A Project Report

On

"Billy- Buddy: An AI-Powered Solution for Cyberbullying Detection, Prevention and Victim Support"

CST- G16

Batch Details

Slno.	Name	Rollno.
1	Mekala Charan Kumar	20211CST0092
2	Krithik S	20211CST0137
3	Gandu Sanjay	20211CST0031
4	Mohammed Kaif	20211CST0014

School of Computer Science,

Presidency University,Bengaluru.

Under the Supervision of,

Dr. Marimuthu K,
Professor,
School of Computer Science and Engineering,
Presidency University.

<u>CONTENTS</u>

1. INTRODUCTION

Cyberbullying, especially among teenagers, has become a major issue in the digital age, involving harmful behaviors like spreading rumors, threats, or hate speech on social media. This often leads to severe psychological effects such as anxiety, depression, and even suicidal thoughts.

Our website offers a comprehensive solution to address this problem. At its core is **"Billy"**, an empathetic chatbot that provides immediate emotional support while maintaining the victim's anonymity. **Billy** not only comforts but also gathers evidence of bullying incidents, which is securely reported to cybercrime authorities, keeping the victim's identity protected.

Additionally, the platform tracks **cyber-crime statistics** in real time, identifying high-risk areas (red-alert zones) for targeted interventions by authorities.

To empower users, we offer **tips and defense tactics** on how to stay safe online. The platform also fosters a **community of survivors**, allowing victims to connect, share experiences through **Q&A sessions**, and learn from each other in a safe, anonymous space.

With its multi-faceted approach—emotional support, secure reporting, data-driven tracking, education, and community building—our platform aims to prevent and reduce cyberbullying while offering meaningful help to victims.

2. LITERATURE REVIEW

Definition and Prevalence of Cyberbullying

Cyberbullying is defined as aggressive behavior that occurs through digital devices, where individuals target others via social media, messaging apps, and online forums. This form of harassment is particularly prevalent among teenagers, with studies indicating that approximately 15% to 35% of youth report experiencing some form of cyberbullying (Kowalski et al., 2014). The anonymity and reach of online platforms contribute to the increasing frequency of such incidents, highlighting the need for effective intervention strategies.

Impact on Victims

The psychological effects of cyberbullying can be severe. Victims often experience a decline in self-esteem, increased anxiety, depression, and suicidal ideation (Hinduja & Patchin, 2010). Research suggests that the emotional impact of cyberbullying can be long-lasting, affecting academic performance, social relationships, and overall mental health (Tynes et al., 2010). Understanding these consequences is crucial for developing support systems that effectively address the needs of victims.

Technological Solutions for Support

Recent advancements in technology have led to the development of various online support mechanisms. Chatbots, such as the user-friendly interface proposed in our website, have been shown to provide immediate assistance and emotional comfort to users experiencing distress (Shah et al., 2020). By ensuring user anonymity, these tools can encourage victims to share their experiences without fear of retribution. Moreover, reporting mechanisms integrated into such platforms can facilitate the collection of evidence and enhance the response from cybercrime authorities (Li et al., 2020).

Data Tracking and Community Engagement

The implementation of statistical tracking systems is essential for identifying patterns and

hotspots of cyberbullying. By monitoring incidents in real time, authorities can allocate resources more effectively to regions identified as high-risk (Beran & Li, 2005). Furthermore, creating a community for victims fosters shared experiences and support. Online forums and Q&A sessions allow individuals to connect, share coping strategies, and learn from one another, significantly enhancing their resilience against future incidents (Bandyopadhyay et al., 2018).

Educational Resources and Preventive Measures

Educational initiatives are crucial for empowering youth to navigate the digital landscape safely. Providing tips and defense tactics on websites can help young people recognize and respond to cyberbullying, fostering a culture of awareness and prevention (Wright, 2017). Comprehensive strategies that combine emotional support, technological intervention, community building, and education represent a holistic approach to combatting cyberbullying effectively.

