Preventing Cyberbullying on Social Networks with Spanish Parental Control NLP System

Gabriel A. León-Paredes[1], Omar G. Bravo-Quezada[2], Pedro P. Bermeo-Aguaysa[3]
María J. Peláez-Currillo[4] and Ledys L. Jiménez-González[5]
Universidad Politécnica Salesiana, Cuenca, Ecuador[1,2,3,4]
Universidad Bolivariana del Ecuador, Durán, Ecuador[5]

Abstract*—The boom in social networks and digital communication has given place to innovative forms of social interaction. However, it has also made possible new forms of harassment of others anonymously and without repercussions. Such is the case of cyberbullying, an increasingly common problem, especially among young people. Its effects on individuals can be devastating, ranging from anxiety and depression to social isolation and low self-esteem. Furthermore, there is a wide variety of applications called parental control, which allow parents to show, the pages the child or adolescent has accessed, know how often the child or adolescent accesses them, and control the time spent on social networks or other entertainment platforms. Therefore, the present research aimed to analyze, design, and implement an intelligent application based on data mining algorithms and the Latent Semantic Analysis (LSA) method for the presumed detection of cyberbullying in social networks in adolescents. The methodological process of the study was carried out following the fundamentals of applied research with a qualitative-quantitative descriptive, and cross-sectional approach. As a result, a multi-platform application was obtained that alerts about suspected bullying to parents or guardians. For the validation of the application, the technique of expert judgment was applied. Also, the process of obtaining negative and positive text similarity was performed based on cosine similarity. In the analysis of Twitter accounts, values of 46% with negative texts and 6.71% with positive texts are obtained, which allows inferring that this is a presumed case of cyberbullying in this account.

Keywords*—*Cyberbullying; control parental system; natural language processing; Spanish cyberbullying prevention system

I. Introduction

Social networks have transformed the way people communicate and interact with each other, and have made it possible to instantly connect with people all over the world. Undoubtedly, the era of digital transformation has created new opportunities in various areas of society; for education, commerce, and culture, and has allowed people to connect and share ideas in ways never before imagined. In this sense, it is valid to say that there are many satisfactions experienced by users of digital media with the advancement of technologies, although positive experiences do not always occur given the appearance of malicious users that cause negative effects on people. Among these negative effects is cyberbullying on social networks; an increasingly common problem. It refers to bullying, harassment, intimidation, and other forms of aggressive behavior that take place online through social networks and other digital platforms. The effects of cyberbullying can be devastating, from anxiety and depression to social isolation and low self-esteem [1].

Today, everyone can be a victim of cyberbullying, but young people are more vulnerable [2] for example, adolescents are more likely than adults to spend extended time online and be more involved in social networks. This means they have greater opportunities to interact with other users, including people who may have bad intentions. Also, young people often lack the emotional maturity and experience to deal with cyberbullying situations [3]. Often, they may feel embarrassed or scared to talk to someone about bullying, which can make the situation worse. In addition, they are more likely to make impulsive or risky decisions in online situations, which may increase their vulnerability to victimization in digital media.

Another factor contributing to young people's vulnerability to cyberbullying is the lack of adult supervision. Parents often do not have a full understanding of online platforms and the social interactions their children have with them, which can make it more difficult for them to detect signs of cyberbullying or to intervene before situations become serious [4]. Also, it should be considered that many of these young people use these platforms as their primary means of communication and socialization. However, they are unprepared to deal with cyberbullying, feeling alone and isolated if they do not have the support of their parents and friends. Therefore, cyberbullying can have a very negative impact on the social and emotional lives of adolescents.

As a serious problem that can lead to significant emotional and psychological consequences, parents should rely on technological advances to limit the exposure of adolescents to inappropriate content. It is important to note that these consequences are not exhaustive, as the experience of each victim of cyberbullying may be different. However, their impact underscores the importance of creating strategies to prevent and address bullying in any space. In this sense, the study carried out by the Ministry of Education of Ecuador with World Vision and UNICEF, in which 5,511 students from 126 institutions were consulted, states that in Ecuador 6 out of 10 students have been victims of bullying and the use of social networks. The students surveyed state that they have been victims of the dissemination of messages; in some cases to reveal private conversations and in other cases to generate threats by anonymous users [5].

School violence has been silenced, not because it has been solved, but because it now occurs in digital scenarios, which has generated new terms to be taken into account by adults, such as the well-known cyberbullying, a form of harassment based on the use of Information and Communication Technologies (ICTs) [6], [7]. In addition to social networks, it occurs in message-sharing platforms, video games, and blogs, among others [8]. Therefore, the diversification of online environments makes it difficult for adults to monitor them. This happens, first, because most parents are not tech-savvy. Secondly, because parents or guardians do not have enough time to carry out a constant review of the new media; and, thirdly, in many cases young people keep this type of situation secret. By the above, adults have been forced to adapt digitally in a fast way to the new generations to carry out adequate supervision [9].

