SocialBullyAlert: A Web Application for Cyberbullying Detection on Minors' Social Media

Elizabeth Adriana Nina-Gutiérrez, Jesús Emerson Pacheco-Alanya, Juan Carlos Morales-Arevalo
Faculty of Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Perú

***Abstract*—The severe problem of cyberbullying towards minors is addressed, which has been shown to have significant impacts on the mental and emotional health of children and adolescents. Subsequently, the effectiveness of existing artificial intelligence models and neural networks in detecting cyberbullying on social media is analyzed. In response, a web platform is developed whose contribution is to identify offensive content, adapt to various slangs and idioms, and offer an intuitive interface with high usability in terms of user experience (UX) and user interface (UI) design. The application was validated with cyberbullying experts (teachers, principals, and psychologists), and the UI/UX design was also validated with users (parents). Limitations and future challenges are discussed, including varying cyberbullying regulations, the need for constant updates, and adapting to multiple languages and cultural contexts. This highlights the importance of ongoing research to enhance parental control tools in digital environments.**

***Keywords*—Cyberbullying; artificial intelligence (AI); neural networks; parental control; social media; offensive content detection; User Experience (UX); User Interface (UI); mental health**

I. Introduction

Cyberbullying towards children and adolescents is a social problem, where the perpetrators are often other young people who know the victim. In a qualitative study, adolescents indicated that public harassment on social media was more harmful than private internet attacks. In turn, attacks from bullies who knew their victims generated a greater negative impact [1].

Likewise, the most relevant cause is the one pointed out by [2]; they demonstrated in their study that 96.6% of children indicated that they received their first cell phone at nine and a half years old. These figures show that children are not being properly supervised and are misusing the technology offered to them.

Moreover, online harassment negatively affects the psychological well-being of adolescents, as proven in a study conducted in India [3]. They found that being a victim of cyberbullying is associated with an increased risk of depression and suicidal thoughts in adolescents and young adults. Additionally, 29.63% of participants reported having experienced cyberbullying. Furthermore, being a victim of cyberbullying was associated with a higher risk of depression (with a prevalence rate of 15.56%) and suicidal thoughts (with a prevalence rate of 22.02%) compared to those who were not victims of cyberbullying.

Additionally, analyzing a specific case in the Peruvian context, the study by [4] conducted in schools in Iquitos found that only 36.7% of students were not involved in bullying or cyberbullying. Regarding cyberbullying alone, 13.6% were cyber victims, 6.1% were cyberbullies, and 16.7% were both cyber victims and cyberbullies.

On the other hand, to address cyberbullying through technological platforms, various models were found that use artificial intelligence for the detection of offensive texts. The research in [5] points out in their review article that Machine Learning is the most widely used branch of artificial intelligence (AI) when creating technological tools to combat bullying and cyberbullying. Apps are mostly created to detect inappropriate language based on patterns and systems that identify social media profiles.

However, the following limitations have been identified in current Artificial Intelligence solutions: dataset dependency, difficulty in detecting subtle offenses, language and data limitation, and limitation in adapting to different platforms and media types. For instance, in the AI model proposed by the authors [6], it has been observed that it encounters difficulties in classifying ambiguous tweets or those with mixed contexts, especially when they contain offensive or emotive words. Therefore, it can be said that it has a deficiency in detecting subtle offenses and a limitation in platforms since it can only cover one social network. Additionally, the relevance of context and implicit information in tweets for hate speech detection is highlighted. On the other hand, the method proposed by study [7] and study [8] presents a significant limitation related to language, as it is trained and evaluated with English datasets, which restricts its ability to generalize to other languages and domains. Furthermore, by being based on a model pre-trained solely in English, there is a risk of introducing linguistic and cultural biases in applications for other languages.

The main approach in this research consists of a parental control platform that detects cyberbullying on users' social media and alerts parents about it. To achieve this, the architecture integrates different APIs to collect, process, and analyze data from minors' social media profiles. The APIs utilized include: Apify, to obtain information from social media profiles; a fine-tuned model based on GPT-3.5, to detect hate speech or offensive language in texts; and Google Cloud Vision, for the detection of offensive or inappropriate images.

Likewise, the main contribution is an innovative parental control web application that employs AI to analyze content and detect risks on children's and adolescents' social media profiles. It was carefully designed with a focus on user experience and an intuitive interface, combining the power of AI with excellent

usability for parents. This solution will be validated with expert opinions and user surveys.

This article is divided into the following sections: First, Section II reviews related works on the design of platforms and solutions for detecting cyberbullying. Section III describes the main contribution in more detail. Additionally, Section IV explains the main functionalities offered by this platform for cyberbullying towards minors, and to verify its effectiveness, it was tested through two types of validations in Section V. Following this, Section VI presents the Results of the experiments. Finally, Section VII shows the pending points for improvement or for future research, and Section VIII covers the general conclusions.

II. Related Work

Through technological platforms, various models using artificial intelligence for the detection of offensive texts have been found. [5] points out in their review article that Machine Learning is a discipline of artificial intelligence most widely used when creating technological tools to combat bullying and cyberbullying. Applications are mostly created that detect inappropriate language based on patterns and systems that identify social media profiles.

This section explores several artificial intelligence models, developed in recent years, designed for the detection and prevention of cyberbullying on social media. The contributions and limitations of these models will be evaluated, providing a critical view of how these models address the challenge of online cyberbullying.

