Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

DETECTION OF CHILD PREDATORS CYBER HARASSERS ON SOCIAL MEDIA

Tata Rao Vana, Assistant Professor, Department of CSE**,** Raghu Engineering College**,** Dakamarri, Andhrapradesh Email: - vanatatarao@gmail.com
A. Aditya Tarun, B Tech Student, Department of CSC, Raghu Institute of Technology, Dakamarri, Andhrapradesh Email: - Adityatarun999@gmail.com
K. Sai Sravanthi, B Tech Student, Department of CSC, Raghu Institute of Technology, Dakamarri, Andhrapradesh Email**: -** Saisravanthikannuru@gmail.com
J. Jagannadha Sandeep, B Tech Student, Department of CSC**,** Raghu Institute of Technology, Dakamarri, Andhrapradesh Email**: -** jayanthijagannadhasandeep@gmail.com
S. Vashist, B Tech Student, Department of CSC, Raghu Institute of Technology, Dakamarri, Andhrapradesh Email**: -** 213j5a4606@raghuinstech.com

ABSTRACT

Professional psychologists need to be knowledgeable about how to safeguard children from sex predators and the risks associated with internet sex abuse. Although the internet has many positive aspects as well, one of its most negative characteristics is the possibility of sexual postulation. Online, sexual predators have easy access to many children while going mostly unrecognized. The major goal of our project is to identify child predators through comments and postings on social media so that the administrator of the cyber jail is aware of the predator's past. According to a recent national poll, one in five young adults engage in annual online sex activities (finkelhor, mitchell, & wolak, 2000; Mitchell, finkelhor, & wolak, 2001). This project report details the most current changes we made to the system to make it function. Any accounts discovered to be child predators will be reported to the admin for further action in accordance with the established policy

1. INTRODUCTION

Child predator detection system on social media is a web Based application this project aims to detect child predator comments and post on social media like fb, insta etc and send report to cyber cell admin. To develop an well-designed database to store all comments and post of social online contact of children in pedophiles is a rapidly growing problem on social media. As of march 2014, the national society for the hindrance of cruelty to kids (NSPCC), reported that i) 12-tone system of 11 –16year olds within the kingdom have received unwanted sexual messages; and ii) 8% of 11-16year olds in the UK have received requests to

send or respond to a sexual message. The detection of kids cyber sexual-offenders is so a crucial issue that must be addressed. Kids in their teens have

Beg an to use social media as their main means that of communication. Moreover, a recent study of cognition, adolescents and mobile phones (scamp) has revealed that 70% of 11-12year olds in the UK now own a mobile phone rising to 90% by age 14. A common attack of pedophiles is the so-called online child grooming, where adults eventually exchange sexually explicit content through social media outlets. Such grooming consists of building a trust-relationship with a minor, which finally leads into convincing a child to meet them in person. Previous research on detecting cyber pedophilia online, including the efforts of the first international sexual predator identification competition.

2. LITERATURE SURVEY AND RELATED WORK

2.1 Introduction to literature Survey:

Cyber grooming may be a compelling drawback worldwide today and plenty of reports powerfully instructed that it becomes terribly imperative to tackle this drawback to safeguard the kids from sexual exploitation. during this study, we have a tendency to propose a good technique for sexual predator identification in on-line chats supported two-stage classification. the aim of the primary stage is to tell apart predatory languages from the traditional ones whereas the second stage aims to inform apart between the predator user and therefore the victim at intervals one predatory conversation. Finally, some distinctive predators square measure derived from the second stage result. we have a tendency to investigate many machine learning classifiers as well as Naive Bayes, Support Vector Machine, Neural Network, provision Regression, Random Forest, K-Nearest Neighbours, and call Tree with Bag of Words options victimization many totally different term weight strategies for this task. we have a tendency to additionally projected 2 ensemble techniques to enhance the classification task. The experiment results on PAN12 dataset show that our greatest technique victimization soft vote primarily based} ensemble for initial stage And Naive Bayes based technique for the second stage obtained an F zero.5 -score of zero.9348, which might place as favourite within the PAN12 competition ranking

