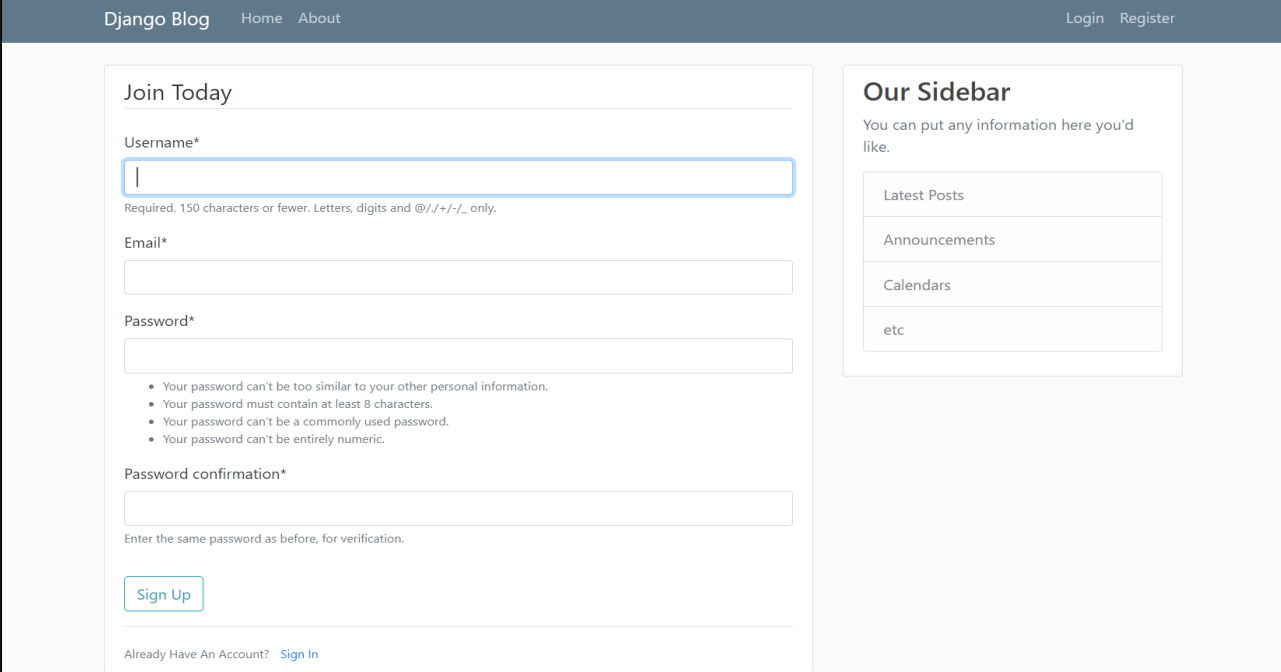


Fig 7.1.2 Login Page

7.1.3 Register Page



The screenshot shows the 'Join Today' registration form on the Django Blog website. The form includes fields for Username, Email, Password, and Password confirmation. The Username field is highlighted with a blue border. Below the Password field, there are four bullet points providing password requirements. A 'Sign Up' button is located at the bottom of the form. To the right of the form is a sidebar titled 'Our Sidebar' with a list of links: Latest Posts, Announcements, Calendars, and etc. The top navigation bar contains links for Django Blog, Home, About, Login, and Register.

Django Blog Home About Login Register

Join Today

Username*

Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Email*

Password*

- Your password can't be too similar to your other personal information.
- Your password must contain at least 8 characters.
- Your password can't be a commonly used password.
- Your password can't be entirely numeric.

Password confirmation*

Enter the same password as before, for verification.

Sign Up

Already Have An Account? [Sign In](#)

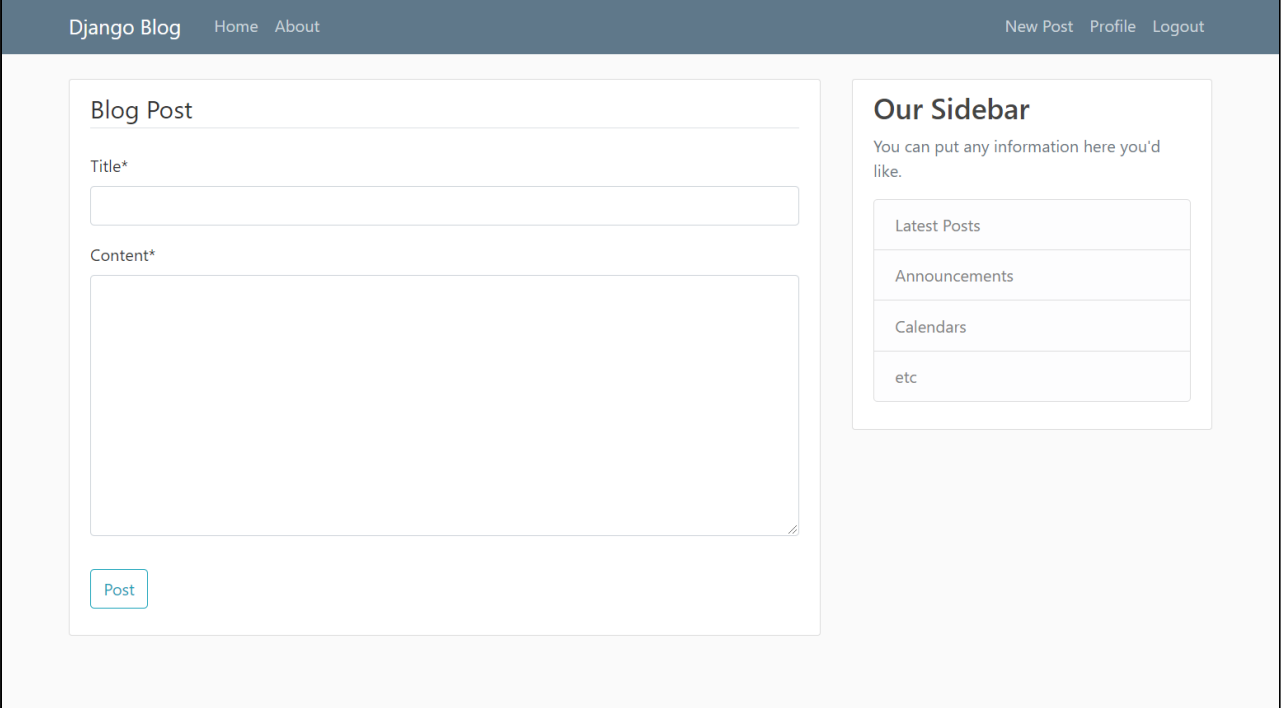
Our Sidebar

You can put any information here you'd like.