On one hand, the study [9] uses a Twitter API to identify "critical points" of cyberbullying by analyzing the language loaded in tweets. It proposes a prediction model to identify possible incidents of cyberbullying on Twitter. Its contribution lies in the discovery that certain loaded language, especially related to "biology", "sexual" and "swear", can be a potential indicator of cyberbullying, thus providing a valuable tool for mediation agencies such as school counselors and law enforcement. However, the main weakness of the study is its exclusive reliance on Twitter text analysis, which may limit its applicability to other cyberbullying contexts where the language or platform differs, and the lack of consideration of other contextual factors that could influence the accurate identification of cyberbullies.

On the other hand, [10] presents an automated classification model to identify cyberbullying texts on Twitter using artificial intelligence and a deep decision tree classifier. Specifically, they used an innovative deep decision tree classifier that incorporates hidden layers of a neural network as tree nodes. Thus, they achieved that the model's capability can handle large datasets without compromising accuracy, achieving 93.58% accuracy and outperforming conventional methods in all metrics evaluated, making it potentially valuable for authorities in the fight against cyberbullying. However, the study does not address how the model handles specific challenges of Twitter, such as the use of special characters, URL shorteners, and informal language, which raises doubts about its robustness in real-world scenarios of this platform.

Furthermore, the study in [11] propose a hybrid deep architecture, CapsNet-ConvNet, which integrates CapsNet for text analysis and ConvNet for image analysis, thus addressing the limitation of previous studies that focused mainly on textual analysis for the detection of harassment and toxicity on social media. Their main contribution is the ability to analyze both the textual and visual content of posts on YouTube, Instagram, and Twitter, using advanced techniques such as ELMo for text representations and the Google Vision API for separating text from images. However, the study's weakness lies in the potential lack of accuracy when facing data that includes idioms or slang, which is common on social media, suggesting that the model may have difficulties adapting to informal and culture-specific linguistic variations.

On the other hand, in another approach, [12] developed a hate comment classifier applied on social media and freely available for developers. This tool would be very important for quickly identifying offensive comments so that they can be reported or removed. To achieve this, they used machine learning models such as XGBoost and the BERT features. The dataset they used consisted of 49,392 comments from social media platforms like YouTube, Reddit, Twitter, and Wikipedia. The algorithms used were specifically Logistic Regression (LR), NB (Naïve Bayes), SVM, XGBoost, and Feed-forward Neural Network (FFNN). There was a higher risk of errors when analyzing Reddit comments, and there was higher accuracy with Twitter comments. The deficiency that the authors indicate is due to polysemy, meaning that some words considered highly offensive on one social network may seem less offensive on another according to the classifier. Consequently, cyberbullying detection in the analyzed content would be less accurate.

Finally, the solution proposed in study [13], the CyberNet model, is an advanced strategy that employs a hybrid deep CNN with N-gram feature selection for cyberbullying detection on online social media platforms. This innovative approach stands out for its ability to identify both abusive text and abusive images, representing a significant advance in the prevention of harmful online behaviors. However, a potential weakness of the model could lie in its reliance on a supervised learning approach, which could limit its effectiveness in detecting new forms of cyberbullying that are not represented in the training data, suggesting the need for continuous adaptability to address the evolution of cyberbullying tactics.

III. Platform Design

A. General Architecture

The architecture of SocialBullyAlert includes the use of an external API to collect data from the child's social media profile. This data goes through AI processing which is a fine-tuned model based on GPT-3.5 to identify cyberbullying in texts. The offensive content is stored in a PostgreSQL database to generate alerts and periodic reports, which are distributed through the web application (Angular) so that parents can monitor their children. The architecture of the solution can be seen in Fig. 1, where the interaction that the SocialBullyAlert system has with external services is observed. The information processing flow for cyberbullying detection is detailed as follows:

