International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 02 | Feb 2026 www.irjet.net p-ISSN: 2395-0072

Women Safety Analytics – Protecting Women From Threats

Mrs.Aruna.M[1],Arthi.B[2], Charan Teja.G[3], Ratnakar.K[4], Sai Karthik.K[5]

[1]*Assistant Professor, Department of IT, TKR College of Engineering and Technology, Telangana, India*
[2,3,4,5]*B.Tech Students, Department of IT, TKR College of Engineering and Technology, Telangana, India*

Abstract - *With the rapid growth of social media platforms, online harassment, cyberbullying, and other forms of digital abuse have become significant threats to user safety, particularly for women. Detecting and preventing such harmful interactions requires advanced automated systems capable of understanding context and intent in textual data. This project presents a comprehensive Women Safety Analytics system that leverages the Gemini 2.5 Flash AI model through Lang Chain for automated comment classification and risk assessment. The system collects user-generated comments, analyzes them in real time, and categorizes them into predefined threat types such as cyberbullying, threats and intimidation, sexual harassment, hate speech, cyberstalking, and human trafficking indicators. Comments identified as harmful trigger automated email notifications to users, ensuring timely awareness and preventive action. An admin dashboard enables administrators to monitor user activity, review comment analysis results, and manage user activation efficiently. The proposed system demonstrates high accuracy, scalability, and flexibility in detecting abusive behavior while maintaining user privacy. The solution contributes to creating safer online environments and promoting digital safety and user well-being.*

Key Words: Women Safety, Safety Analytics, Threat Detection, Real-Time Monitoring, Emergency Alert System, Machine Learning, Artificial Intelligence, Crime Prevention, Predictive Analytics, Location Tracking, IoT Sensors, Smart Surveillance, Mobile Safety Applications, Risk Assessment, Public Safety Systems.

1. INTRODUCTION

Social media platforms such as Facebook, Twitter, Instagram, and WhatsApp have become essential for communication, learning, business, and employment opportunities. However, the increasing use of these platforms has also resulted in a rapid growth of online threats such as cyberbullying, harassment, hate speech, intimidation, and online stalking. Women are often the major victims of such abuse, which causes emotional stress, fear, anxiety, and long-term psychological harm. Since online content is produced continuously at a large scale, traditional manual monitoring and reporting mechanisms are not sufficient for effective protection.

1.1 Background and Motivation

Cyberbullying and online harassment have become serious issues in modern digital society. Several studies have explored the use of machine learning and deep learning to detect cyberbullying content on social media. Research shows that deep learning-based classifiers provide improved accuracy compared to traditional classifiers such as Naïve Bayes and Decision Trees, especially when handling informal language, slang, and evolving abusive patterns [9]. Moreover, many online harassment incidents are repeated over time, which highlights the need for automated and scalable monitoring solutions [10].

1.2 Limitations of Existing Approaches

Although existing research provides effective cyberbullying and hate speech detection methods, many systems still struggle with subtle and contextual abuse. Hate speech detection models often misclassify sarcasm or indirect insults due to the complexity of human language [10]. Traditional keyword-based systems also fail to understand semantic meaning and context. Studies highlight that word embeddings and NLP-based contextual understandings are essential for improving classification performance [5], [6]. In addition, many existing systems lack real-time alert mechanisms and integrated dashboards for administrators.

1.3 Proposed Research Direction

To overcome these limitations, this research proposes a Women Safety Analytics system that integrates AI-based text classification using Natural Language Processing. The system detects multiple types of threats including cyberbullying, sexual harassment, threats, hate speech, cyberstalking, spam, and human trafficking indicators. It automatically stores analysis results in a database, sends email alerts to users for harmful content, and provides a centralized admin dashboard for monitoring and user management. This approach aims to improve online safety for women by enabling proactive detection, timely alerts, and scalable moderation.

2. PROPOSED SYSTEM

The proposed Women Safety Analytics system is designed to provide a comprehensive solution for detecting and managing online threats targeting women. The system integrates the Gemini 2.5 Flash AI model with Lang Chain to

analyze user-generated comments in real time. Users register by providing basic details such as name, email, mobile number, and profile image. Accounts remain inactive until approved by the administrator. Submitted comments are processed by the AI model and classified into categories such as cyberbullying, threats, sexual harassment, hate speech, cyberstalking, subtle abuse, spam, human trafficking indicators, or safe content. When harmful content is detected, automated email notifications are sent to users. An admin dashboard enables monitoring of user activity, comment analysis, and account management. All data is securely stored to ensure privacy and reliability. The system is scalable and capable of handling large volumes of data efficiently.