- Latest Posts
- Announcements
- Calendars
- etc

Fig 7.1.3 Register Page

7.1.4 New Post Page



The screenshot shows the 'New Post' page on the Django Blog website. The page has a header with links for Django Blog, Home, About, New Post, Profile, and Logout. The main content area is titled 'Blog Post' and contains a 'Title*' field and a 'Content*' text area. A 'Post' button is located at the bottom of the content area. To the right of the main content area is a sidebar titled 'Our Sidebar' with a list of links: Latest Posts, Announcements, Calendars, and etc.

Django Blog Home About New Post Profile Logout

Blog Post

Title*

Content*

Post

Our Sidebar

You can put any information here you'd like.

- Latest Posts
- Announcements
- Calendars
- etc

Fig 7.1.4 New Post Page

7.1.5 Details Page

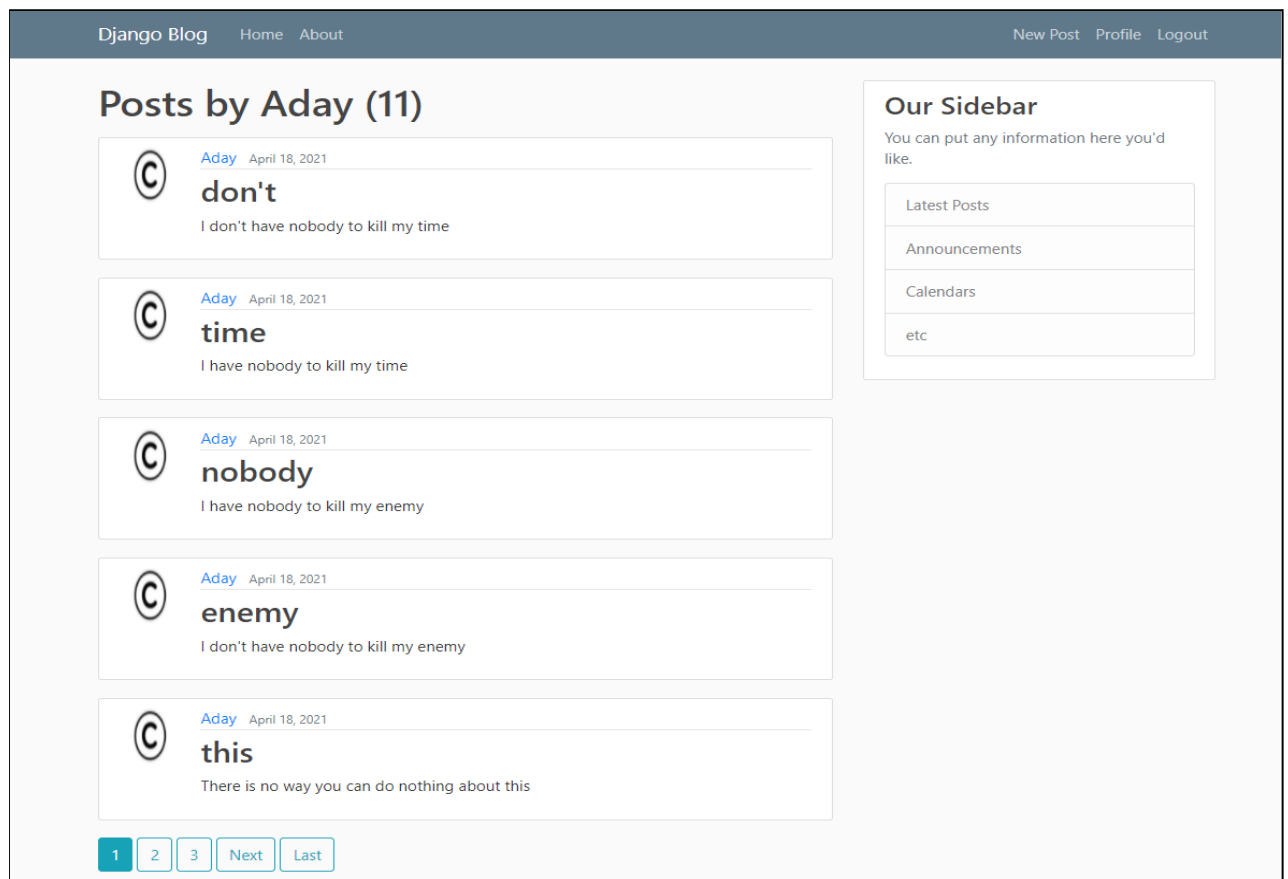


Fig 7.1.5 Details Page

7.1.6 Admin Page

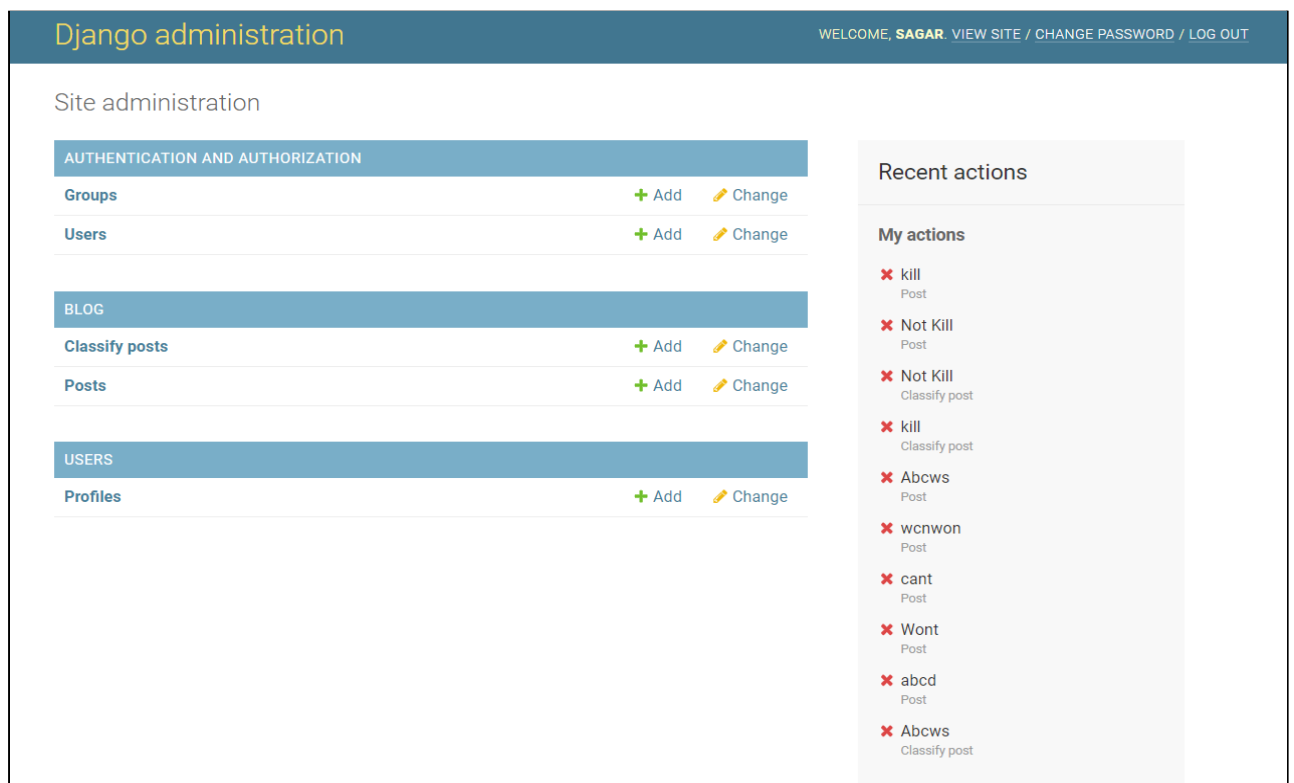


Fig 7.1.6 Admin Page

7.1.7 Post Details Page

Django administration

WELCOME, SAGAR. [VIEW SITE](#) / [CHANGE PASSWORD](#) / [LOG OUT](#)

[Home](#) > [Blog](#) > [Classify posts](#) > don't

Change classify post

HISTORY

User:

Aday

User id no:

13

User name:

Aday

User email:

aday@gmail.com

Title:

don't

Content:

I don't have nobody to kill my time

Toxic:

39.49%

Severe toxic:

47.52%

Obscene:

50.73%

Insult:

24.23%

Threat:

18.44%

Identity hate:

31.74%

Fig 7.1.7(a) Post Details Page

Date posted:

Date:

2021-04-18

Today

Time:

15:02:23

Now

Note: You are 5.5 hours ahead of server time.

Timezone:

Asia/Kolkata

Continent code:

AS

Country code:

IN

Country:

India

Region:

Maharashtra

City:

Ulhasnagar

Organization:

AS134913 JETWAY BROADBAND INDIA PVT LTD

Organization name:

JETWAY BROADBAND INDIA PVT LTD

Fig 7.1.7(b) Post Details Page

7.1.8 Fake Account

```
[41] df.head(3)
```

	user	listed_count	followers_count	favorite_count	statuses_count	friends_count
0	TDataScience	1281	75385	60	20993	1722
1	sidhuwrites	113	78729	44	59410	2214
2	NVIDIAHPCDev	1107	52163	72	7408	734

```
[19] # RANDOM FOREST

rf_classifier = RandomForestClassifier(n_estimators=100, max_depth=2, random_state=0)
rf_classifier.fit(X_train, y_train)
train_predictions = rf_classifier.predict(X_train)
prediction = rf_classifier.predict(X_test)

[42] j=rf_classifier.predict([[20993,75385,1722,60,1281,2,0]])
#statuses_count', 'followers_count', 'friends_count', 'favourites_count', 'listed_count', 'sex_code', 'lang

print(j)

[0]
```

Fig 7.1.8 Fake Account Page

7.2. Performance Evaluation measures

7.2.1 Analysis

The F1 Score is the $2 \cdot ((\text{precision} \cdot \text{recall}) / (\text{precision} + \text{recall}))$. It is also called the F Score or the F Measure. The F1 score conveys the balance between the precision and the recall so we had compared the F1 Scores of the Algorithms used.

$$F_1 = 2 \cdot \frac{\text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} = \frac{TP}{TP + \frac{1}{2}(FP + FN)}$$