2.2 Literature Survey:

Michael Ashcroft; Lisa Kaati; Maxime Meyer "A Step Towards sleuthing on-line Grooming -- characteristic Adults simulation to be Children" They enforced machine-controlled analysis of chat area language to discover and attainable tries of grooming nline grooming may be a major drawback in today’s society wherever additional and longer is spent on-line. To become friends and establish a relationship with their young victims in on-line communities, groomers typically faux to be kids. during this paper, we have a tendency to describe AN approach that may be wont to discover if AN adult is simulation to be a baby during a chat area language. The approach involves a 2-step method whereby authors square measure initial classified as being kids or adults, so every kid is being examined and false kids distinguished from real kids. Our results show that notwithstanding it's arduous to separate standard adults from kids in chat logs it's attainable to tell apart real kids from adult’s simulation to be kids with a high accuracy. during this paper, we are going to discuss the accuracy of the strategies projected, additionally because the options that were vital in their success. we have a tendency to believe that this work is a vital step towards machine-controlled analysis of chat area language to discover and attainable tries of grooming. Our approach wherever we have a tendency to use text analysis to tell apart adults World Health Organization square measure simulation to be kids from actual kids may be wont to inform kids regarding verity age of the person who they're 14 human activity. this might be a step towards creating the web safer for young kids and eliminate grooming. Patrick Bours, Halvor Kulsrud Detection of Cyber Grooming in on-line Conversation They enforced system to discover on-line cyber grooming. during this paper, we are going to specialise in the detection of sexual predators in on-line chat conversations. we have a tendency to use three totally different approaches (message-based, author-based and conversation-based) combined with five {different| totally totally different| completely different} classification algorithms and a pair of different options sets. the simplest results were obtained victimization either the author-based approach with the Neural Network classifier on the TF-IDF feature set, or the conversation-based approach victimization the Ridge or the Naïve Bayes classifier on the TF-IDF feature set. during this paper, for the primary time, we have a tendency to checked out however fast a predator may be detected, and located that in most cases 26-161 messages of a language were comfortable. This constitutes solely alittle fraction of the complete conversations, showing that we will have AN early detection system of sexual predators rather than knowing looking back that a baby was the victim of a sexual predator. Stefan C. Dombrowski, John W. Le Masney, and Claude Elwood Shannon A. Dickson they study regarding skilled psychologist’s ought to additional absolutely perceive the risks of on-line sexual solicitation and ways that during which to safeguard youth from sexual predators World Health Organization use the web. though the web has several positive aspects, one in every of the foremost pernicious aspects is its potential use for on-line sexual predation. the web represents a medium that permits sexual predators access to innumerable kids during a comparatively anonymous setting. this text reviews the overall ways of sexual perpetrators and their characteristics, additionally because the on-line ways and characteristics of the cyber sexual predator. data on a way to shield kids from this crime through a review of technological, psych instructional, and legal issues is provided. an outline of the relevant laws as they relate to on-line solicitation and active psychologists is additionally provided Hee-Eun Lee Tatiana Ermakova Vasilis Ververis Benjamin Fabian This gift analysis provides a comprehensive synthesis and an interpretation of the present analysis accomplishments and challenges within the CSAM detection domain, expressly considering the size of policy and legal framework, distribution channels, and detection applications and implementations. Among alternative aspects, it reveals and aggregates data associated with image hash info, keywords, web-crawler, detection supported filenames and information, and visual detection. The findings recommend that CSAM detection applications yield the simplest results if multiple approaches square measure utilized in combination, such as deep-learning algorithms with multi-modal image or video descriptors incorporate along. Deep-learning techniques were shown to surpass alternative detection strategies for unknown CSAM. 15 Muhammad Ali Fauzi Apostle Bours during this study, we have a tendency to propose a good technique for sexual predator identification in on-line chats supported two-stage classification. the aim of the primary stage is to tell apart predatory languages from the traditional ones whereas the second stage aims to inform apart between the predator user and therefore the victim at intervals one predatory conversation. Finally, some distinctive predators square measure derived from the second stage result. we have a tendency to investigate many machine learning classifiers as well as Naive Bayes, Support Vector Machine, Neural Network, provision Regression, Random Forest, K-Nearest Neighbours, and call Tree with Bag of Words options

3. Implementation Study

In this project we are using various machine learning algorithms such as SVM, Random Forest, Naïve Bayes, K Nearest Neighbours, and Decision Tree to predict child harasser’s posts from social networks. Using all algorithms we will build train model with normal and harasser’s word and messages and this train model will applied on new posts from users to predict whether new post is normal or contain harasser’s stuff