3. MOTIVATION

Cyberbullying is a pressing issue in today's digital era, especially among teenagers who are active on social media platforms. Observing its devastating impact on victims—ranging from emotional distress and depression to extreme consequences like suicidal ideation—motivated us to tackle this problem.

The growing prevalence of cyberbullying, coupled with its anonymity and rapid spread, creates an urgent need for innovative solutions. Many victims feel helpless and isolated, unsure where to turn for support, while perpetrators often evade accountability. This gap in effective intervention and awareness inspired us to create a solution that provides immediate, anonymous assistance while ensuring justice and protection.

Additionally, the emotional toll cyberbullying takes on victims and their families further strengthened our resolve to contribute positively to society. By developing a platform that not only provides support but also helps the authorities track cybercrime patterns, we aim to foster a safer digital environment.
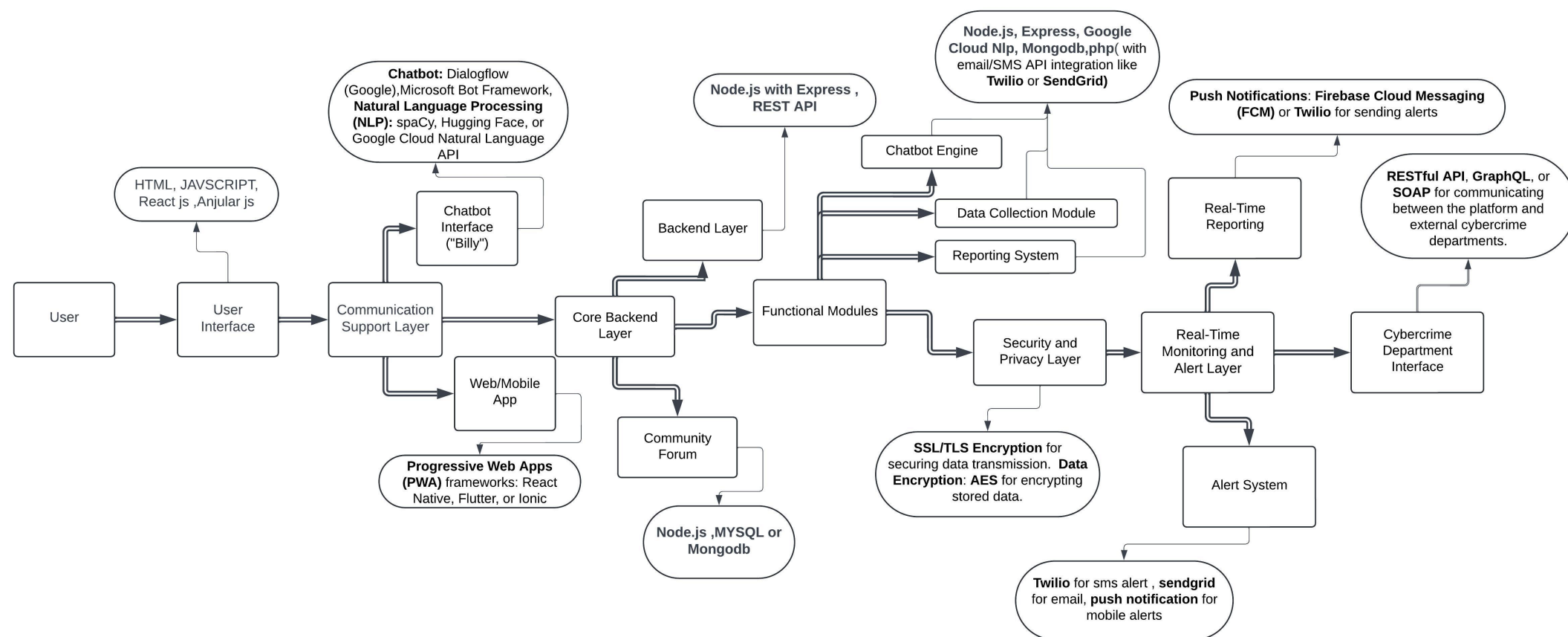
Our project also seeks to empower victims and communities by facilitating shared experiences and collective learning. Providing actionable tips, promoting awareness, and building a supportive network can bring lasting change. Ultimately, the goal is to create an ecosystem where everyone feels safe, supported, and educated about combating cyberbullying effectively.