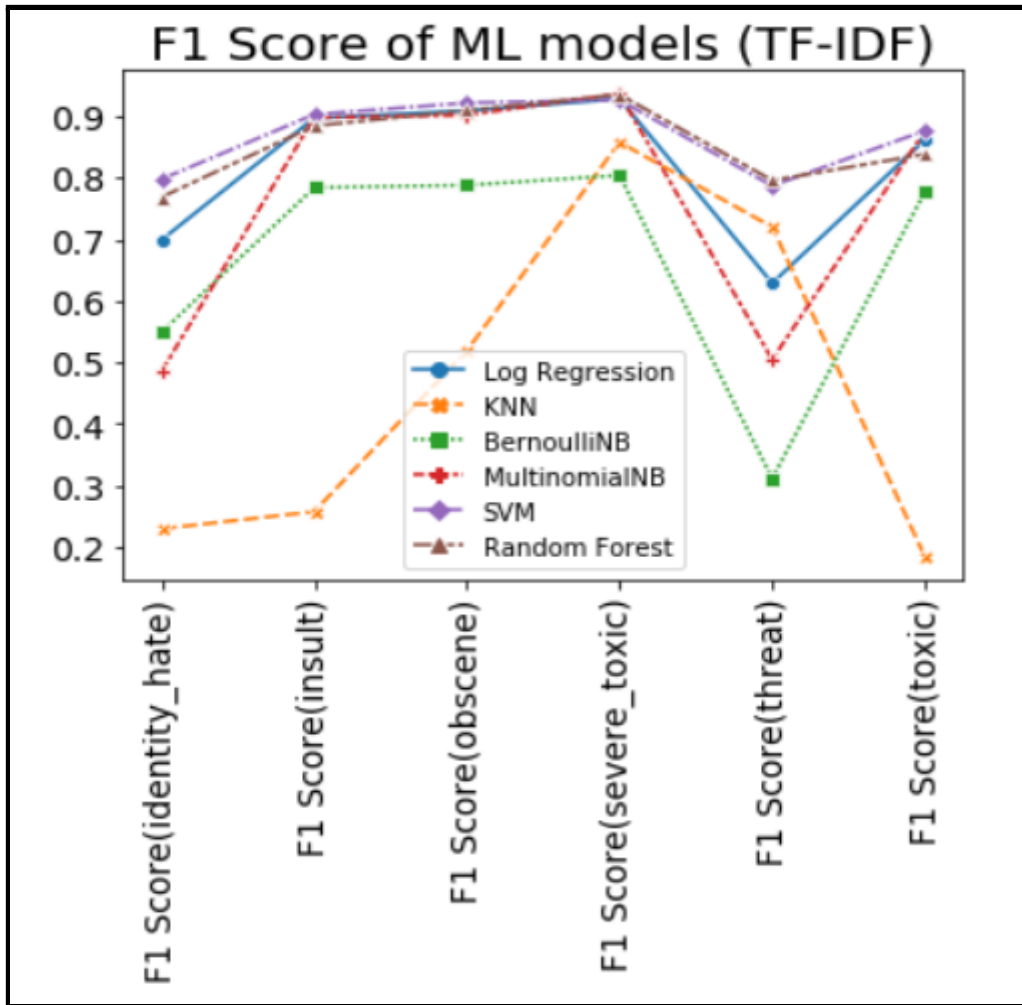


Fig 7.2.1 Comparison of F1 Score of the different Algorithm in graph form

7.2.2 Performance Overview of Algorithm Used

The Random Forest Algorithm is used to solve both regression and classification problems, making it a diverse model that is widely used by engineers.

When performing Random Forests based on classification data, you should know that you are often using the Gini index, or the formula used to decide how nodes on a decision tree branch

$$Gini = 1 - \sum_{i=1}^c (p_i)^2$$

This formula uses the class and probability to determine the Gini of each branch on a node, determining which of the branches is more likely to occur. Here, p_i represents the relative frequency of the class you are observing in the dataset and c represents the number of classes.

7.3. Input Parameters / Features considered

7.3.1 Cyberbullying Dataset

The Cyberbullying Dataset contains 7 parameters that is 1)comment_text 2)toxic 3)severe_toxic 4)obscene 5)threat 6)insult 7)identity_hate

- 1) comment_text - The following parameter contains the bad words or the bully words in each tuple and this column is processed using the Count Vectorizer Method which groups the similar words in to one so that if the similar kind of bully or bad words if used then can be recognized in the post
- 2) toxic - If the comment related to the cyberbully is toxic then the entry of the toxic parameter is set to '1' else it will have value '0'
- 3) severe_toxic - This parameter will contain the value as '1' i the commen_text to which it is related is severe_toxic else it will be by default '1'
- 4) obscene - Obscene parameter in this dataset with respect to its comment_text is set to '1' if it is an obscene or else '0'
- 5) threat - A warning that somebody may hurt, kill or punish you related to the text if found in comment_text then it is '1' or '0'
- 6) insult - This Parameter contain value as '1' if found text related to it is found to be insult else '0'
- 7) identity_hate - It is set to '1' if comment_text parameter to which it is related is found to be identity hate else it is set to '0'

	B	C	D	E	F	G	H
1	comment_text	toxic	severe_toxic	obscene	threat	insult	identity_hate
2	Explanation	0	0	0	0	0	0
3	D'aww! He matches	0	0	0	0	0	0
4	Hey man, I'm really	0	0	0	0	0	0
5	"	0	0	0	0	0	0
6	You, sir, are my hero	0	0	0	0	0	0
7	"	0	0	0	0	0	0
8	COCKSUCKER BEFORE	1	1	1	0	1	0
9	Your vandalism to the	0	0	0	0	0	0
10	Sorry if the word 'no	0	0	0	0	0	0
11	alignment on this su	0	0	0	0	0	0
12	"	0	0	0	0	0	0
13	bbq	0	0	0	0	0	0
14	Hey... what is it..	1	0	0	0	0	0
15	Before you start	0	0	0	0	0	0
16	Oh, and the girl abo	0	0	0	0	0	0
17	"	0	0	0	0	0	0
18	Bye!	1	0	0	0	0	0
19	REDIRECT Talk:Voyd	0	0	0	0	0	0
20	The Mitsurugi point	0	0	0	0	0	0
21	Don't mean to	0	0	0	0	0	0
22	"	0	0	0	0	0	0
23	"	0	0	0	0	0	0
24	"	0	0	0	0	0	0
25	"	0	0	0	0	0	0
26	"	0	0	0	0	0	0
27	Radial symmetry	0	0	0	0	0	0
28	There's no need to a	0	0	0	0	0	0
29	Yes, because the mo	0	0	0	0	0	0
30	"	0	0	0	0	0	0
31	"== A barnstar for	0	0	0	0	0	0
32	How could I post be	0	0	0	0	0	0
33	Not sure about a he	0	0	0	0	0	0
34	Praise	0	0	0	0	0	0
35	I was able to post	0	0	0	0	0	0
36	"	0	0	0	0	0	0
37	"	0	0	0	0	0	0
38	"	0	0	0	0	0	0
39	pretty much everyon	0	0	0	0	0	0
40	Hi Explicit, can you	0	0	0	0	0	0
41	Notability of	0	0	0	0	0	0
42	"	0	0	0	0	0	0
43	TFD	0	0	0	0	0	0
44	You are gay or	1	0	1	0	1	1
45	FUCK YOUR FILTHY N	1	0	1	0	1	0

Fig 7.3.1 Cyberbully Dataset

7.3.2 Fake Account Dataset

The Fake Account Detection dataset has the following parameters i.e

- 1) Name - It has names of the account holders.
- 2) Status Count - Total Status updated by users.
- 3) Followers Count - It shows the number of people the account holder follows.
- 4) Friends Count - It shows the total number of friends count of users.
- 5) Url - The user profile's URL
- 6) Time Zone - It is the time zone.
- 7) Listed Count - It counts how many websites the user visits.