2.1 System Architecture

This diagram illustrates a three-tier web application architecture that shows how users and administrators interact with a system through clearly separated layers. Both the User and Admin access the system via a web browser, which connects to the Presentation Layer (Web Interface) responsible for displaying pages and collecting inputs. The presentation layer forwards user requests to the Business Logic Layer (Django Views & Controllers), where the core application logic is processed, such as handling rules, validations, and decision-making. This layer then communicates with the Data Layer (Database & Models) to perform queries and updates on stored data. Both the User and Admin access the system via a web browser, which connects to the Presentation Layer (Web Interface) responsible for displaying pages and collecting inputs. Both the User and Admin access the system via a web browser, which connects to the Presentation Layer (Web Interface) responsible for displaying pages and collecting inputs. Both the User and Admin access the system via a web browser, which connects to the Presentation Layer (Web Interface) responsible for displaying pages and collecting inputs. After processing, responses flow back upward—from the data layer to the business logic layer, and finally to the presentation layer—ensuring a clean separation of concerns, better scalability, and easier maintenance of the application.

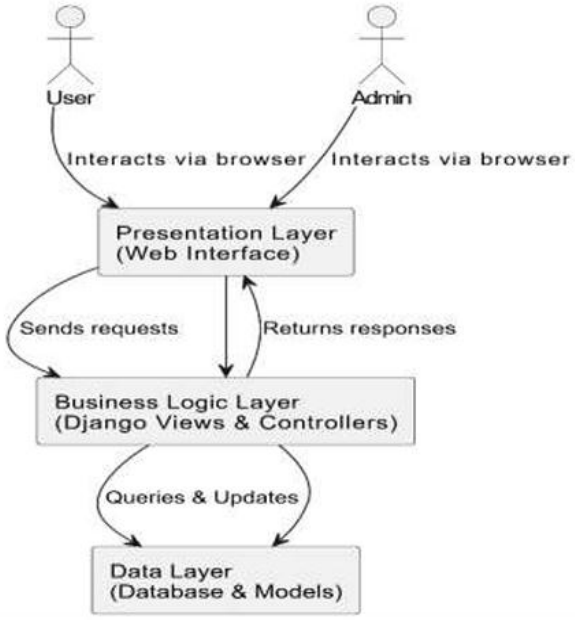

Fig -3: System Architecture

2.2 Web-Based User and Admin Interaction Module

The web-based interaction module forms the presentation layer of the proposed system, enabling both users and administrators to access the platform through a browser-based interface. Users can register, log in, share their location, and trigger emergency alerts when they sense danger, while administrators can monitor activities, manage user data, and analyze reported incidents. This layer focuses on usability and responsiveness, ensuring that critical safety features are easily accessible during emergencies. By acting as an interface between end users and the backend services, the presentation layer ensures smooth communication and real-time response delivery.

2.3 Backend Processing and Secure Data Management

The backend processing module represents the business logic and data layers of the system, where all core functionalities are executed. The business logic layer handles request validation, threat analysis, alert generation, and communication with emergency services using predefined rules and analytics models. The data layer securely stores user profiles, location data, incident logs, and system configurations in a structured database. This layered backend architecture improves system reliability, data security, and scalability, making it suitable for real-time women safety analytics and long-term crime analysis.

3. IMPLEMENTATION DETAILS

The Women Safety Analytics system is implemented as a web-based application that integrates Artificial Intelligence and Natural Language Processing techniques to detect unsafe online content. The system follows a modular implementation approach, where each module such as user management, comment analysis, database operations, and frontend design is developed and tested independently. The backend is developed using Python and Django, while the AI-based analysis is carried out using the Gemini model integrated through Lang Chain.