In this sense, technological progress has allowed the development of intervention alternatives that facilitate parental control processes. Parental control systems are nowadays a viable alternative for parental intervention in the protection of adolescents from bullying on social networks. Likewise, it can help identify and prevent bullying situations, providing parents with the ability to monitor and control the use of digital environments and prevent cyberbullying [10]. However, these apps generally offer features such as monitoring browsing history, blocking inappropriate websites, monitoring messages and phone calls, and setting time limits for device use [10]. Hence, there is limited research related to parental performance in the mechanisms of prevention and intervention in the face of cyberbullying [11].

Among the limitations of existing applications is that they do not focus on analyzing the activities that adolescents carry out on their social networks to determine whether any action taken against an adolescent is alleged cyberbullying [12]. In this regard, [6] argues that the use of Natural Language Processing (NLP), as a branch of Artificial Intelligence (AI), in applications for parental control, is part of the technological innovation of recent times in the field of online protection. Among its potentialities is the ability to understand and process human language with high levels of similarity to that of people. Over the last few years, it has been applied in social network analysis to identify topics, sentiments, and other characteristics of natural text [13]. In addition, it contains a variety of tools and techniques to extract valuable information in large volumes of texts, identify trends, and determine opinion patterns, preferences, and user behaviors [14]. These techniques find functionality through the creation of algorithms that allow the analysis of specific information and obtaining accurate results in real-time [15]. One such tool is the Latent Semantic Analysis (LSA) method, which uses mathematical and statistical techniques to create a numerical representation of words and documents in a corpus. This numerical representation allows patterns to be identified in the way words are used in different documents and how they are related to each other [16], [17].

Despite its innumerable advantages, the documentary review evidences a limited availability of NLP applications developed to detect cyberbullying in the Spanish language. Likewise, NLP uses the LSA method for the identification of semantic patterns and relationships in sets of texts. Although the usefulness of LSA has been demonstrated in different NLP applications and has significant contributions in language pattern identification, topic detection, sentiment analysis, and language variant detection; its use in cyberbullying detection applications in social networks is also limited. According to [18], LSA is useful in a wide variety of applications, because of its ability for information retrieval, automatic document classification, topic clustering, and content recommendation. In addition, it is used in the construction of search engines to identify relevant information in large text datasets.

Attention to such, this paper presents the results of the research developed to analyze, design, and implement an application based on NLP for the prevention of presumptive cyberbullying in the social networks of Ecuadorian adolescents. As a contribution, a multiplatform application for parental control based on NLP in Spanish and using the Latent Semantic Analysis method is presented. The proposal responds to the need to protect Spanish-speaking adolescents from online cyberbullying and the scarce production of solutions based on these technologies in Spanish. Taking advantage of the potential of NLP and semantic analysis made it possible to develop an effective tool to detect and prevent cyberbullying in the linguistic and cultural context of the Spanish language, giving parents and guardians the ability to protect adolescents in digital environments.

To effectively communicate the findings and contributions of the study on the multiplatform application of parental control through Natural Language Processing in the Spanish language. This paper is organized as follows. In Section II, we present some studies related to the use of information and communication technologies for the detection and prevention of cyberbullying, highlighting the limitations of the most recent studies. Section III, outlines the methodological components of the research, as well as the phases guiding the development of the Intelligent Parental Control System. In the Results Section IV, the data obtained in the implementation of the mobile and web applications are detailed. In the Discussion Section V, the results are interpreted in a broad context of cyberbullying in social networks, comparing the results of related works with the challenges for the practical implementation of the designed application. Finally, in Section VI, conclusions derived from the study are presented, highlighting the contributions of the NLP-based application in Spanish for the prevention of presumptive cyberbullying in the social networks of adolescents.

II. Related Works

The following are the results of the main research developed to prevent cyberbullying using advances in Information and Communication Technologies.

Researchers from the National University of the USA developed the SafeGuard Web application, intending to detect dangerous situations in educational institutions based on social networks [19]. By constantly monitoring publications on social networks, SafeGuard determines the relationship of the language users use with pre-established keywords such as suicide, death, violence, and so on. When these terms are identified, the application sends alert messages to the system administration, thus protecting potential victims from any emotional or physical harm. SafeGuard's configuration employs web technologies with hosting in the cloud environment, allowing login from any location. In terms of operation, SafeGuard employs IP address-based access restrictions for client login over the network and uses a JSON Web token with expiration times. To respond to client requests, the application uses the HTTPS protocol. The results of its implementation show the application's ability to detect cyberbullying, threats, or distress situations through the configuration of monitors or keywords. However, it requires adding weighting factors to the monitors that favor the search for particular keywords by the weighting assigned to them.