- 8) Screen Name - It is the display name of the user on the website.
- 9) Profile Bio - It describes the profile of the user on different social media.
- 10) Location - it identifies the current location from where the user is operating.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
id	name	screen_n	statuses	followers	friends	c_favourite	listed	co_created	url	lang	time_zone	location	default_c	default_g	geo_enat	profile	ir_profile	b_profile	u_profile	b_profile	te_profile	ir_profile	si_profile	b_profile
3.7E+08	perfectmo	perfectmo	24	4	588	16	0	Thu Sep 08 13:20:35	en							http://a0.	https://tw	1	https://tw	333333	https://tw	FFFFFF		
37384589	SAK Nair	bsknair15	656	57	693	597	0	Sun May 03 07:35:13	en			Kuwait		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
72110028	Deepak	dedjyen	1234	15	104	1150	0	Sun Sep 06 19:50:08	en			Internatio	India			1	http://a0.	NULL	1	https://si	333333	https://si	EEEEEE	1
82885728	Marcos Vi	BrowAlve	573	14	227	530	0	Fri Oct 16 14:02:48	+en			Rio de Janeiro				http://a0.	NULL	1	https://si	1F1D1F	https://si	CODEED		
1.1E+08	Shri Kant	kanaujias	675	18	519	653	0	Sun Jan 31 12:08:41	en			New Delh	lucknow	1	1	http://a0.	NULL	1	https://si	333333	https://si	CODEED		
1.34E+08	Shree vis	shreeswa	1333	73	1998	1262	1	Sun Apr 18 12:04:04	en			Chennai				1	http://a0.	NULL	1	https://tw	333333	https://tw	EEEEEE	1
1.96E+08	crystiane	crystiane	99	26	1548	80	0	Mon Sep 27 21:53:12	es			Hawaii		1	1	http://a0.	NULL	1	https://si	333333	https://si	CODEED		
2.53E+08	shashank	creativab	553	63	1930	497	0	Tue Feb 15 16:34:46	en			Hawaii	Pune	1	1	http://a0.	NULL	1	https://si	333333	https://si	CODEED		
2.9E+08	santosh r	santoshn	1576	8	501	1402	1	Sat Apr 30 11:24:34	en			Ranai				http://a0.	NULL	1	https://si	0C3E53	https://si	F2E195		
3.04E+08	DATTARAI	DATTARAI	1378	48	1998	1108	0	Mon May 23 17:15:11	en			Chennai		1		http://a0.	https://si	1	https://si	333333	https://si	CODEED		
3.49E+08	suraj jad	surajjadh	1444	35	390	1283	0	Sat Aug 06 01:23:19	en			amravati	maharatra	india		http://a0.	NULL	1	https://si	333333	https://si	CODEED	1	
4.76E+08	Nirmal	smartnrm	1351	7	328	1273	1	Fri Jan 27 11:24:28	+en					1	1	http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Rochell C	rochellca	43	17	641	0	0	Sat Jun 23 15:30:29	+en			DIADEMA		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Thomase	thomase	50	20	630	0	0	Sat Jun 23 15:31:34	+en			In your hc		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Arnetta W	whitfield	68	22	602	0	0	Sat Jun 23 15:31:45	+en			Arizona		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Tonia Jac	toniajaco	60	14	592	0	0	Sat Jun 23 15:32:21	+en			ØÑ#Ø,Ø%		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Kasandra	kasandra	52	27	620	0	0	Sat Jun 23 15:32:47	+en			Rio Granc		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Stefania	searsfo	67	32	639	0	0	Sat Jun 23 15:32:53	+en			queens r		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Shamika	shamikag	44	21	614	0	0	Sat Jun 23 15:32:47	+en			pontiana		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Esperanz	maxwellll	66	23	650	0	0	Sat Jun 23 15:32:52	+en			malaysia		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Janina Ca	janinahzr	56	20	643	0	0	Sat Jun 23 15:33:05	+en			WORLDW		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Myrtle Bo	bowmanf	65	23	641	0	0	Sat Jun 23 15:33:06	+en			Fairburn,		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Genevieve	genevieve	79	20	779	0	0	Sat Jun 23 15:33:12	+en			Arizona		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Awilda Fc	awildagm	59	16	622	0	0	Sat Jun 23 15:32:59	+en			bangalori		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Margarite	roblesxyfi	64	15	649	0	0	Sat Jun 23 15:33:15	+en			Canada		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Delilla Ke	delillanbl	81	29	756	0	0	Sat Jun 23 15:33:22	+en			Liverpool		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Iris Wigg	wigginsstf	62	25	600	0	0	Sat Jun 23 15:33:05	+en			Where Th		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Izola Tili	izolaywvr	70	22	621	0	0	Sat Jun 23 15:33:16	+en			Accra- Gh		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		
6.16E+08	Brian Dili	brianen	52	19	735	0	0	Sat Jun 23 15:33:32	+en			Victoria i		1		http://a0.	NULL	1	https://si	333333	https://si	CODEED		

Fig 7.3.2 Fake Account Dataset

7.4. Graphical and statistical output

7.4.1 Exploratory Data Analysis of comments based on different categories

The below graph shows the comparison of the different categories of text or comment and their total values found in the dataset as compared to others.