3.1 Existing Methods

There exists various child predator detection system which are used in gaming, audio chat and in various online entertainment platform. While playing games or for using online audio chat there exists a child predator system which detects an online sexual harassment and prevent child from getting abused or getting harassed by sexual predator as this existing system is only used when the children are playing games on internet or doing any audio chats. As now we are in internet era various children are now days using social media platform for various social activities. They are mostly active on social media so to prevent child harassment we need a child predator detection system for social media. In existing system use 5 classification algorithm Neural Network classifier on the TF-IDF feature set, or the conversation-based approach using the Ridge or the Naıve Bayes classifier on the TFIDF feature set. In our system, we will implement only one algorithm for image and text classification. We will give more accuracy as compare to existing system because of The Support Vector Machine (SVM) is a supervised machine learning model that uses classification algorithms for two-group classification problems

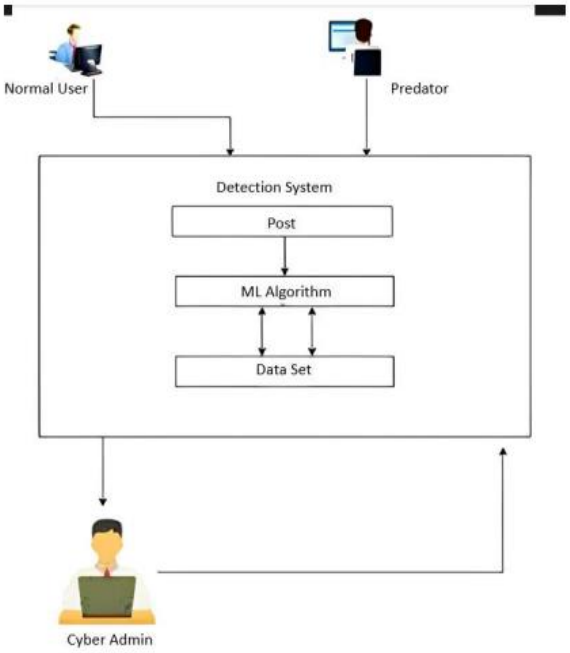


Fig 1: -SYSTEM ARCHITECTURE for proposed Method

4 METHODOLOGIES & ALOGRITHAM

This chapter explains the design and implementation phases of the system. It depicts the class diagram, ER diagram and database schema the System. Moreover, the implementation phase combines the requirements, design phase outputs, and process them using the appropriate technologies.

Modules:

User module:

The User Component of the platform permits individuals to establish a profile by registering, whereby they gain access to the application upon successful login. Upon entering the system, users are equipped to send and inspect posts.

Technology Description:

- URL routing
- HTML, XML, JSON, and other output format tinplating
- Manipulation of database
- Security against Cross-site request forgery (CSRF) and other attacks
- Storage and retrieval of session

Web frameworks differ in their inclusion of functionality, ranging from specialized frameworks that focus on a specific use case to comprehensive frameworks that encompass all known web framework features for all developers. Some frameworks follow a "batteries-included" approach, bundling all possible functionality with the framework, while others provide a minimal core package that can be extended with additional packages. There have been several updates in the Python version over the years. The question is how to install Python? It might be confusing for the beginner who is willing to start learning Python but this tutorial will solve your query. The latest or the newest version of Python is version 3.7.4 or in other words, it is Python 3.

4.1 Navie Bayes Alogritham

step-by-step explanation of the Naive Bayes algorithm:

1. Understanding the Problem: Naive Bayes is a supervised machine learning algorithm used for classification tasks. It's based on Bayes' theorem, which calculates the probability of a hypothesis given the data.

2. Collecting Data: Gather a dataset that contains features (attributes) and their corresponding labels (classifications).