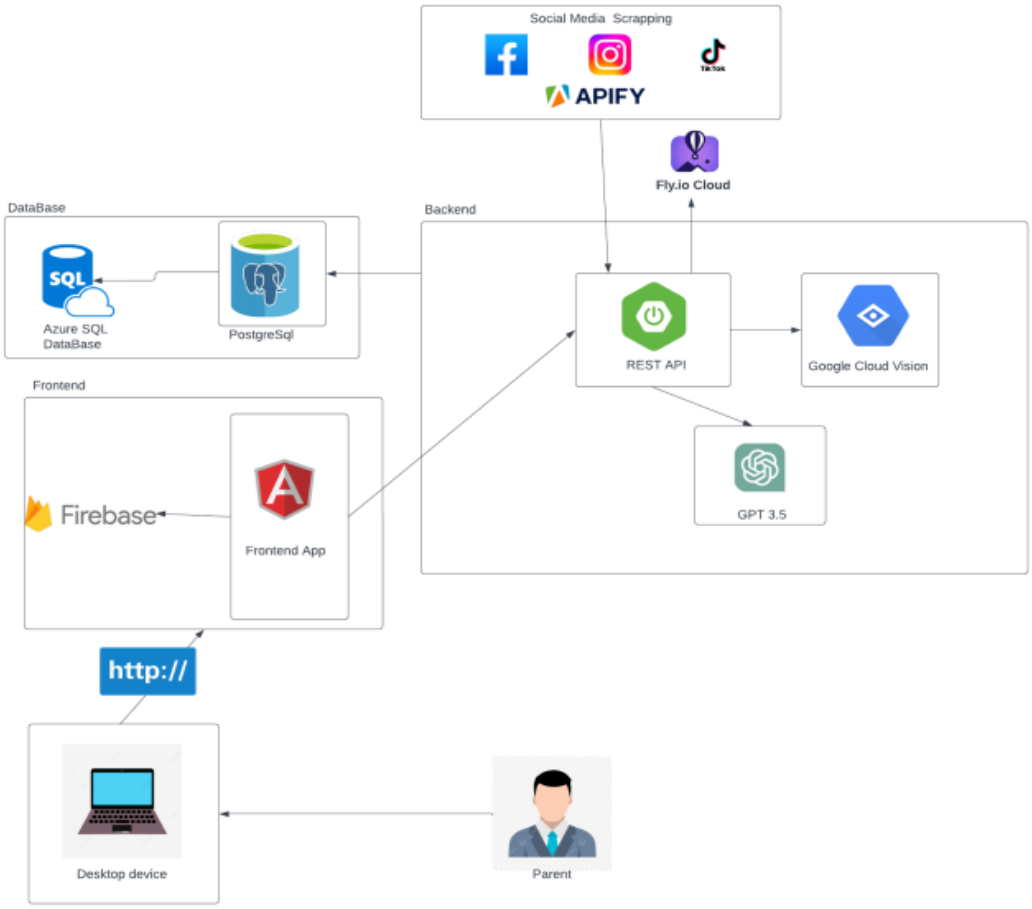

Fig. 1. Solution architecture.

- Collection: In this step, an external API (Apify) is employed to extract all visible information from a child's social media profile. The data can be text, image, or image with embedded text. This information is obtained in JSON format [14].
- Data Processing: The data obtained from the child's social media is processed using both Google Cloud Vision [15] and a fine-tuned model based on GPT-3.5. First, the comment or post is decomposed into text and image if present. The texts go through an AI specialized in cyberbullying detection, which is an artificial intelligence that can identify subtle offences in English and various Spanish language dialects. The result is a JSON object indicating whether the text contains offensive language and hate speech. On the other hand, the images go through analysis by Google Cloud Vision [15]; this AI will be responsible for categorizing the image as "Adult Content", "Mocking Content", "Medical Content", "Violent Content", and "Racy Content".
- Alert Generation: The comment or post containing hate speech, offensive language, or any inappropriate image will be stored in a PostgreSQL database. In this way, the system will be able to generate linear graphs based on time periods and parental advice based on the latest alerts on a child's profile.
- Alert Distribution: The graphs, parental advice, and alerts will be reflected in the web application, which is developed in the Angular framework, prioritizing user experience and an intuitive interface, so that the application is responsive and works correctly on desktop and mobile devices from the most popular browsers.

B. Key Components

The architecture of SocialBullyAlert consists of several key components that work together to provide a comprehensive solution for cyberbullying detection and alert generation. These components leverage cutting-edge technologies, such as artificial intelligence services, web data extraction APIs, and web application development frameworks. The main components that make up the system are described below:

- Apify: It is a web data extraction platform that allows you to create actors (small programs) to collect information from websites efficiently and scalably. They have a very extensive library that offers scrapers for many social networks. It is also widely used by well-known companies such as Microsoft and Samsung [14]. In this particular case, only 6 actors were used to obtain

posts and comments from the social networks Facebook, Instagram, and TikTok.

- Google Cloud Vision: It is an artificial intelligence-based visual recognition service that allows developers to integrate powerful image analysis capabilities into their applications [15]. It has very important features for cyberbullying detection, such as explicit content classification, where it provides classification probabilities for categories like adult content, medical content, violence, and suggestive content [16]. Additionally, it provides optical character recognition (OCR) functionality, which will help extract text present in images.
- Angular: It is a web framework maintained by Google that provides tools, APIs, and libraries to simplify and streamline the development workflow. It provides a solid platform for building fast, reliable, and scalable applications, both in terms of team size and codebase. Angular allows developers to create high-performance web applications efficiently, taking advantage of its extensive set of features and resources [17].
- Fine-tuned GPT-3.5-based model for cyberbullying detection: This is a model based on GPT-3.5 for detecting hate speech and offensive language in English, Peruvian Spanish, Chilean Spanish, and Spanish from Spain. It is a tool that has significantly higher precision compared to similar models. It will serve to detect cyberbullying in textual content found on children's social media, even detecting subtle offences or country-specific slang forms [5]. Thanks to GPT-3.5, it is possible for it to function with more languages in addition to the languages it was trained on.

C. User Interface and User Experience

The interface the platform has follows Nielsen's heuristics, which are considered the best due to their universality and adaptability, having even served as the basis for more specialized heuristics [18]. The following describes how each of the 10 principles has been met:

1) Match between the system and the real world: The application supports language switching between English and Spanish, maintaining the integrity of meaning, and uses universal icons on the buttons that reflect everyday objects, establishing an intuitive connection between the represented action and the button's function, facilitating understanding for a diverse user base (Fig. 8).

2) Visibility of system status: The platform implements dynamic animations that indicate data loading (Fig. 2), along with floating messages that inform the user about the success or failure of processes, thus providing clear and continuous feedback that enhances the user's perception of the system's status and activity.