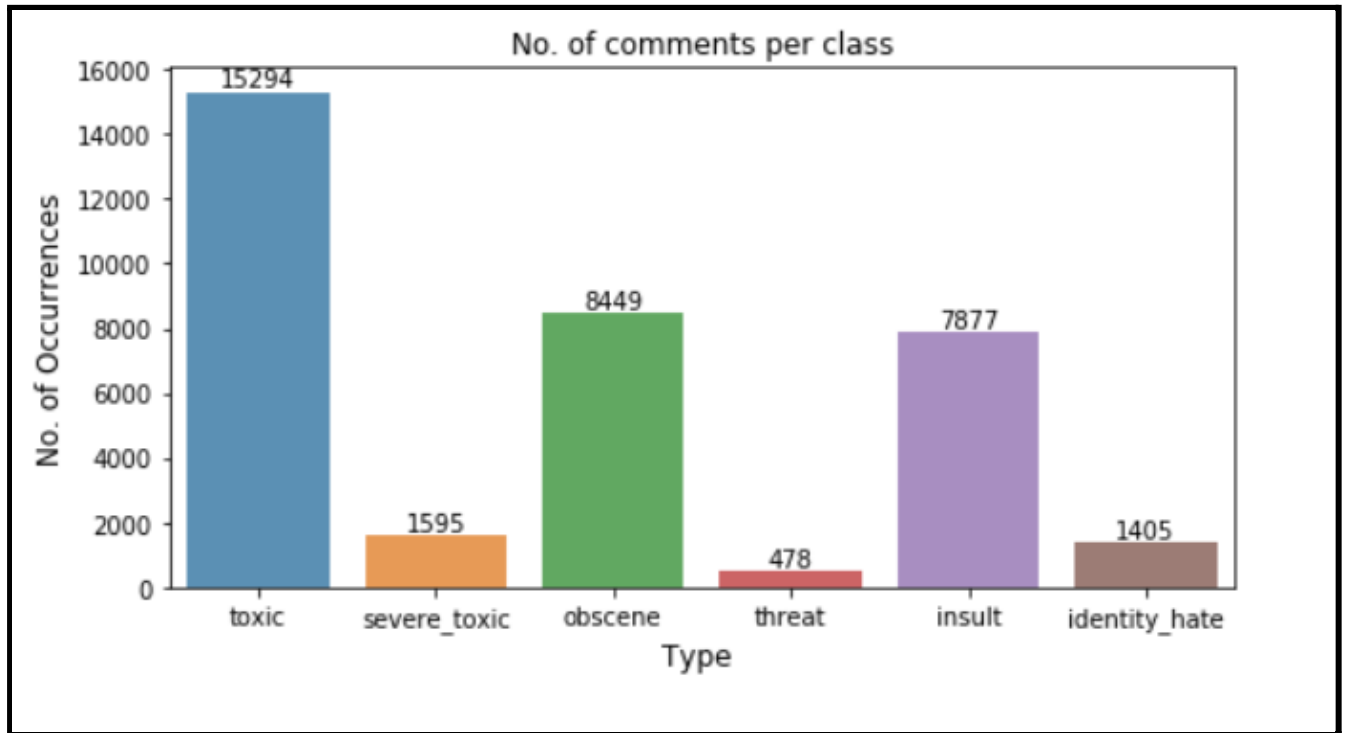


Fig 7.4.1 Exploratory Data Analysis of comments based on different categories

7.4.2 Exploratory Data Analysis of comments based on different categories

As shown below after applying the ML algorithms based on each category we had first compared the accuracies i.e F1 Score of the different algorithms and concluded that the Random Forest algorithm will give the best of all.

	Log Regression	KNN	BernoulliNB	MultinomialNB	SVM	Random Forest
F1 Score(toxic)	0.861234	0.185120	0.776521	0.874958	0.876133	0.838055
F1 Score(severe_toxic)	0.927879	0.857416	0.803707	0.936170	0.926004	0.934874
F1 Score(obscene)	0.908655	0.519056	0.787830	0.901463	0.921378	0.909091
F1 Score(insult)	0.896599	0.257992	0.783762	0.897411	0.902619	0.883993
F1 Score(threat)	0.628821	0.720000	0.311828	0.504762	0.786765	0.795539
F1 Score(identity_hate)	0.699029	0.230159	0.549206	0.485857	0.797516	0.768448

Fig 7.4.2 Comparison of F1 Score of the different Algorithms

7.4.3 Accuracy Comparison for Fake Account

In below diagram we had compare the accuracy of Decision Tree algorithm, Kernel SVM , Random Forest algorithm and as shown the Random Forest algorithm had given the best Accuracy

1 .Decision Tree
0.9852289512555391
2. Kernel SVM
0.9940915805022157
3. Random Forest
0.9955686853766618

Fig 7.4.3 Accuracy Comparison For Fake Account

7.5. Comparison of results with existing systems

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.

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] 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.

7.6. Inference drawn

Increase of Cyber Crime and Bullying at Social Networking Sites have increased nowadays so there is a Need for Detection and categorization of cyberbully and Removal of Fake Accounts so we had developed a website where we provide a Secure Environment for Users of any Age so that they can post any blog or comment they want but if that comment or text or post is found bully then we had applied the Machine Learning to remove the Cyber Crime and Bullying by first categorizing them and showing them to the Admin which can login to the admin panel and can review it and hence we had achieved Secure System Entry also Operations Layout which will be well Maintained. For the Fake account detection we had first trained our dataset and then we fetched the live data from twitter where we had tested whether the account is fake or not.

CHAPTER – 8

CONCLUSION

8.1 Limitations

- Intel Pentium Processor
- RAM \geq 4GB
- Anaconda
- Visual Studio
- Windows 10 SDK
- Continuous network connectivity required
- Process or requirement varies according to the Dataset

8.2 Conclusion

In this project, we proposed an approach to detect cyberbullying using machine learning techniques. We have evaluated our model on Different ML Algorithms and we have also used Countvectorizer for features extraction By using machine learning algorithms to its full extent. We have evaluated our model on First Cyberbully by comparing accuracies of the different algorithms we can conclude that Random Forest gives us the best accuracy and from the model results evaluated on the Fake Account we found that the best accurate algorithm is Decision Tree having the accuracy of By using machine learning algorithms to its full extent, we have eliminated the need for manual prediction of a fake account, which needs a lot of human resources and is also a time-consuming process.