4. OBJECTIVES

Based on the observations and research gaps identified in the literature survey, the following specific objectives have been formulated:
➢ Use the chatbot "Billy" to offer instant, compassionate support to victims of cyberbullying.
➢ Protect victims identities while enabling them to report cyberbullying incidents to the cybercrime department.
➢ Track and monitor cyberbullying incidents geographically to help law enforcement focus on high-risk areas.
➢ Create a platform where victims can connect, share experiences, and learn coping strategies from others who have faced cyberbullying.
➢ Provide tips, educational materials, and defense tactics to empower individuals to protect themselves from online harassment.
➢ Collect data on cyberbullying incidents to identify trends and help policymakers address the issue proactively.

5. METHDOLOGY

Chatbot: Dialogflow (Google),Microsoft Bot Framework, **Natural Language Processing (NLP):** spaCy, Hugging Face, or Google Cloud Natural Language API

HTML, JAVSCRIPT, React.js ,Anjular js

Chatbot Interface ("Billy")

Node.js with Express , REST API

Node.js, Express, Google Cloud Nlp, Mongodb,php(with email/SMS API integration like **Twilio** or **SendGrid**)

Chatbot Engine

Data Collection Module

Reporting System

Push Notifications: Firebase Cloud Messaging **(FCM)** or **Twilio** for sending alerts

Real-Time Reporting

RESTful API, GraphQL, or **SOAP** for communicating between the platform and external cybercrime departments.

User → User Interface → Communication Support Layer → Core Backend Layer → Functional Modules → Security and Privacy Layer → Real-Time Monitoring and Alert Layer → Cybercrime Department Interface

Backend Layer

Web/Mobile App

Progressive Web Apps (PWA) frameworks: React Native, Flutter, or Ionic

Community Forum

Node.js ,MYSQL or Mongodb

SSL/TLS Encryption for securing data transmission. **Data Encryption: AES** for encrypting stored data.

Alert System

Twilio for sms alert , **sendgrid** for email, **push notification** for mobile alerts

1. User Interface (UI):
  - The user interacts with the system via a web or mobile application. This interface is built using technologies like **HTML, JavaScript, React.js, or Angular.js**. These technologies ensure that the user experience is interactive and smooth.

2. Communication Support Layer:
  - After the user interacts with the system through the UI, the **Communication Support Layer** helps manage the communication between the user and the core system functionalities, including chatbot communication.

3. **Chatbot Interface**:
  - A chatbot interface (referred to as "Billy") is used to facilitate interactions. The chatbot uses **Natural Language Processing (NLP)** to understand user input. Technologies like **Dialogflow, Microsoft Bot Framework, or NLP libraries (e.g., spaCy, Hugging Face, Google Cloud NLP)** can be used here to process and understand human language.

4. Backend Layer:
  - This layer, built using **Node.js with Express** and REST APIs, handles the business logic of the system. It receives requests from the user or chatbot interface and processes them to provide responses or perform tasks.

5. Core Backend Layer:
  - This layer is the heart of the system that coordinates various modules and functionalities. It processes data, requests, and actions as per the system's logic.

6. Functional Modules:
  - The core backend layer works in conjunction with functional modules like:
    - **Data Collection Module**: Collects and processes user or system data.
    - **Reporting System**: Generates reports from the data collected.

7. Security and Privacy Layer:
  - Ensures secure data transmission through **SSL/TLS Encryption**. For stored data, encryption techniques like **AES (Advanced Encryption Standard)** are used to keep sensitive information safe.

8. Real-Time Monitoring and Alert Layer:
  - This module monitors the system in real-time and generates alerts for specific conditions or events. These alerts can be related to cybercrime activities or system errors.

9. Real-Time Reporting:
   - Gathers information and generates reports in real-time, which can be used for system monitoring or to notify relevant teams (like cybercrime departments).

