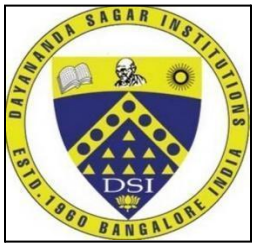

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

DAYANANDA SAGAR COLLEGE OF ENGINEERING

AN AUTONOMOUS INSTITUTE AFFILIATED TO VTU
APPROVED BY AICTE & UGC, ACCREDITED BY NAAC WITH 'A' GRADE, ACCREDITED BY NBA.

A Project Synopsis

on

"DETECTION OF CYBER CRIME ON SOCIAL MEDIA USING MACHINE LEARNING ALGORITHM"

Submitted as a part of the Final Year Project of

BACHELOR OF ENGINEERING

in

INFORMATION SCIENCE AND ENGINEERING

Submitted by

1DS19IS068	**POOJA M**
1DS19IS076	**RAKSHITHA K**
1DS19IS108	**SREENIKETH MADGULA**

Under the guidance of

Dr. MUZAMEEL AHMED
Associate Professor
Dept. Of ISE, DSCE

2022-2023

<table>
<tr><td>TITLE OF THE PROJECT</td><td>Detection of Cyber Crime on Social Media using Machine Learning Algorithm</td></tr>
<tr><td>PROJECT GUIDE DETAILS</td><td>Dr. MUZAMEEL AHMED, Associate Professor
9980465900
muzameelahmedise@dayanandasagar.edu</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>STUDENT DETAILS</td><td>
<table>
<tr><th>USN</th><th>NAME</th><th>PHONE NO.</th><th>EMAIL ID</th></tr>
<tr><td>1DS19IS068</td><td>POOJA M</td><td>7795826640</td><td>poojamanchu2002@gmail.com</td></tr>
<tr><td>1DS19IS076</td><td>RAKSHITHA K</td><td>8431783324</td><td>rakshithaaaa.9@gmail.com</td></tr>
<tr><td>1DS19IS108</td><td>SREENIKETH MADGULA</td><td>9986020902</td><td>sreeniketh.madgula@gmail.com</td></tr>
</table>
</td></tr>
<tr><td>PROJECT TIMELINE (Tentative Start and End Date)</td><td>November 2022-April 2023</td></tr>
<tr><td>PROJECT COORDINATORS</td><td>Dr. Vaidehi M
Prof. Bhavani K</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>DOMAIN OF PROJECT</td><td>Cyber Security and Machine Learning</td></tr>
<tr><td>BACKGROUND OF PROJECT WITH REGARD TO THE DRAWBACK ASSOCIATED WITH EXISTING PROJECT</td><td>The base papers describe a system that provides a platform that does sentiment analysis on uploaded text from social media platforms. Users upload comments, posts etc. to the developed system rather than the system extracting these from social media platforms directly.

The system should rather detect cybercrime from the posts automatically, and also from related comments and threads.</td></tr>
<tr><td>OBJECTIVES OF THE PROJECT</td><td>Provide a platform where users can upload links to social media posts to evaluate whether they are offensive or not.</td></tr>
</table>

	Define a metric to gauge whether a comment or media shared publicly accounts to cybercrime (cyberbullying). Scrape urls of posts for related comments and shared links; evaluate them and add to the score of the post Determine the legitimacy of links shared publicly, ads etc. Detect fraudulent links and warn against crimes like credit card frauds (phishing)
PROBLEM STATEMENT	Social media posts are a way for users to express their views on a public platform. But there have been many instances of cyber bullying where users share extremist views, offensive comments, threats etc. Enhancements are required, to address the shortcomings of the existing platforms. Many links and ads on the internet have trackers that try to extract user data. This data is used generally for analytics, but there are also many cases of phishing. There is a dire need of a system to tend to this widespread issue.
SUMMARY OF THE PROJECT	This project is a web platform that allows users to upload url links of social media posts to check if it is a case of cyberbullying or not. The url of the post is scraped for the related comments and media, and embedded links which in turn are scraped again. The collected data is fed into a pipeline that performs sentiment analysis on each of the components to add to a final score that classifies the post/article as positive, negative, or neutral. Apart from the web platform, this project involves the development of a web extension that warns users against navigating to malicious links, indicating the risk of a potential fraud (credit card fraud etc.)
MODE OF CARRYING OUT THE PROJECT	Within the Department of Information Science and Engineering, Dayananda Sagar College of Engineering.
INTENDED BENEFICIARIES OF THE PROJECT	Users of social media platforms Public browsing the internet
BASE PAPERS/ RELATED WORK	1. Saeed Al Mansoor, Afrah Almansoori, Mohammed Alshamsi, Said A Salloum, Khaled Shaalan, “Suspicious Activity Detection of Twitter and Facebook using Sentimental Analysis”, November 2022 2. Puneetha KR, Reena Rodrigues, Shreenidhi Shetty, Pooja H, “Proactively Discouraging Cyberbullying Activities”, October 2022
ABSTRACT	The purpose of this project is to evaluate malicious activity by users of

	social media platforms like Meta (Facebook), Instagram, Twitter, etc.. Some comments thrown across these platforms may guise as normal but can be perceived offensive by many communities. Users tend to express extremists and abusive views publicly exploiting their freedom to post without immediate consequences. This project involves the use of machine learning algorithms, specifically NLP techniques to classify media into positive, negative or neutral groups and also the degree to which they fall into a group. Malicious links on the internet have many trackers which are used to conduct crimes like credit card fraud. They usually have multiple redirects which finally navigate to an endpoint of an ad or survey. Multiple layers of these traversed links have trackers that are used for phishing activities. As part of this project, a browser extension is to be developed that blocks and warns users against such links.
KEYWORDS	Sentiment Analysis, NLP

Signature of Guide

Signature of Domain Expert

Project Coordinators
(Dr. Vaidehi M, Prof. Bhavani K)

HOD-ISE
(Dr. Rajeshwari M)