8.3 Future Scope

- To reduce the toxicity classification on the Double negative sentence (For e.g “I don't have nobody to kill my time”)
- If a post contains a normal text and a web page link ,our system will identify the web link as the simple text and will calculate the percentage of all the categories.we can use a web crawling method to scrap the text from the web page and calculate the percentage of all the categories.
- 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.

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

CHAPTER – 9

REFERENCES

References (papers + books + Patent)

- [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. View at: [Google Scholar](#).
- [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. View at: [Publisher Site](#) | [Google Scholar](#).
- [4] R. Kohavi, “A study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection,” in *Proceedings of the 14th international joint conference on Artificial intelligence*, pp. 20–25, 1995. View at: [Google Scholar](#).
- [5] J. W. Patchin and S. Hinduja, “Bullies Move Beyond the Schoolyard; a Preliminary Look at Cyberbullying,” *Youth Violence and Juvenile*.
- [6] N. E. Willard, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*.
- [7] J. C. Platt, “Fast Training of Support Vector Machines using Sequential Minimal Optimization.

CHAPTER – 10

APPENDIX

10 Appendix

1. Paper I Details

a. Paper published



Fig 10.1.1(a) IEEE Paper

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 i.e., 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.

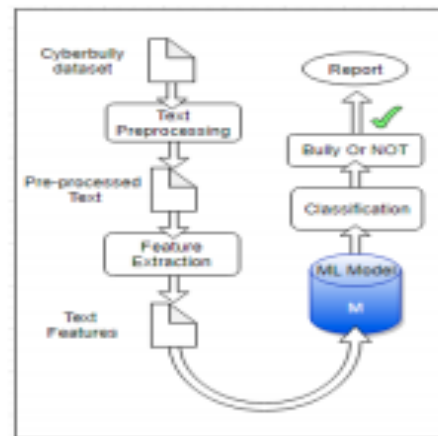


Fig 4.1 - Block diagram For Cyber Bullying

- 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.

Fig 10.1.1(b) IEEE Paper

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.

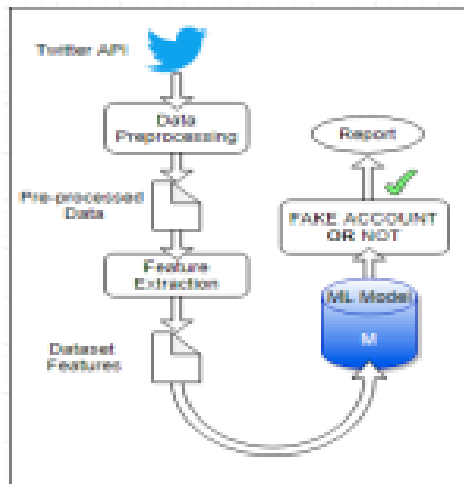


Fig 4.2 - Block diagram For Fake Account

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, 2004.
- [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.