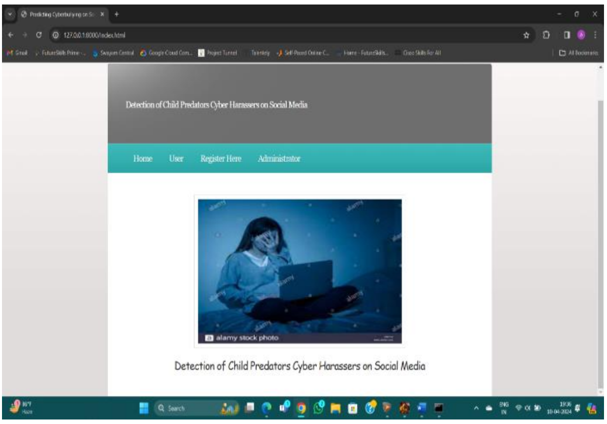
3. Preprocessing Data: Before using the data, it's essential to preprocess it. This includes handling missing values, encoding categorical variables, and scaling numerical features if necessary.
4. Splitting Data: Divide the dataset into two parts: training data and testing data. The training data will be used to train the model, while the testing data will be used to evaluate its performance.
5. Calculating Class Probabilities: For each class label, calculate the prior probability, which is the probability of each class occurring without considering any features. This is calculated by dividing the number of instances of each class by the total number of instances.
6. Calculating Feature Probabilities: For each feature given the class label, calculate the conditional probability using the training data. This involves calculating the likelihood of each feature value occurring for each class.
7. Making Predictions: Given a new instance with feature values, use Bayes' theorem to calculate the probability of each class label given the features. The class label with the highest probability is then assigned to the instance.
8. Model Evaluation: After making predictions on the testing data, evaluate the performance of the model using metrics such as accuracy, precision, recall, or F1-score.
9. Iterating and Tuning: Depending on the performance of the model, you may need to iterate by adjusting hyperparameters or preprocessing steps to improve its accuracy.
10. Deployment: Once satisfied with the model's performance, deploy it to make predictions on new, unseen data.

4.2 SVM ALOGRITHAM

step-by-step explanation of the Support Vector Machine (SVM) algorithm:
1. Understanding the Problem: SVM is a supervised machine learning algorithm used for classification and regression tasks. It works by finding the hyperplane that best separates the data into different classes.
2. Collecting Data: Gather a dataset that contains features (attributes) and their corresponding labels (classifications or target values).
3.Preprocessing Data: As with any machine learning algorithm, preprocessing steps may include handling missing values, encoding categorical variables, and scaling numerical features if necessary.
4. Splitting Data: Divide the dataset into two parts: training data and testing data. The training data will be used to train the SVM model, while the testing data will be used to evaluate its performance.
5. Choosing a Kernel Function: SVMs use kernel functions to map the input data into a higher-dimensional space where it's easier to find a separating hyperplane. Common kernel functions include linear, polynomial, and radial basis function (RBF) kernels. Choose an appropriate kernel function based on the problem at hand and the characteristics of the data.
6. Training the SVM Model: In this step, the SVM algorithm learns the parameters of the hyperplane that best separates the different classes in the training data. This involves solving an optimization problem to maximize the margin between the classes while minimizing classification errors.
7. Optimizing Hyperparameters: SVMs have hyperparameters that can significantly affect the performance of the model, such as the regularization parameter (C) and the kernel parameters (e.g., gamma for RBF kernel, degree for polynomial kernel). Use techniques like cross-validation to tune these hyperparameters and find the optimal values.
8. Making Predictions: Once the SVM model is trained, it can be used to make predictions on new, unseen data. Given a new instance with feature values, the model predicts the class label based on which side of the hyperplane the instance falls.
9. Model Evaluation: Evaluate the performance of the SVM model using the testing data. Common evaluation metrics for classification tasks include accuracy, precision, recall, F1-score, and ROC-AUC score.
10. Iterating and Tuning: Depending on the performance of the model, you may need to iterate by adjusting hyperparameters, trying different kernel functions, or exploring different preprocessing techniques to improve its accuracy.

11. Deployment: Once satisfied with the model's performance, deploy it to make predictions on new, unseen data in real-world applications.