3) User control and freedom: Before executing important actions such as starting an analysis or deleting a child's profile (Fig. 5), the platform presents confirmation dialogs, allowing the user to review and potentially undo their decision, thus preventing irreversible errors and providing a sense of control over the actions performed.

4) Consistency and standards: The application adopts industry-standardized iconography for common functions such as menu, search, save, and delete, ensuring a consistent user experience and reducing the learning curve by aligning with universal interface design conventions.

5) Recognition rather than recall: The system utilizes tooltips (contextual aids) and displays the current status of each analysis, providing relevant information without the user having to remember specific details, thereby reducing cognitive load (Fig. 4).

6) Flexibility and efficiency of use: The platform offers a home panel that allows parents to quickly view their children's latest cyberbullying alerts, including a line graph that shows the temporal evolution of the alerts, facilitating efficient identification of patterns and trends to avoid input errors, optimizing process efficiency and reducing user frustration (Fig. 6).

7) Aesthetic and minimalist design: The platform's design is minimalist, utilizing a reduced color palette and presenting concise information, minimizing visual distraction and improving comprehension.

8) Error prevention: Real-time validation messages are implemented in each form field, proactively guiding the user and focus, especially for parents with limited technology experience. (Fig. 9).

9) Help users recognize, diagnose, and recover from errors: Specific error messages are implemented, such as notification of an already registered email (Fig. 3), and it is clearly indicated when an analysis fails, prompting the user to take corrective actions like a new analysis (Fig. 5). The dynamic field validation and floating messages also justify this heuristic.

10) Help and documentation: The application provides a link to the terms and conditions to inform users and has incorporated a tutorials section that explains the application's operation and educates about the issue of cyberbullying, thus aligning the functionality with the platform's preventive mission.

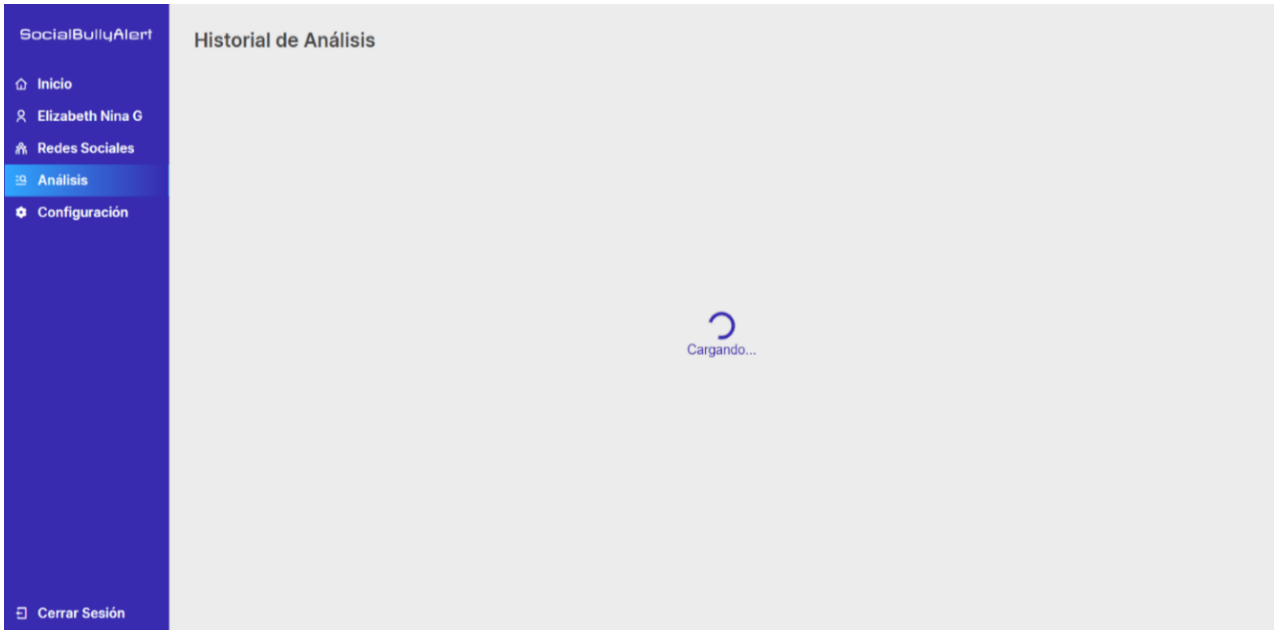

Fig. 2. Animation indicating process loading on the platform (In Spanish).