The authors of the study [20] analyzed the increase in cyberbullying over the last 15 years, and came up with BullyScan. It is a novel framework based on natural language processing and machine learning with the ability to identify online bullying automatically with high accuracy and efficiency. The application employs a logistic regression algorithm developed from the validation and testing of five different machine-learning models with the combination of three datasets of cyberbullying and/or hate speech. The tests conducted demonstrated 92% accuracy in detecting cyberbullying in real time, evidencing the ability to significantly reduce cyberbullying rates and increase positivity on social networks, as well as prevent the consequences of cyberbullying.

On the other hand, [21] proposes a system that employs PLN and machine learning to detect bullying related to messages in digital environments in the English language. For the research, 1651 tweets were collected and applied to a PLN approach to identify the most offensive terms related to cyberbullying. Using the obtained dataset, Random Forest (RF) and Support Vector Machine (SVM) algorithms were trained. The former outperforms the latter with an accuracy of 98.5%. The analysis of the results was performed using the Root Mean Square Error (RMSE) and the Mean Square Error (MSE). The RF algorithm scored better than the SVM. The results show the existence of cyberbullying and the need to address it immediately.

Similarly, the authors [22], agree that cyberbullying is an extremely prevalent issue at the moment; as access to social platforms increases, messages of hate, toxicity, and cyberbullying. In this sense, it is fundamental to generate mechanisms that guarantee the security of social networks and that any form of violence or hate crime can be automatically detected. Based on this, they proposed the analysis of cyberbullying through natural language processing employing the compression of the use of slang in social networks. As a result of their research, they achieved greater accuracy in identifying online harassment situations through experiments with multiple models such as Bi-LSTM, GloVe, and BERT and the application of the unique processing technique for the incorporation of an abusive corpus of slang. The model demonstrates greater effectiveness than models that do not contain slang preprocessing.

In a more comprehensive perspective, [23] developed an NLP tool that uses the social network Twitter as a basis for the extraction of information related to cyberbullying. The methodological procedure followed consisted of analyzing a set of tweets with the SARNA technique and classifying them based on their content as cyberbullying or neutral. The authors created a labeling system for people to classify the tweets using a reliability scale from 1 to 4, where ratings 1 and 2 indicate that they are non-cyberbullying tweets, while 3 and 4 refer to tweets with cyberbullying content. For the classification process, the BERT model was used, which was trained to identify aggressive, toxic, or threatening comments with label 1 and neutral comments with label 0. The results obtained demonstrate the importance of providing an adequate knowledge base, training the supervised learning model, and conducting case studies to accurately detect cyberbullying using NLP techniques; nevertheless, the authors do not detail the data obtained during the process.

In the same context, the Salesian Polytechnic University has promoted the development of applications that contribute to the reduction of the effects of this problem. The authors in [6], which some authors are also authors of this paper have deployed a Cyberbullying Prevention System (CPS) in Spanish based on Natural Language Processing and the use of Machine Learning techniques such as Naive Bayes, Support Vector Machine, and Logistic Regression. As in the previously mentioned research, the social network Twitter was used for the extraction of the database or corpus. As for the training process, it consisted of the use of precision metrics, and corpus sizes with variability. The level of accuracy of the SPC system was validated with the application in three case studies, obtaining a 93% of reliability.

Furthermore, according to [24] most of the research developed to detect bullying on social network platforms is based on machine learning models that use datasets extracted from individual social networks. Therefore, they have proposed a cross-platform data system that uses text collected from posts made on seven social networks. They propose an annotation system composed of a series of stages and techniques to identify posts and hashtags through crowdsourcing, and then identify posts that require annotation through machine learning methods. The advantage of the presented model lies in the possibility of cyberbullying cases and the limitation of the particular characteristics of the publications, unlike traditional methods based on post-selection and tagging. The training process of the models on the diverse dataset evidences a good performance and allows for an increase in the number of positive examples with the same amount of resources and the applicability of the models in different media.

Thus, although research related to cyberbullying has advanced in recent years, there are still great challenges to be faced. Among these challenges is the need to address the issue in a standardized manner [25] and the generation of applications that consider the linguistic and cultural context in the automatic detection of situations related to cyberbullying. In addition, the aforementioned related works differ from our proposal, since to our knowledge and according to the analysis of the state of the art, there are no applications proposed at the international and even more at a local level that use the Latent Semantic Analysis method for the detection and prevention of cyberbullying in social networks. In Table I, we present a comparative analysis of the cyberbullying detection studies presented before and we have included the present research.