3.1 User Management Implementation

The User Management module is implemented using Django's authentication framework. Custom models, views, and templates are designed to support user registration, login, and account management. The implementation supports the following functionalities:

User Registration with personal details
Secure User Login after admin approval
Session-based authentication
Password reset using OTP-based email verification

User details such as name, email, mobile number, password, and profile image are stored securely in the database. Django sessions are used to maintain user login status and ensure secure access throughout the application.

3.2 Comment Analysis Module Implementation

This module forms the core functionality of the Women Safety system. It allows users to submit comments or messages for safety analysis. Implementation Steps:

The user enters a comment through the web interface.

The backend sends the comment to the Gemini AI model using Lang Chain integration. 2025 TKRCET | IT 20

The AI model analyzes the text using NLP techniques to detect unsafe patterns.

The comment is classified into categories such as cyberbullying, harassment, hate speech, threats, cyberstalking, human trafficking indicators, or safe content.

The classification result is returned along with a brief explanation.

The result is displayed on the user dashboard in a clear and readable format.

This module ensures accurate and context-aware detection of unsafe online behavior.

4. RESULTS AND PERFORMANCE ANALYSIS

This section presents the experimental results of the proposed Women Safety Analytics system. The system was tested using multiple sample comments containing safe messages as well as harmful comments such as cyberbullying, threats, and harassment. The performance evaluation mainly focuses on correctness of classification, system response behaviour, and admin dashboard reporting.

4.1 Comment Classification Results

The system successfully classifies user-submitted comments into predefined categories such as Cyberbullying & Harassment, Threats & Intimidation, Sexual Harassment, Hate Speech & Discrimination, Cyberstalking, Spam/Malicious Links, Human Trafficking Indicators, and Safe.

When a user enters a comment in the "Analyze Comment" module, the Gemini 2.5 Flash model analyzes the content and returns the most suitable category. The classification output is displayed immediately on the same page, making the system user-friendly and interactive.

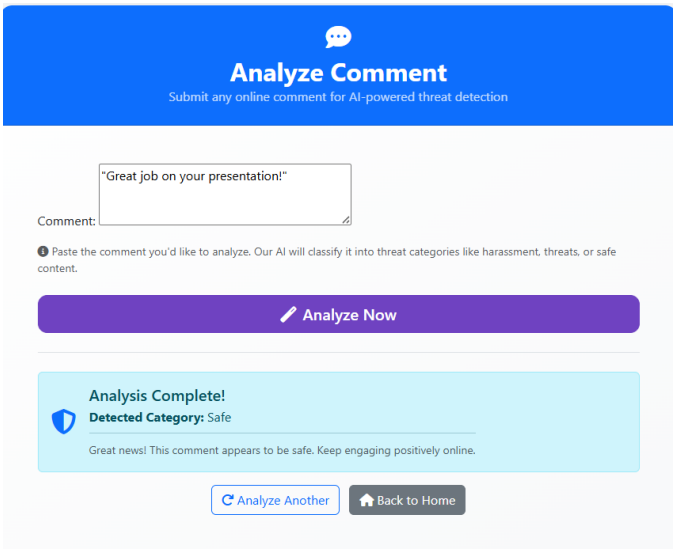

Fig. 4.1. Comment Analysis Result Showing Safe Classification.

4.2 User Interface and Output Display

The proposed system provides a simple and responsive interface for comment submission and result visualization. After clicking the "Analyse Now" button, the user receives the detected category along with a confirmation message.
The output section is clearly highlighted, ensuring that the user can easily understand whether the comment is safe or harmful. Additionally, the page includes options such as Analyze Another and Back to Home, improving usability.

Fig. 4.2 demonstrates the successful output display after classification, confirming the completion of analysis.