5 RESULTS AND DISCUSSION SCREEN SHOTS

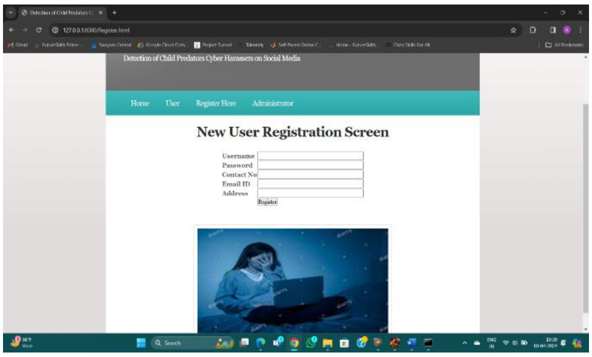


Detection of Child Predators Cyber Harassers on Social Media

Detection of Child Predators Cyber Harassers on Social Media

Figure- 2 Home page In above screen click on ‘Register Here’ link and add new user to create account

To proceed, locate and click on the "Register Here" link displayed on the screen. This action will redirect you to the registration page where you can create a new user account. Fill out the required information, including username, email address, and password, then submit the form to successfully register and create a new user account. Upon completion, you'll receive a confirmation message indicating that your account has been successfully created, allowing you to log in and access the application's features. upon clicking the "Register Here" link, you'll be directed to the registration page where you can input your details. Ensure to provide accurate information, including your desired username, valid email address, and a secure password. After filling out the required fields, proceed to submit the form to create your account. Once successfully registered, you'll receive a verification email or confirmation message, depending on the application's setup, your newly created credentials and begin exploring the application's features.



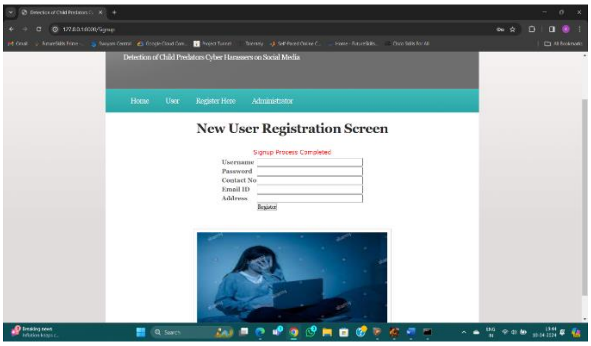
Detection of Child Predators Cyber Harassers on Social Media

New User Registration Screen

Username
Password
Contact No
Email ID
Address

Figure- 3 User Registration Screen In above screen now click on ‘Register’ button to add details

After selecting the "Register Here" link, you'll be redirected to the registration page. On this page, locate and click the "Register" button to proceed with adding your details. Fill in the necessary information, such as username, email address, and password, ensuring accuracy and compliance with any validation requirements. Once all required fields are completed, click the "Register" button again to submit your details and create your account. Upon successful registration, you'll receive a confirmation message confirming the creation of your account, allowing you to log in and access the application's features.



Detection of Child Predators Cyber Harassers on Social Media
Home
User
Register Here
Administrator
Register

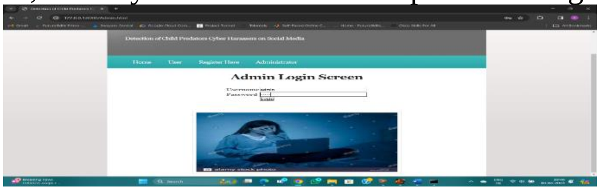
New User Registration Screen

Signup Process Completed

Username
Password
Contact No
Email ID
Address

Figure- 4 Registration Complete

Following the completion of the sign-up process, navigate to the "Administrator" link and click on it to access the admin dashboard. Once on the admin dashboard, locate the section or tab where user details are displayed. Here, you'll be able to view the newly registered user's information, including their username, email address, and any additional details captured during registration.



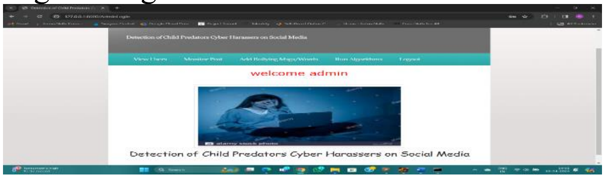
Detection of Child Predators Cyber Harassers on Social Media
Home
User
Register Here
Administrator
Login