III. Parental Control Multiplatform System for the Prevention of Cyberbullying

The methodological framework followed for this research was based on the principles of applied research whose purpose is to contribute to the solution of society's problems through the application of knowledge and tools of a specific scientific discipline. In this sense, the research is focused on the (a) design and (b) implementation of a multiplatform system based on Natural Language Processing for the prevention of pre-

TABLE I. COMPARATIVE ANALYSIS OF CYBERBULLYING DETECTION STUDIES HIGHLIGHTING METHODOLOGIES, KEY FEATURES, OUTCOMES, AND UNIQUE CONTRIBUTIONS OF EACH STUDY, INCLUDING THE PRESENT RESEARCH

Study	Methodology	Key Features	Outcomes/Accuracy	Unique Contributions
SafeGuard (Wyne, 2021)	Web application, keyword monitoring	Cloud hosting, IP address restrictions, HTTPS protocol	Effective in detecting cyberbullying via keyword monitoring	Focus on educational institutions, requires keyword weighting
BullyScan (Shrimali, 2022)	NLP & ML, Logistic Regression	Combination of three datasets, real-time detection	92% accuracy	High accuracy and efficiency in real-time detection
Afrifa et al. (2022)	NLP & ML, RF and SVM algorithms	Analysis of 1651 tweets, RMSE and MSE evaluation	98.5% accuracy with RF algorithm	High accuracy, focus on English language messages
Bhatia et al. (2022)	NLP, Bi-LSTM, GloVe, BERT	Slang preprocessing, abusive corpus analysis	High accuracy in identifying online harassment	Effectiveness in slang and abusive language detection
Soto et al. (2022)	NLP, BERT model	SARNA technique, labeling system for tweets	Not detailed	Importance of adequate knowledge base and training
CPS (Leon Paredes, 2019)	NLP & ML, Naive Bayes, SVM, Logistic Regression	Twitter data extraction, precision metrics	93% reliability	Focus on Spanish language, high reliability
Van et al. (2020)	Cross-platform data system, ML	Posts from seven social networks, crowdsourcing annotation	Good performance	Cross-platform applicability, diverse dataset
Present study	NLP & LSA, cosine similarity analysis	Focus on Spanish language, multiplatform application, analysis of Facebook, Ask.fm, and Twitter	46% with negative texts and 6.71% with positive texts	Unique use of LSA for cyberbullying detection in Spanish

sumptive cyberbullying in the social networks of adolescents focused in the city of Cuenca - Ecuador.

On the one hand, we detail some important points related to the (a) design of the Parental Control Multiplatform System for the Prevention of Cyberbullying based on NLP. To implement an accurate design, we need to know how young people (students between 18 and 24 years old) of the Salesian Polytechnic University use digital media to determine the main problems of cyberbullying in social networks in our local context. Hence, a structured survey called "Survey of Safety and Cyberbullying in Social Networks" was applied. The survey consisted of 20 items with dichotomous and polytomous response options. The instrument with the questions was applied to 133 students enrolled in the Computer Science program. The size of the probabilistic sample was defined considering Eq. (1) for a finite population. The total population was 5,576 on-campus students from all UPS courses. The procedure for the selection of the sample is indicated below,

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2} \tag{1}$$

where, *n*, is equal to the size of the sample; *N*, is equal to the size of the population; σ, is equal to the standard deviation of the population, when a value is not available the constant value of 0.5 is used; *Z*, is obtained by confidence levels, in case of not having a value 95% of confidence is placed and this is equivalent to 1.96 (it is the one commonly used); *e*, is equal to the acceptable limit of the sampling error, when a value is not available a range from 1% (0.01) and 9% (0.09) is used, this value depends on the interviewer.

The process of tabulating the results obtained through the survey was crucial within the methodology proposed for the design of the Parental Control Multiplatform System, so we highlight the most important results below. The analysis of the results shows that 88% of the participants are between 18 and 24 years of age, 86% are male, and 100% use social networks. Regarding the use of social networks by the participants, 9% stated that they use social networks to meet new people, while 37% use them for entertainment, 16% to communicate with people who live in different places, 36% to communicate with friends, family, acquaintances, among others, and only 2% responded that they use the networks for other situations such as business. The data obtained show that most of the young students surveyed use social networks to communicate with other people.

Furthermore, when participants were asked about the time they spend using social networks, 2% use social networks for less than one hour, 31% use them for one to two hours a day, 41% use them for three to four hours a day, 17% use them for five to six hours a day, 4% use them for seven to eight hours a day, and 5% use social networks for more than nine hours a day. In this sense, it is evident that most of the participants use social networks for several hours during the day. Regarding the most used social networks, 23% of the participants stated that they use WhatsApp, 22% use Facebook, 8% use Twitter, 1% use Tumblr, 23% use YouTube, 20% use Instagram, and 3% use Pinterest. Thus, the majority of the surveyed students mostly use social networks such as WhatsApp, Facebook, YouTube, and Instagram.

An important fact to be considered is that 46% of participants confirm having received cyberbullying messages. Regarding the social networks in which they have sent, known, or received messages of cyberbullying, 15% indicate WhatsApp, 38% indicate Facebook, 4% indicate Twitter, 11% indicate Instagram, 1% indicate that Snapchat, Tinder, and Badoo are social networks where this type of problem happens, 2% indicate that YouTube is the social network where messages of cyberbullying are sent, known or received, 1% indicate that in no social network this problem happens, and 27% did not respond. Thus, most of the participants who send, know, or receive cyberbullying messages have received it at least once on any of the social networks WhatsApp, Facebook, Instagram, Twitter, Snapchat, Tinder, and YouTube. Finally, it is important to highlight that 95% of participants say that if they had a computer tool to prevent and detect cyberbullying, they would use it.