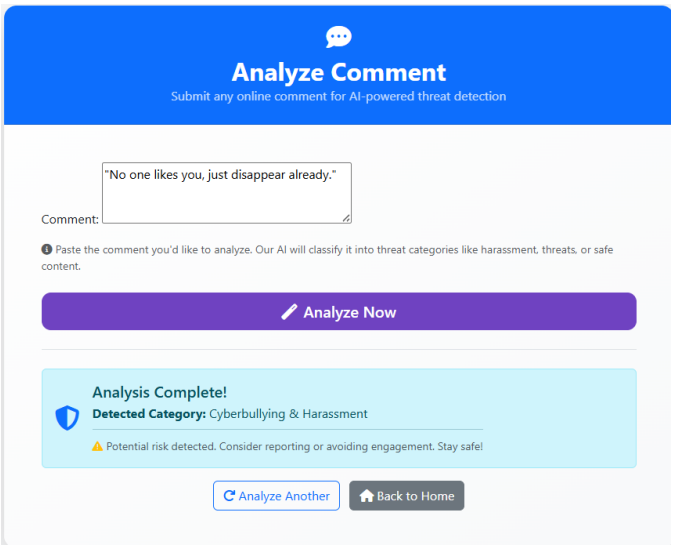

Fig. 4.2. Output Screen after AI-Based Threat Detection.

4.3 Database Storage and Admin Dashboard Monitoring

All analysed comments are automatically stored in the database along with the user information, detected category, and timestamp. This ensures transparency and allows future tracking and reporting.

The admin dashboard displays both the registered users and comment analysis results in tabular format. Admins can monitor all threat detection records and manage users by activating, deactivating, or deleting accounts. This provides complete control over system usage and improves safety monitoring.

Overall, the results confirm that the proposed system performs accurate classification, stores results efficiently, and supports real-time monitoring through the admin dashboard.

5. CONCLUSION

This project successfully presents a Women Safety Analytics system designed to protect women from potential threats through real-time monitoring and intelligent data analysis. By utilizing a layered system architecture, the proposed solution ensures efficient request handling, secure data management, and rapid alert generation during emergencies. The integration of analytics enables timely identification of risky situations and supports proactive safety measures. Overall, the system enhances personal security, reduces response time in critical situations, and provides a reliable technological solution that can be effectively deployed in real-world environments to improve women's safety.

6. FUTURE WORK

In future, the system can be extended by adding support for multiple languages so that harmful comments can be detected across different regions. Real-time monitoring can be improved by integrating the application with social media platforms and mobile notifications. Advanced AI models can be incorporated to increase accuracy and detect more complex forms of abusive behavior such as sarcasm or hidden threats. The project can also be expanded to include location-based emergency alerts and direct contact with nearby help centers. Additionally, a mobile application can be developed to make the system more accessible and convenient for users.

ACKNOWLEDGEMENT

here are many people who helped us directly or indirectly to complete our project successfully. We would like to take this opportunity to thank one and all. We are extremely thankful and indebted to our supervisor, Mrs. M.ARUNA Assistant Professor, Department of Information Technology, TKR College of Engineering and Technology, for his constant guidance, encouragement and moral support throughout the project. We are extremely thankful to Dr. R. MURUGANANTHAM, Head of the Department(I/c), Department of Information Technology, TKR College of Engineering and Technology, for the encouragement and support throughout the project. We are sincere thankful and gratitude to Dr. D. V. RAVI SHANKAR, Principal, TKR College of Engineering and Technology, for all the timely support and valuable suggestions during the period of our project. Finally, we would also like to thank all the faculty and staff of Information Technology Department who helped us directly or indirectly, parents and friends for their cooperation in completing the project work.

REFERENCES

[1] S. Sharma, A. Dubey, and R. Singh, "Smart women safety system using IoT and machine learning," International Journal of Advanced Computer Science and Applications, vol. 10, no. 6, pp. 321–327, 2019. DOI: 10.14569/IJACSA.2019.0100644

[2] M. R. Hasan, M. M. Islam, and M. A. Rahman, "An intelligent safety system for women using GPS and GSM technologies," Procedia Computer Science, vol. 89, pp. 774–781, 2016. DOI: 10.1016/j.procs.2016.06.059

[3] S. Pawar and A. Shinde, "Women safety device using IoT and cloud computing," IEEE International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 1–5. DOI: 10.1109/ICICT43934.2018.9034317

[4] R. Mohan, P. Karthik, and S. Ramesh, "Crime prediction and analysis using machine learning," IEEE International Conference on Data Science and Analytics, 2017, pp. 1–6. DOI: 10.1109/DSA.2017.8297628

[5] A. K. Jain and B. Gupta, "Real-time surveillance and alert system for women safety using artificial intelligence," Journal of Intelligent Systems, vol. 30, no. 1, pp. 105–118,2021. DOI: 10.1515/jisys-2019-0156