10. Alert System:
   - When an alert is triggered, notifications can be sent via multiple channels like SMS, email, or mobile app push notifications. APIs like **Twilio** for SMS, **SendGrid** for email, and **Firebase Cloud Messaging (FCM)** for push notifications can be integrated for these alerts.

11. Cybercrime Department Interface:
   - There is an interface to communicate with external cybercrime departments via **RESTful APIs, GraphQL, or SOAP**, ensuring timely action against potential threats or suspicious activities.

12. Community Forum:
   - A forum built using technologies like **Node.js, MySQL, or MongoDB** where users can interact with the community or seek help.

13. Progressive Web Apps (PWA):
   - For better mobile responsiveness, the system can use **PWA frameworks** such as **React Native, Flutter, or Ionic** to create mobile-first experiences.

6. ALGORITHM

User Interface Module

- Technology: HTML, JavaScript, React.js, Angular.js
- Function: Provides a front-end experience to the user.
- Steps:
    - Step 1.1: Load the homepage, showing the chatbot, support resources, and community options.
    - Step 1.2: Accept user input and send it to the Communication Support Layer.
    - Step 1.3: Display responses from the chatbot and other modules.

Communication Support Layer

- Function: Manages user interactions and relays them to relevant backend services.
- Steps:
    - Step 2.1: Initialize the chatbot interface (Billy).
    - Step 2.2: Route user queries to the Chatbot Interface or other support services.
    - Step 2.3: Direct users to the Web/Mobile App interface or the Community Forum as needed.

Chatbot Interface ("Billy")

- Technology: NLP services like Dialogflow, Microsoft Bot Framework, and NLP libraries (spaCy, Hugging Face).
- Function: Interacts with users to provide comfort and guidance.
- Steps:
    - Step 3.1: Greet users and assess their needs.
    - Step 3.2: Ask if they want to report an incident and collect relevant details if yes.
    - Step 3.3: Provide support, tips, or resources based on user input.

◦ Step 3.4: Forward collected data to the Data Collection Module and Reporting System if a report is made.

Backend Layer

- Technology: Node.js with Express, REST API
- Function: Manages data processing and integrates with various modules.
- Steps:
    ◦ Step 4.1: Handle requests from the User Interface and Chatbot Interface.
    ◦ Step 4.2: Relay data between the Core Backend Layer and other modules.

Core Backend Layer

- Function: Core processing and data storage.
- Steps:
    ◦ Step 5.1: Store and manage user data securely.
    ◦ Step 5.2: Route data to the Functional Modules for analysis, reporting, or community interaction.

Functional Modules

- Components: Community Forum, Chatbot Engine, Data Collection Module, Reporting System
- Steps:
    ◦ Step 6.1: Community Forum - Allows users to interact anonymously with others. Provides Q&A and sharing options.
    ◦ Step 6.2: Chatbot Engine - Processes chatbot inputs, using NLP tools to enhance interactions.
    ◦ Step 6.3: Data Collection Module - Aggregates information from reports to generate analytics.
    ◦ Step 6.4: Reporting System - Sends anonymized reports to the cybercrime department.

Security and Privacy Layer

- Technology: SSL/TLS for secure data transmission; AES for stored data encryption.
- Function: Ensures data privacy and security.
- Steps:
    ◦ Step 7.1: Encrypt all data transmitted between modules using SSL/TLS.
    ◦ Step 7.2: Store data securely with AES encryption to protect user privacy.

Real-Time Monitoring and Alert Layer

- Function: Monitors real-time data and triggers alerts for high-risk areas or urgent cases.
- Steps:
    ◦ Step 8.1: Use data from the Reporting System to identify red-alert zones.
    ◦ Step 8.2: Trigger alerts for high-incidence areas and escalate cases as needed.

Alert System

- Technology: Twilio for SMS alerts, SendGrid for email, Firebase Cloud Messaging for push notifications.
- Function: Notifies users and authorities of high-risk situations.
- Steps:
    ◦ Step 9.1: Send real-time alerts to the cybercrime department and relevant stakeholders.

- Step 9.2: Notify users of updates or provide resources as needed through push notifications.