Hence, based on this diagnosis, we have determined the features that the Parental Control Multiplatform System proposed in this paper should have. First, we have designed it to be used by parents, guardians, teachers, and psychologists,

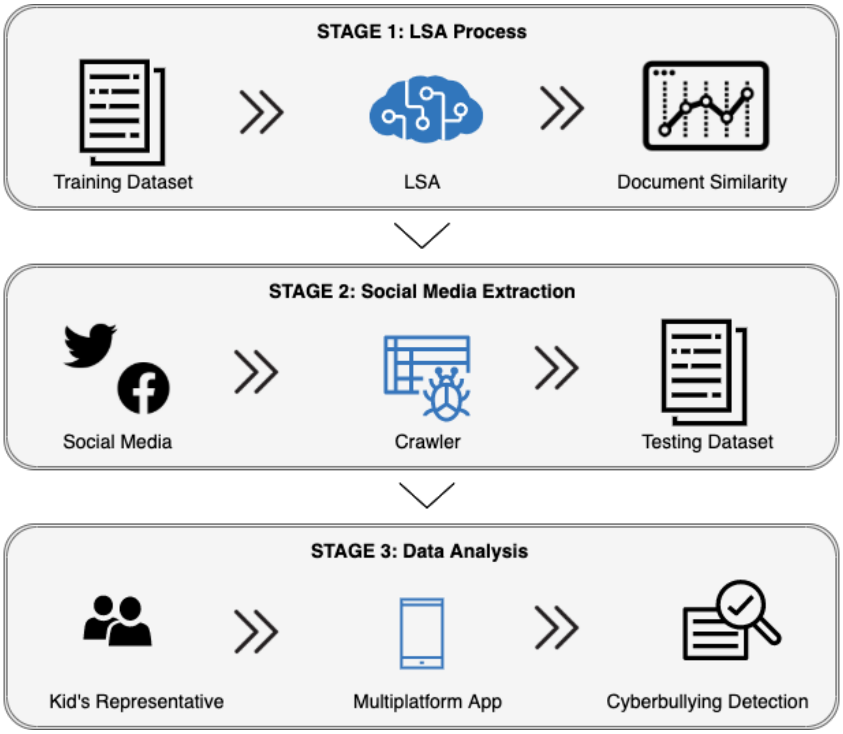


Fig. 1. Stages followed for the implementation of the parental control multiplatform system.

among others, and to be aware of the type of information that adolescents receive through social networks. We have focused on young people who have initiated using these platforms and do not have the knowledge to deal with bullying situations. Also, the Parental Control System was designed to work both in web environments and mobile devices, through the creation of a multiplatform system. It is necessary to note that, for web environments, the application has features that differ from the version for mobile devices, mainly due to the incorporation of extra functionalities.

On the other hand, we detail the (b) implementation of the Parental Control Multiplatform System based on Natural Language Processing through the Latent Semantic Analysis (LSA) method for preventing presumptive cases of cyberbullying in social networks. The system has been divided into three main stages, as shown in Fig. 1.

For the first stage of system implementation, we utilize the Latent Semantic Analysis (LSA) method, which allowed us to obtain a base training model for detecting cases of presumptive cyberbullying in several social networks. At this point, it is important to indicate that this paper is oriented to the Natural Language Processing of the Spanish language with an emphasis on social network users from Ecuador. So, we started by obtaining a Spanish dataset related to cases of cyberbullying in Ecuador. We need this specific type of dataset due to the slang used among adolescents. Thus, we worked with a dataset referred to a previous paper published by some authors of this work, as shown in the research document "*Presumptive Detection of Cyberbullying on Twitter through Natural Language Processing and Machine Learning in the Spanish Language*".

As mentioned in study [6], the dataset is compounded with a total of 960,578 tweets, of which 416,567 correspond to presumptive cyberbullying. Then, all the tweet's text data was cleaned up by using text processing techniques such as the removal of stopwords, lemmatizing, and stemming of the remaining words. After the processing of the tweet's text data, we constructed the Term-by-Document matrix, and then we reduced this matrix to 300 k dimensions by applying the Singular Value Decomposition (SVD) truncated method [26].

At this point, it is important to clarify how we used the Latent Semantic Analysis method for the presumptive detection of cyberbullying. As mentioned, we employed a dataset of 416,567 tweets with plausible cyberbullying, and 544,011 tweets with no presumptive cyberbullying to train our knowledge base. Then, each comment of a post made on the social network of the adolescent is compared against the trained dataset (cyberbullying, and no cyberbullying). Therefore, a similarity value is obtained for each trained document from the dataset versus the comment post issued on the social network. Next, these values are ordered from highest to lowest. We left with the top 10 values, to subsequently obtain a general similarity value of the comment posted on the social network by applying the following equation,

$$SimPos = \frac{\sum_{i=1}^{10} SimDoc_i}{10} \tag{2}$$

where, *SimPos* is equal to the general similarity of the comment posted on the social network, *SimDoc* is equal to the similarity obtained between each document of the trained dataset and the comment posted on the social network. Finally, the value of *SimPos* is then evaluated between the general similarity obtained of the trained dataset with presumptive cyberbullying and the trained dataset with no presumptive cyberbullying, which allows us to determine whether the comment post contains presumptive cyberbullying or not. For our case studies, if the general similarity of the trained dataset with presumptive cyberbullying is greater than the general similarity of the no presumptive cyberbullying dataset, then it can be inferred that the comment contains presumptive cyberbullying.