b. Certificate of publication



Fig 10.1.2(a) ICAST Conference Certificate



Fig 10.1.2(b) ICAST Conference Certificate



Fig 10.1.2(c) ICAST Conference Certificate

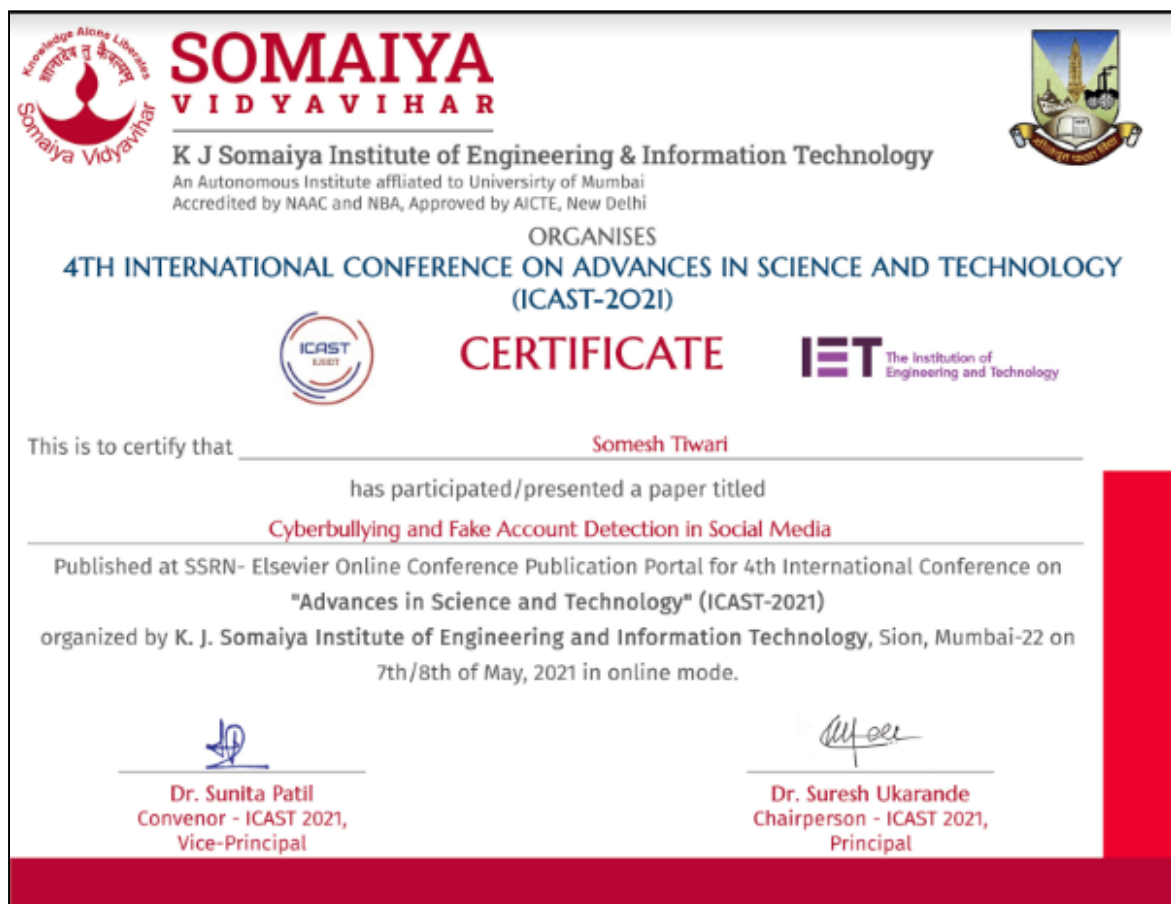


Fig 10.1.2(d) ICAST Conference Certificate



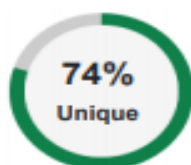
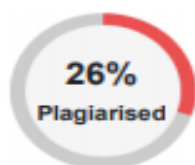
Fig 10.1.2(e) ICAST Conference Certificate

c. Plagiarism report



Fig 10.1.3(a) Plagiarism Report

PLAGIARISM SCAN REPORT



Excluded Url : None

Content Checked For Plagiarism

. 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. 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. I. Jolliffe, Principal Component Analysis, 2002.View at: MathSciNet. S. Sperandei, "Understanding logistic regression analysis," *Biochemia Medica*, vol. 24, no. 1, pp. 12–18, 2014. 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. N. E. Willard, "Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress", Research Press, 2007. 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] 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 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. I. Jolliffe, Principal Component Analysis, 2002.View at: MathSciNet. S. Sperandei, "Understanding logistic regression analysis," *Biochemia Medica*, vol. 24, no. 1, pp. 12–18, 2014. 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. N. E. Willard, "Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress", Research Press, 2007.

11% Plagiarized

Fig 10.1.3(b) Plagiarism Report

d. Project review sheet

Inhouse/ Industry: Group No.:													Class: D17 A/B/C Group No.:48		
Project Evaluation Sheet 2020 - 21															
Title of Project: Cyberbullying and fake profile detection in Social Media															
Group Members: Jayesh Samtani (57) D17A, Sagar Sidhwa (62) D17A, Somesh Tiwari (71) D17A, Riva Wadhwani(74) D17A															
Engineering Concepts & Knowledge	Interpretation of Problem & Analysis	Design / Prototype	Interpretation of Data & Dataset	Modern Tool Usage	Societal Benefit, Safety Consideration	Environment Friendly	Ethics	Team work	Presentation Skills	Applied Engg & Mgmt principles	Life - long learning	Professional Skills	Innovative Approach	Research Paper	Total Marks
(5)	(5)	(5)	(3)	(5)	(2)	(2)	(2)	(2)	(2)	(3)	(3)	(3)	(3)	(5)	(50)
4	4	4	2	3	2	2	2	2	2	2	3	2	2	4	40

Lifna C S (Reviewer1)

Engineering Concepts & Knowledge	Interpretation of Problem & Analysis	Design / Prototype	Interpretation of Data & Dataset	Modern Tool Usage	Societal Benefit, Safety Consideration	Environment Friendly	Ethics	Team work	Presentation Skills	Applied Engg & Mgmt principles	Life - long learning	Professional Skills	Innovative Approach	Research Paper	Total Marks
(5)	(5)	(5)	(3)	(5)	(2)	(2)	(2)	(2)	(2)	(3)	(3)	(3)	(3)	(5)	(50)
3	3	3	2	3	2	2	2	2	2	2	2	2	1	3	34

Date: **2nd March, 2021** **Richard Joseph** (Reviewer2)

- **Twitter API**
- **LSTM not implemented**
- **Fake Account Detection Remaining**
- **Revise the paper to incorporate the integration of these modules**

Fig 10.1.4(a) Project Review Sheet-1

Inhouse/ Industry: Group No.:													Class: D17 A/B/C Group No.: 48		
Project Evaluation Sheet 2020 - 21															
Title of Project: Cyberbullying and fake account detection in social media															
Group Members: Jayesh Samtani D17A-57, Sagar Sidhwa D17A-62, Somesh Tiwari D17A-71, Riya Wadhwani D17A-74															
Engineering Concepts & Knowledge	Interpretation of Problem & Analysis	Design / Prototype	Interpretation of Data & Dataset	Modern Tool Usage	Societal Benefit, Safety Consideration	Environment Friendly	Ethics	Team work	Presentation Skills	Applied Engg & Mgmt principles	Life - long learning	Professional Skills	Innovative Approach	Research Paper	Total Marks
(5)	(5)	(5)	(3)	(5)	(2)	(2)	(2)	(2)	(2)	(3)	(3)	(3)	(3)	(5)	(50)
4	4	5	3	4	2	2	2	2	2	3	3	2	2	4	44

Lifna C S (Reviewer-1)

Engineering Concepts & Knowledge	Interpretation of Problem & Analysis	Design / Prototype	Interpretation of Data & Dataset	Modern Tool Usage	Societal Benefit, Safety Consideration	Environment Friendly	Ethics	Team work	Presentation Skills	Applied Engg & Mgmt principles	Life - long learning	Professional Skills	Innovative Approach	Research Paper	Total Marks
(5)	(5)	(5)	(3)	(5)	(2)	(2)	(2)	(2)	(2)	(3)	(3)	(3)	(3)	(5)	(50)
4	4	4	3	4	2	2	2	2	2	3	3	2	2	3	42

Date: **26th April, 2021** **Richard Joseph** (Reviewer-2)

Comments :

1. Consider writing the second paper with Tweets as the input for classification.
2. Include a separate class if the tweet / text belongs to any of the 6 classes discussed in the Review.
3. Also, can try exploring the tinyURLs which are present in the tweets as an Extension of the project while considering for the second paper.

Fig 10.1.4(b) Project Review Sheet-2

2. Video Presentation Link

<https://drive.google.com/drive/folders/1aKjvB451-9hCupwt-0LNYT5CceBgy2s2?usp=sharing>