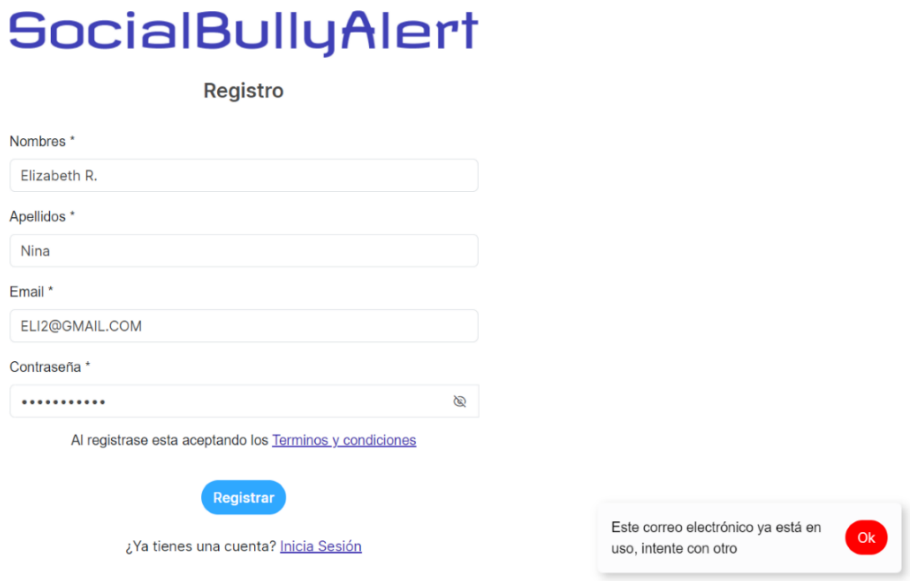

Fig. 3. Floating message specifying error on the platform (In Spanish).

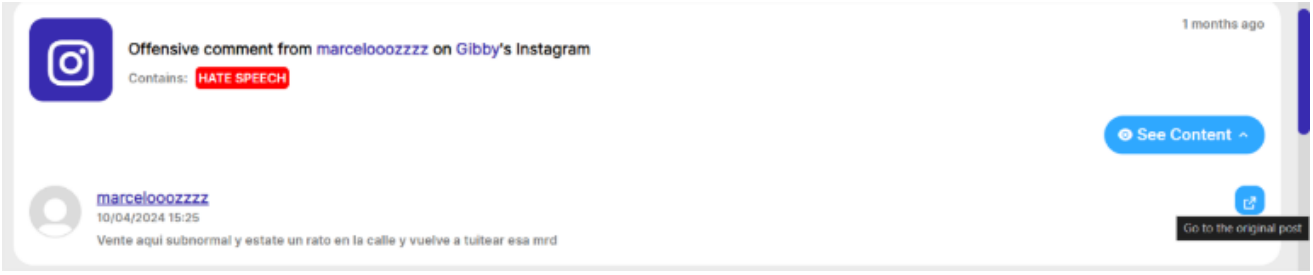

Fig. 4. Content of a hate speech alert.

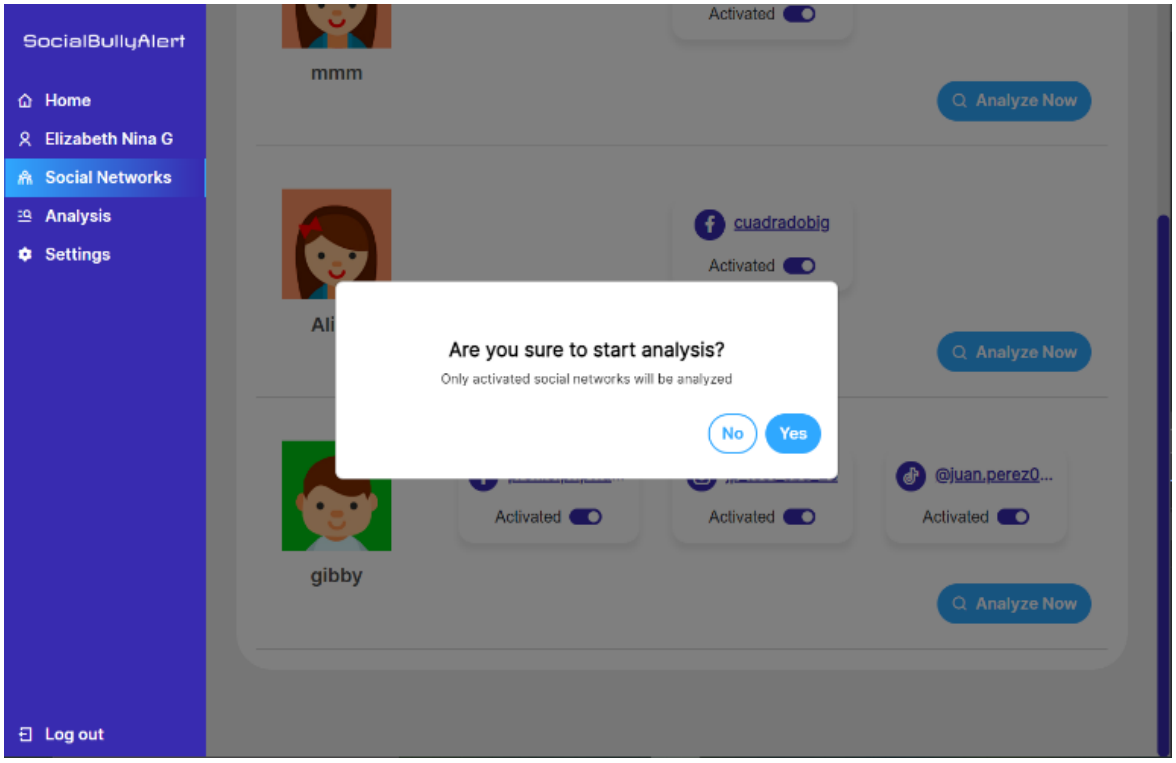

Fig. 5. Confirmation dialogue to start an analysis.

Fig. 6. Home section including alert graph and parental advice.