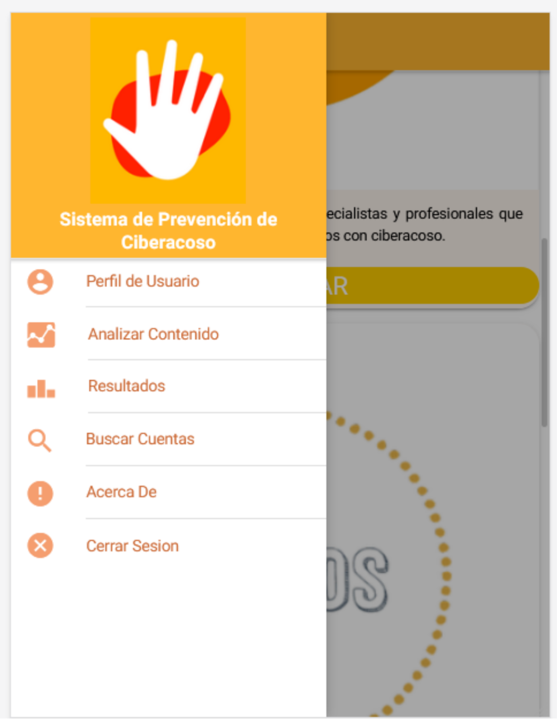
In the second stage of the implementation of the Parental Control Multiplatform System, we crawled the text data from social networks, in this case, Twitter, Facebook, and AskFM. First, the system needs the credentials of the Facebook and AskFM social network user, to extract the text interaction of its account. Thus, for these cases, we utilized frameworks, that can automate the web browser navigation throughout the execution of programming scripts. However, for the case of Twitter, we used the official API, which can permit us to extract the text tweet data of a specific user when its account is public. Hence, for this case, we don't need the user credentials, only a key API consumer of a Twitter developer account.

Moreover, the data crawled from the social network has to be extracted constantly to detect them as soon as possible the presumptive cyberbullying. Consequently, we proposed and developed automated tasks on the server side to extract the social network text data using the crawlers specified in the previous paragraph. These automated tasks can be executed hourly, daily, weekly, or monthly depending on the configuration each user makes on the system.

In the last stage, we developed the multiplatform (progressive web and mobile) system. Some of the functionalities created have been focused on registering new users, authenticating and authorizing user accounts, recovering account passwords, registering and authorizing the credentials of the adolescent's social network accounts, crawling the text data from the registered and authorized social network accounts, scheduling when the text data is extracted, and presenting the analysis results of the presumptive or not cyberbullying, as shown in Fig. 2, and 4. In addition, as part of raising awareness of the cyberbullying problem, we added some relevant documentation (articles, videos, and psychologist experts' contacts), as shown in Fig. 3.

Finally, taking into account these three phases in the implementation of the Parental Control Multiplatform System, its "normal" functionality is explained in greater detail below. Then, as a first step, the parent or guardian responsible for the child or adolescent must register as a user within the system, for which personal information such as identification number, full name, address, telephone, email, and password are requested. Next, they must go through a process of verification of their personal data, for which an email is sent to the guardian indicating the steps for activating their account in the system.

With these previous steps completed, the new user will be able to log in and then have the option of registering different social network accounts of his/her tutored. At this point, it is important to indicate that, when registering Facebook and ASK FM social network accounts, the username and password of the adolescent's account must be entered so that this information is sent to the crawlers and the text information can be extracted.