Cybercrime Department Interface

- Technology: RESTful API, GraphQL, or SOAP for data transfer.
- Function: Interface for reporting and monitoring by cybercrime authorities.
- Steps:
    - Step 10.1: Receive reports and alerts from the Real-Time Reporting module.
    - Step 10.2: Provide access to aggregated data and analytics for red-alert areas.

7. OUTCOMES

1. **Increased Reporting of Cyberbullying Incidents:** Victims will feel more comfortable reporting cyberbullying through the anonymous chatbot, leading to a higher number of cases being reported.

2. **Timely Intervention:** The real-time reporting system will enable faster responses from law enforcement, helping to address cyberbullying incidents more promptly.

3. **Improved Victim Support:** Victims will receive instant emotional support through the chatbot, reducing feelings of isolation, fear, and frustration.

4. **Anonymity Assurance:** Victims' identities will remain protected throughout the reporting process, encouraging more individuals to come forward without fear of retaliation.

5. **Increased Awareness of Cyberbullying:** Educational resources and defense tactics on the platform will increase awareness about cyberbullying, its effects, and ways to combat it.

6. **Formation of a Supportive Community:** A virtual community of individuals who have experienced cyberbullying will provide emotional and practical support, helping new victims recover and learn coping strategies.

7. **Data-Driven Law Enforcement:** Cyber-crime statistics collected through the platform will help authorities focus on high-risk areas, enabling better resource allocation and targeted actions.

8. **Reduction in Cyberbullying:** With increased awareness, support, and law enforcement focus, there is potential for a gradual reduction in the overall number of cyberbullying cases.

9. **Empowerment of Youth and Users:** By providing access to self-help tools, defense tactics, and community support, the project will empower individuals to take proactive steps to protect themselves from cyberbullying.

10. **Improved Mental Health Outcomes:** Victims who receive timely support and feel part of a community are more likely to experience improved mental health, reducing the long-term psychological impact of cyberbullying.

8. CONCLUSION

"BILLY-BUDDY AGAINST CYBER BULLYING" is designed to address the rising issue of cyberbullying by providing immediate emotional support, ensuring victim anonymity, and reporting incidents to the cybercrime department. The innovative chatbot "Billy" empowers victims by offering a safe space to share their experiences, collect evidence, and connect with others who have faced similar challenges. By tracking cyber-crime trends and focusing on high-risk areas, this project contributes to a more proactive approach in tackling cyberbullying. Additionally, the platform's educational resources and support community aim to equip individuals with tools to protect themselves and promote a culture of resilience. Ultimately, "Billy" serves as both a protective and empowering resource for victims of online harassment.

9. REFERENCES

1. The role of perceived severity publicity anonymity type of cyberbullying and victim response.Retirved from https://www.sciencedirect.com/journal/computers-in-human-behavior
2. An investigation of the effectiveness and determinants of seeking support among adolescent victims of cyberbullying.Retrieved from https://doi.org/10.1016/j.soscij.2018.09.011
3. "A Study of Cyberbullying Detection U sing Machine Learning Technique", 2020 Fourth International Conference on Computing Methodologies and Communi-cation (ICCMC),Retreived from https://ieeexplore.ieee.org/document/9076550
4. "Offensive text detection using temporal convolutional networks", Int. J. Adv. Sci. Technol, Retreived from https://www.researchgate.offensive text classification
5. "Cyberbullying detection solutions based on deep learning architectures", Multimedia Systems, Retrieved from https://link.springer.com/article/10.1007/s00530-020-00701-5
6. "Towards Automatic Detection of Inappropriate Content in Multi-dialectic Arabic Text", Advances in Computational Collective Intelligence. ICCCI 2022. Communications in Computer and Information Science(CCIS), Retrived from https://link.springer.com/chapter/10.1007/978-3-031-16210-7_7
7. "Multimodal cyberbullying detection using capsule network with dynamic routing and deep convolutional neural network", Multimedia Systems, Retreived from https://link.springer.com/article/10.1007/s00530-020-00747-5