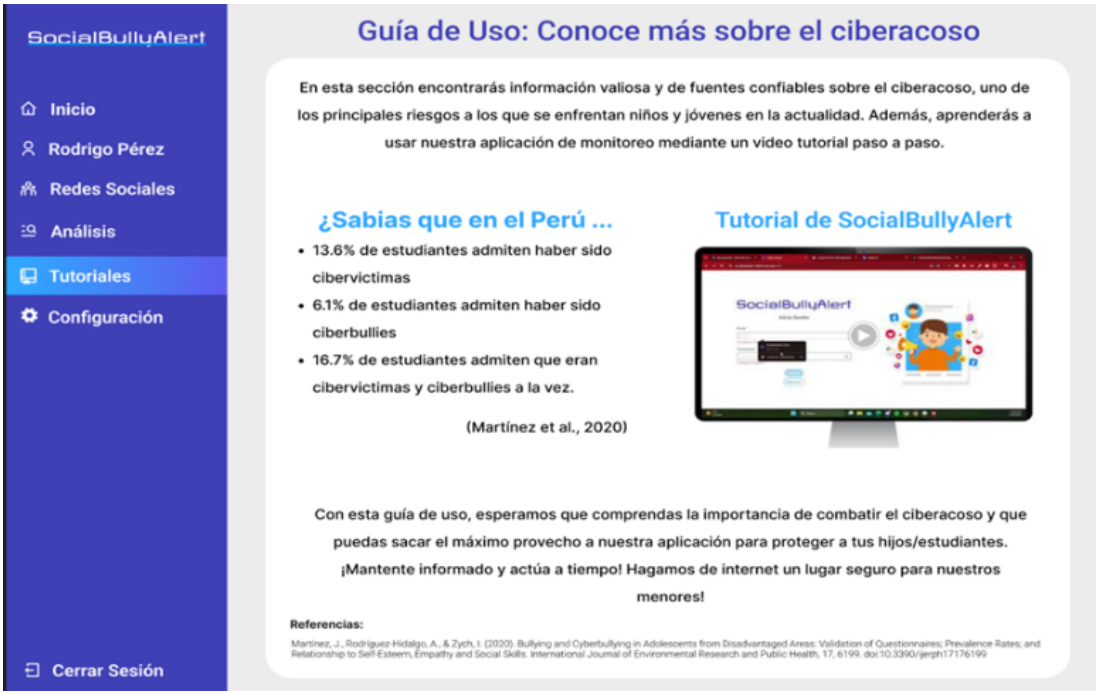

Fig. 7. Tutorials section on the platform (In Spanish).

Fig. 8. History of all analyses performed (In Spanish).

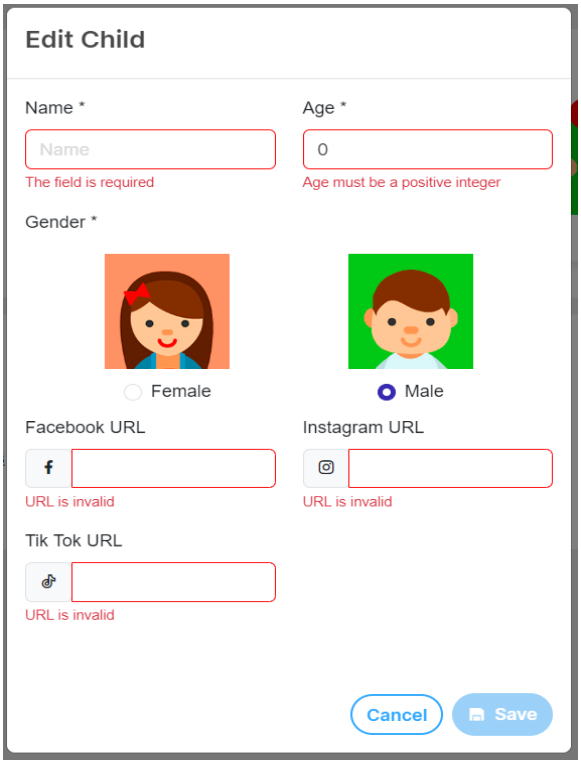

Fig. 9. Child registration form with validation error messages.

IV. Application Features

The monitoring platform offers a comprehensive suite of features designed to provide parents with greater control and visibility over online activities that may pose a danger to their children. These are the key features:

A. Management of Minors' Social Networks to Monitor

This feature allows parents to register on the platform and indicate the children and social networks they wish to monitor. Parents can edit their children's information to keep it up-to-date, as well as add or remove social networks from monitoring as needed. It also allows "activating" and "deactivating" to decide whether or not to include them in the analyses without having to permanently remove the networks from the platform.

B. Analysis and Details of Cyberbullying Alerts

Once monitoring is set up, parents can initiate an analysis of their children's social networks to detect possible cases of cyberbullying. Only social networks with an "Activated" status will be analyzed, and the analysis will take a maximum of approximately five minutes. When the analysis is completed, a summary of the analysis can be viewed. If comments or posts with cyberbullying content are found, the number of hate speech, offensive language, and inappropriate image alerts will be displayed. The number of interactions the child has on each social network and a list of problematic users will also be shown so that the parent can quickly identify potential bullies. If the parent wants to explicitly view the offensive content that generated each alert, they can do so discreetly and view the uncensored image or text, as well as access the bully's profile and the original post where the bullying occurred.

C. Summary of Alerts and Parental Advice

The platform provides personalized parental advice based on the situation reflected on each child's social networks according to the latest alerts received. A line graph can also be viewed, which presents the number of alerts over time for a child in an easier manner. In this way, the "Home" section is a quick access to know the situation of each child.