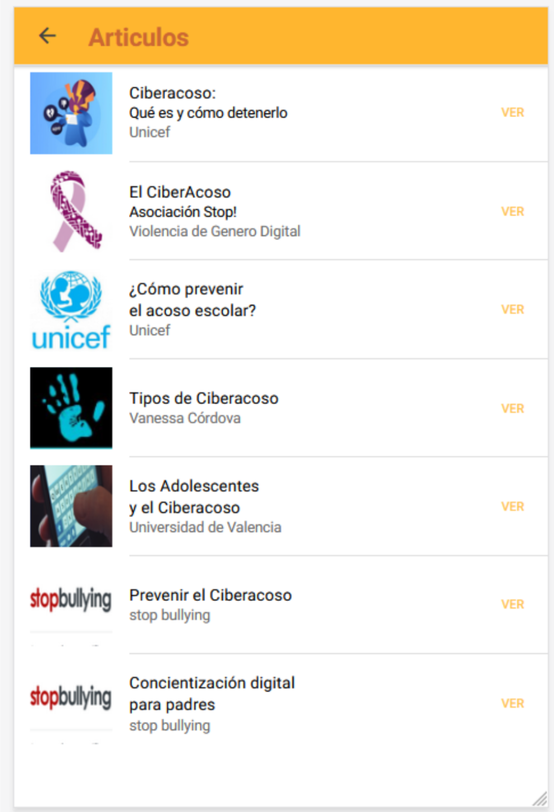


Sistema de Prevención de Ciberacoso

- Perfil de Usuario
- Analizar Contenido
- Resultados
- Buscar Cuentas
- Acerca De
- Cerrar Sesion

ecialistas y profesionales que
os con ciberacoso.

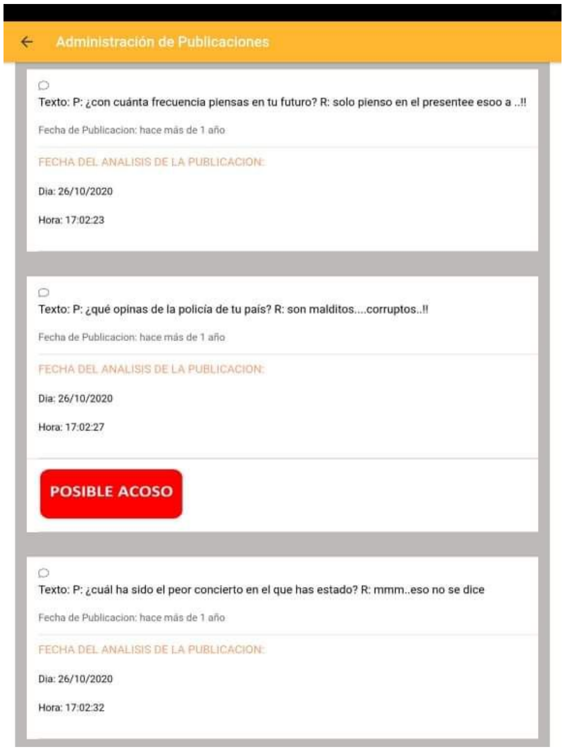
Fig. 2. Graphical user interface of the functionalities that the user of the parental control multiplatform system has access to.



Articulos

Ciberacoso: Qué es y cómo detenerlo	Unicef	VER
El CiberAcoso Asociación Stop!	Violencia de Genero Digital	VER
¿Cómo prevenir el acoso escolar?	Unicef	VER
Tipos de Ciberacoso	Vanessa Córdova	VER
Los Adolescentes y el Ciberacoso	Universidad de Valencia	VER
Prevenir el Ciberacoso	stop bullying	VER
Concientización digital para padres	stop bullying	VER

Fig. 3. Graphical user interface of the relevant documentation related to cyberbullying presented in the parental control multiplatform system.



Texto: P: ¿con cuánta frecuencia piensas en tu futuro? R: solo pienso en el presentee esoo a ..!!

Fecha de Publicacion: hace más de 1 año

FECHA DEL ANALISIS DE LA PUBLICACION:

Dia: 26/10/2020

Hora: 17:02:23

Texto: P: ¿qué opinas de la policía de tu país? R: son malditos....corruptos..!!

Fecha de Publicacion: hace más de 1 año

FECHA DEL ANALISIS DE LA PUBLICACION:

Dia: 26/10/2020

Hora: 17:02:27

Texto: P: ¿cuál ha sido el peor concierto en el que has estado? R: mmm..eso no se dice

Fecha de Publicacion: hace más de 1 año

FECHA DEL ANALISIS DE LA PUBLICACION:

Dia: 26/10/2020

Hora: 17:02:32

Fig. 4. Graphical user interface of the list of publications from the social network adolescents' accounts in the parental control multiplatform system.

Once the corresponding user and account registrations have been made, the frequency of analysis to be performed on the accounts can be configured. This analysis can be hourly, daily, weekly, or monthly and is done through automated tasks on the server side. However, there is the possibility that the user from the system can run a scan at any time. This allows the web services to be consumed to extract the information from the social networks, and subsequently analyze them. Regardless of which of the two analysis options is selected, once the system completes the analysis, a message is sent to the user's email indicating that the analysis is complete.

IV. Results

Below, we present the results of the experiments carried out with the Parental Control Multiplatform System for the prevention of presumed cases of cyberbullying.