Admin Login Screen

Username
Password

Figure- 5 Admin Login Page

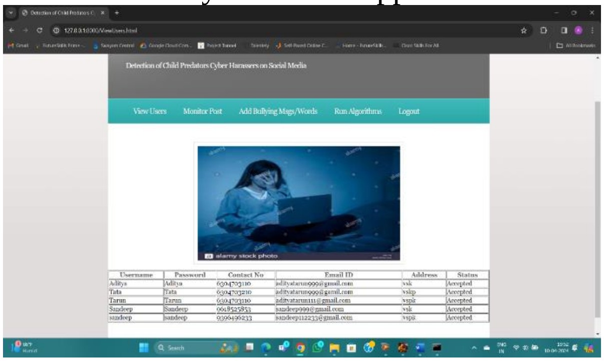
After providing the username "admin" and the password "admin" to log in, you will be directed to the admin dashboard. This dashboard typically provides an overview of various administrative functions and data related to the application. Here, you can access features such as user management, content moderation, system settings, and more. From this screen, you'll have the ability to view and manage user details, including newly registered user information, as well as perform other administrative tasks to maintain the application. In above screen login as 'admin' by giving username as 'admin' and password as 'admin'. After login will get below screen



welcome admin

Detection of Child Predators Cyber Harassers on Social Media

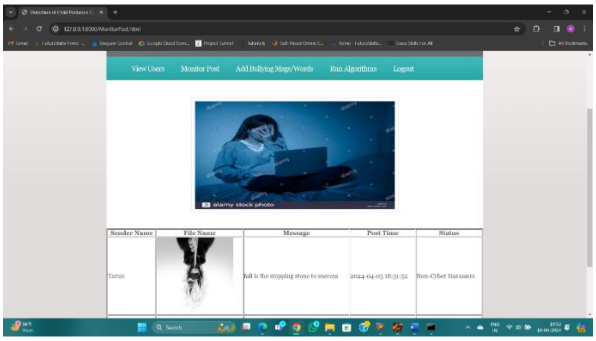
Figure- 6 Admin Home Page Now admin can click on 'View Users' link to view all users list Once logged in as an admin, click on the "View Users" link to access the list of all users registered in the system. This action will navigate you to a page displaying a comprehensive list of user profiles, including their usernames, email addresses, and any additional details captured during registration. From this page, admins can review, edit, or manage user accounts as needed, ensuring proper administration and oversight of user activity within the application.



Username	Password	Contact No	Email ID	Address	Status
Aditya	Aditya	6304703110	adityatarun999@gmail.com	vsk	Accepted
Tata	Tata	6304703210	adityatarun999@gamil.com	vskp	Accepted
Tarun	Tarun	6304703110	adityatarun111@gmail.com	vspk	Accepted
Sandeep	Sandeep	9618525853	sandeep999@gmail.com	vsk	Accepted
sandeep	sandeep	9396496233	sandeep112233@gmail.com	vspk	Accepted

Figure- 7 Users Details

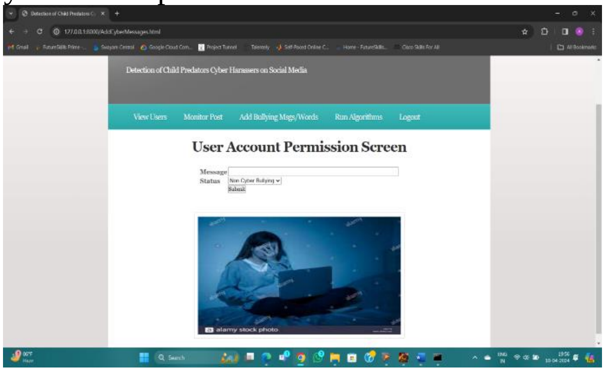
In the current screen, the account for 'Rajesh' has been successfully created. The admin can proceed to click on the 'Monitor Post' option to access and review all posts submitted by past users. This action allows for comprehensive monitoring of user-generated content within the platform.Upon the creation of the 'Rajesh' account, the admin gains the ability to monitor posts made by this user, ensuring adherence to community guidelines and policies. By accessing the 'Monitor Post' feature, the admin can review the content contributed by past users, thereby maintaining a safe and conducive environment within the platform.