V. Experimental Evaluation

The evaluation of SocialBullyAlert's effectiveness and usability involved a two-pronged approach: expert validation and user experience surveys. For the expert validation, in-depth interviews were conducted with a group of professionals including teachers, principals, and psychologists, all of whom possessed extensive experience in managing cyberbullying cases involving minors. These interviews aimed to gather qualitative feedback on the accuracy and relevance of the system's alerts, as well as to solicit suggestions for enhancing the presentation and content of information provided to parents.

To assess user experience, a qualitative evaluation was carried out with end-users. Twenty parents from public schools in Lima were given the opportunity to interact with the application. The evaluation employed a previously validated questionnaire, the User Experience Questionnaire (UEQ) extracted from the article [19], which has been widely used in related research to gauge user perspectives. This questionnaire comprises 26 items, each rated on a scale from 1 to 7, designed to provide comprehensive insights into various aspects of user experience.

VI. Results

The expert validation yielded several key insights. Unanimously, the experts agreed that the proposed web

solution has the potential to reduce cyberbullying and enhance parent-child relationships, provided it is implemented correctly. They emphasized the importance of considering accessibility for parents with limited internet access. Opinions diverged regarding potential negative effects of monitoring on minors' psychological and social development, with some experts advocating for open dialogue to mitigate concerns. The experts identified critical risk factors to monitor, including cyberbullying, inappropriate content, hate speech, fake profiles, and excessive usage time. Generally, they deemed the privacy and security aspects appropriate, given the protective intent of the tool. Experts also believed that most parents would adapt well to consistent use of the solution, given the pressing need for child monitoring tools in digital environments.

Based on expert recommendations, several enhancements were incorporated, including an informative section featuring theories and data from reliable sources, and an explanatory video demonstrating the platform's functionality in an easily comprehensible manner. Other suggestions, such as adding psychoeducational components and creating usage tutorials, were noted for future development (Fig. 7).

The user experience surveys, visualized in Fig. 10, revealed that parents found the solution attractive, efficient, and innovative. These results affirm that the objective of creating an intuitive and appealing platform for parents was successfully achieved. The positive user feedback, combined with constructive input from experts, indicates that SocialBullyAlert shows promise as an effective tool in combating cyberbullying and facilitating safer digital experiences for minors.

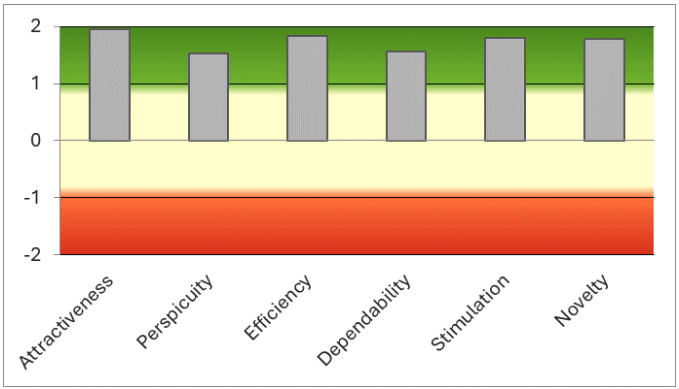

Fig. 10. Bar chart based on usability characteristics.

VII. Discussion

Key limitations include differences in cyberbullying regulations across countries, which may affect the implementation and effectiveness of the proposed solutions [9, 10]. Additionally, variability in parents' educational levels may hinder their adoption and understanding of AI-based parental control tools [11]. Another significant limitation is the need for constant model updating to identify new slangs, idioms, and forms of cyberbullying [12], as well as expanding coverage to other data formats such as videos [11, 13]. These challenges underscore the importance of future research addressing the adaptability and cultural sensitivity of technological solutions to combat cyberbullying in diversified digital environments [5, 13].

VIII. Conclusion

The study highlights the importance of continuous adaptability in the fight against cyberbullying, demonstrating the effectiveness of artificial intelligence models and neural networks in detecting offensive content on platforms like Twitter. The contributions of this work include the presentation of innovative models that represent significant advances in the detection and prevention of online cyberbullying. The implications of this research are reflected in the relevance of considering accessibility and usability for parents when implementing parental control solutions, which can have a positive impact on protecting children and adolescents in digital environments. Finally, this study underscores the importance of continuing to develop effective and culturally sensitive tools to address cyberbullying and its negative impacts on today's society.

IX. Future Work

Future work will focus on enhancing SocialBullyAlert's adaptability to emerging forms of cyberbullying and linguistic diversity. The platform should be continuously updated to recognize and respond to new slangs, idioms, and evolving forms of online harassment as they emerge. This adaptive capability is crucial for maintaining the effectiveness of the cyberbullying detection system in a rapidly changing digital landscape. While the current model is effective in detecting cyberbullying in English and various Spanish dialects, efforts should be made to incorporate more languages and cultural contexts. This expansion would not only increase the global applicability of SocialBullyAlert but also address the challenges posed by diverse linguistic expressions of cyberbullying across different cultures and regions.

References

[1] Kwan, K. Dickson, M. Richardson, W. MacDowall, H. Burchett, C. Stansfield, G. Brunton, K. Sutcliffe, and J. Thomas, "Cyberbullying and Children and Young People's Mental Health: A Systematic Map of Systematic Reviews," Cyberpsychology, Behavior, and Social Networking, vol. 23, no. 2, pp. 72–82, Feb. 2020, doi: 10.1089/cyber.2019.0370.