Sender Name	File Name	Message	Post Time	Status
Tarun		fail is the stepping stone to success	2024-04-05 18:31:52	Non-Cyber Harassers

Figure- 8 Post Viewing

In the depicted screen, the application autonomously determines whether a message is from a non-cyber harasser or a harasser using machine learning algorithms. Admins can further enhance the system's capabilities by clicking on the 'Add Bullying Messages/words' link to include additional bullying messages or keywords for monitoring and detection accessing the 'Add Bullying Messages/words' link, admins can contribute to the system's ongoing improvement by supplementing its database with relevant bullying messages or keywords. This proactive approach empowers administrators to continually refine the platform's detection mechanisms



Detection of Child Predators Cyber Harassers on Social Media

User Account Permission Screen

Message
Status Non Cyber Bullying

Figure- 9 Words Adding Screen

After adding the word "Cyber Bullying" and other potential bullying and non-bullying messages, the admin will be directed to the subsequent screen, displaying the updated list of monitored keywords. Here, the admin can verify and manage the list of flagged terms to ensure comprehensive monitoring for potential instances of cyberbullying within the platform.Once the admin completes the addition of messages, the subsequent screen will showcase the updated list of monitored keywords

Figure- 10 After Adding Words

By clicking on the 'Run Algorithms' link, the admin initiates the process of generating a trained model using the entire dataset. This model will be utilized to predict whether user posts classify as normal or indicative of bullying/harassment behavior. This proactive measure empowers the platform to effectively identify and address potential instances of cyberbullying, ensuring a safer online community for all Here, the admin can verify and manage the list of flagged terms to ensure comprehensive monitoring for potential instances of cyberbullying

6 CONCLUSION AND FUTURE SCOPE

6.1 Conclusion: The cost to youngsters and society of sexual commission is simply too nice to overlook the hazards of on-line solicitation.

The aim of the groomer is to build a relationship with a child inorder to gain access to that child. When grooming takes place it is common that an adult groomer is pretending to be a child with common hobbies or interests to build a relationship that includes trust with the child. In this project, we detect predator of child for child safety. And send report to cyber admin for action.

6.2 Future Scope: The future scope of the project encompasses several key areas aimed at further enhancing the detection and prevention of online grooming, ultimately ensuring the safety of children in the digital realm. Firstly, there is a continual need to advance detection techniques, incorporating more sophisticated machine learning algorithms, natural language processing, and sentiment analysis to better identify predatory behavior online. Additionally, efforts should focus on implementing real-time monitoring capabilities to promptly detect and address suspicious interactions as they occur, leveraging streaming data processing technologies and proactive alerting mechanisms.

7 REFERENCES

[1] C. H. Ngejane, G. Mabuza-Hocquet, J. H. P. Eloff, and S. Lefophane, “Mitigating online sexual grooming cybercrime on social media using machine learning: A desktop survey,” in 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Aug 2018, pp. 1–6.

[2] N. Pendar, “Toward spotting the pedophile telling victim from predator in text chats,” in International Conference on Semantic Computing (ICSC 2007), Sep. 2007, pp. 235–241.

[3] I. McGhee, J. Bayzick, A. Kontostathis, L. Edwards, A. McBride, and E. Jakubowski, “Learning to identify internet sexual predation,” International Journal of Electronic Commerce, vol. 15, no. 3, pp. 103– 122, 2011.

[4] G. Inches and F. Crestani, “Overview of the international sexual predator identification competition at PAN-2012,” in CLEF 2012 Evaluation Labs and Workshop, Online Working Notes, Rome, Italy, September 17-20, 2012, 2012.

[5] E. Villatoro-Tello, A. Juarez-Gonz ´ alez, H. J. Escalante, M. Montes-y- ´ Gomez, and L. V. Pineda, “A two-step approach for effective detection ´ of misbehaving users in chats,” in CLEF 2012 Evaluation Labs and Workshop, Online Working Notes, Rome, Italy, September 17-20, 2012, 2012.

[6] G. Eriksson and J. Karlgren, “Features for modelling characteristics of conversations,” in CLEF 2012 Evaluation Labs and Workshop, Online Working Notes, Rome, Italy, September 17-20, 2012, 2012

[7] Muhammad Ali Fauzi, Patric Bours, “Ensemble Method for Sexual Predator Identification”. IEEE, 2020,25 June 2020

[8] Michael Ashcroft, Lisa Katti, Maxime Meyer “A Step Towards Detecting Online Grooming-Identifying Adults Pretending to be Children”. European Intelligence and Security Informatics Conference,2019

[9] Elif Varol Altay, Bilal Altas “Detection of Cyber Grooming in Online Conversation”. International Conference on Big Data Deep Learning and Fighting cyber–Terrorism Ankara, Turkey IEEE 03/12/2018