[2] G. Catone, V. P. Senese, S. Pisano, M. Siciliano, K. Russo, P. Muratori, R. Marotta, A. Pascotto, and M. R. Broome, "The drawbacks of Information and Communication Technologies: Interplay and psychopathological risk of nomophobia and cyber-bullying, results from the bullying and youth mental health Naples study (BYMHNS)," Computers in Human Behavior, vol. 113, p. 106496, Dec. 2020, doi: 10.1016/J.CHB.2020.106496.

[3] C. Maurya, T. Muhammad, P. Dhillon, and P. Maurya, "The effects of cyberbullying victimization on depression and suicidal ideation among adolescents and young adults: a three year cohort study from India," BMC Psychiatry, vol. 22, no. 1, Dec. 2022, doi: 10.1186/s12888-022-04238-x.

[4] J. Martínez, A. Rodríguez-Hidalgo, and I. Zych, "Bullying and Cyberbullying in Adolescents from Disadvantaged Areas: Validation of Questionnaires; Prevalence Rates; and Relationship to Self-Esteem, Empathy and Social Skills," International Journal of Environmental Research and Public Health, vol. 17, no. 17, p. 6199, Aug. 2020, doi: 10.3390/ijerph17176199.

[5] P. Cedillo, A. Bermeo, A. Betancourth, F. Espinosa, L. Illescas, and J. Jadán, "A Systematic Literature Review on Technological Solutions to Fight Bullying and Cyberbullying in Academic Environments," in International Conference on Computer Supported Education, 2022, vol. 1, pp. 413–420, doi: 10.5220/0011091800003182.

[6] M. Zampieri, T. Ranasinghe, D. Sarkar, and A. Ororbia, "Offensive language identification with multi-task learning," Journal of Intelligent Information Systems, Feb. 2023, doi: 10.1007/s10844-023-00787-z.

[7] I. Mollas, Z. Chrysopoulou, S. Karlos, and G. Tsoumakas, "ETHOS: a multi-label hate speech detection dataset," Complex and Intelligent Systems, vol. 8, no. 6, pp. 4663–4678, Dec. 2022, doi: 10.1007/s40747-021-00608-2.

[8] R. Sangeethapriya and J. Akilandeswari, "Classification of cyberbullying messages using text, image and audio in social networks: a deep learning approach," Multimed Tools Appl, vol. 83, pp. 2237–2266, 2024, doi: 10.1007/s11042-023-15538-z.

[9] D. Van Bruwaene, Q. Huang, and D. Inkpen, "A multi-platform dataset for detecting cyberbullying in social media," Language Resources and Evaluation, vol. 54, no. 4, pp. 851–874, Dec. 2020, doi: 10.1007/s10579-020-09488-3.

[10] N. Yuvaraj, V. Chang, B. Gobinathan, A. Pinagapani, S. Kannan, G. Dhiman, and A. Raja, "Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification," Computers and Electrical Engineering, vol. 29, p. 107186, Sep. 2021, doi: 10.1016/j.compeleceng.2021.107186.

[11] A. Kumar and N. Sachdeva, "Multimodal cyberbullying detection using capsule network with dynamic routing and deep convolutional neural network," Multimedia Systems, vol. 28, pp. 2043–2052, 2022, doi: 10.1007/s00530-020-00747-5.

[12] J. Salminen, M. Hopf, S. A. Chowdhury, S. Jung, H. Almerekhi, and B. J. Jansen, "Developing an online hate classifier for multiple social media platforms," Human-Centric Computing and Information Sciences, vol. 10, no. 1, Dec. 2020, doi: 10.1186/s13673-019-0205-6.

[13] V. L. Paruchuri and P. Rajesh, "CyberNet: a hybrid deep CNN with N-gram feature selection for cyberbullying detection in online social networks," Evolutionary Intelligence, Apr. 2022, doi: 10.1007/s12065-022-00774-3.

[14] Apify, "Apify: Web Scraping, Data Extraction and Web Automation in the Cloud," Apify.com. [Online]. Available: https://apify.com/. [Accessed: 11-Jun-2024].

[15] Google Cloud, "Visión de Cloud: Documentación | Cloud Vision API | Google Cloud," Cloud.google.com. [Online]. Available: https://cloud.google.com/vision/docs?hl=es-419. [Accessed: 11-Jun-2024].

[16] Google Cloud, "Características | Visión de Cloud | Google Cloud," Cloud.google.com. [Online]. Available: https://cloud.google.com/vision/docs/features-list?hl=es-419. [Accessed: 11-Jun-2024].

[17] Angular, "Angular," Angular.dev. [Online]. Available: https://angular.dev/overview. [Accessed: 11-Jun-2024].

[18] J. Nielsen, "10 Usability Heuristics for User Interface Design," Nielsen Norman Group, 24-Apr-1994. [Online]. Available: https://www.nngroup.com/articles/ten-usability-heuristics/. [Accessed: 11-Jun-2024].

[19] B. Laugwitz, T. Held, and M. Schrepp, "Construction and evaluation of a user experience questionnaire," in HCI and Usability for Education and Work, 2008, pp. 63–76, doi: 10.1007/978-3-540-89350-9_6.