A. Results of the Analysis of Accounts from Different Social Networks using the Latent Semantic Analysis Method

This sub-section presents the results of the analysis of social network accounts that have been specifically selected for testing and validation. The objective of these experiments is to test the performance of the LSA method. So, these selected accounts have published content considered as alleged harassment, even some accounts belonging to a well-known case in Cuenca - Ecuador, where the implicated user faced legal problems and is currently serving a sentence. On the other hand, accounts of public figures that publish messages of peace and love considered as "without harassment" have been used. The validation procedure consisted of first extracting the information from the social network accounts and then analyzing this information using the LSA method. As a final phase, the results were presented with the percentage of similarity, both in texts with presumptive cyberbullying (negative) and without presumptive cyberbullying (positive) as can be seen in Fig. 4, which shows an example of how the analysis results are presented in the Parental Control Multiplatform System. Then, for this experiment, two Twitter accounts were analyzed.

For this experiment, two Twitter accounts were analyzed. In the first account, we analyzed posts issued by a known user in the city of Cuenca - Ecuador who committed serious crimes against adolescent women, and his main communication media were social networks, where he hooked his victims, for which he faced legal problems and is currently serving a sentence. In this first account analyzed, although the total value of the similarity of "positive" texts prevailed over "negative" texts, the algorithm evidences the existence of texts with assumed cyberbullying as some examples can be seen in Table II. The analysis reveals the ability of the Parental Control Multiplatform System designed to identify terms that suggest harassment, manifested through swearing, insults, words with high levels of aggressiveness or derogatory phrases, and even threats. An example of a threat identified by the algorithm is the phrase *"a cada PUERCA le llega su carnival"*, which means in English "every PIG has its own carnival". It should be noted that in the local context, a carnival is a local holiday where families come together to eat a pig. Therefore, in this post, the user refers to his victims as animals. In this sense, the documentary review argues that it is completely normal for a social network stalker to use phrases with insinuations to threaten his victim [25]. This is because, cyberbullying can take different forms, including spreading rumors, posting humiliating comments, or direct threats, among others. The insinuations can be used as a form of psychological harassment [27], which seeks to destabilize the victim and make them feel uncomfortable or insecure.

Likewise, the phrase "When you are cold look for me", detected by the algorithm as a form of cyberbullying, might seem like an innocent offer, but it is designed to make the victim feel observed or surveilled. This is explained by the fact that in some cases, the cyberbully may use subtle or indirect language to avoid detection by security filters or by the victim's parents and guardians [28]. These insinuations may seem harmless or even flattering at first glance. Therefore, the difference between the percentage of negative and positive text is minimal. Nevertheless, the system determines that it is a threatening or intimidating message that should alert parents or guardians.

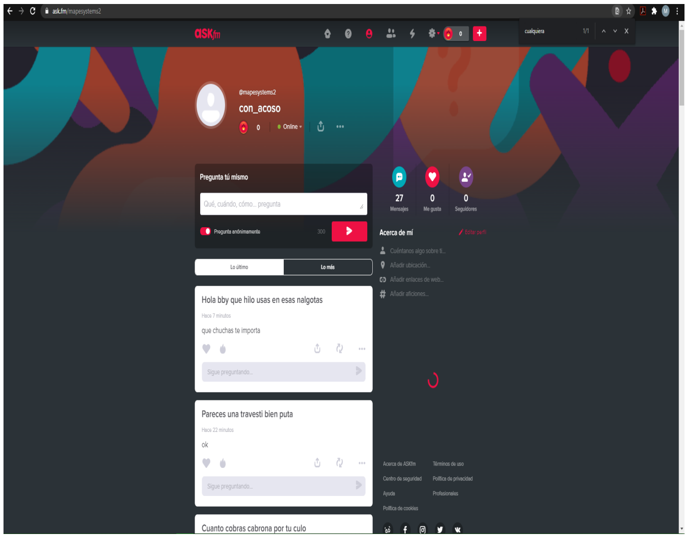
The second Twitter account analyzed was the account of Pope Francis, Supreme Pontiff of the Catholic Church; to establish a comparison of the percentages of similarity between the analyzed account with presumed cyberbullying publications and the @Pontifex_es account. As shown in Table III, the percentage of similarity of "positive" text is well above the "negative" text. This indicates that there is a minimal percentage of text linked to cyberbullying. The Parental Control Multiplatform System developed in this proposal has obtained alarms from this account on posts where terms such as "war", "weapons", "pain", and "hurt" appear. In this sense, although the main function of the LSA method is to identify patterns

TABLE II. SAMPLES OF THE RESULTS OBTAINED BY THE ALGORITHM OF THE PARENTAL CONTROL MULTIPLATFORM SYSTEM WHEN ANALYZING THE FIRST TWITTER ACCOUNT OF THE USER WHO HAS BEEN SENTENCED IN THE CITY OF CUENCA - ECUADOR FOR CRIMES WHERE SOCIAL MEDIA WAS HIS MAIN COMMUNICATION MEDIA

QUERY	% SIMILARITY NEGATIVE TEXT	% SIMILARITY POSITIVE TEXT	CYBERBULLYING?
Ustedes no son nada mas que P”t’s Del Cabaret,	35.45	11.07	Yes
Prefiero que sean p”t’s pero no mentirosas	46.59	06.71	Yes
Una zorra se merece tu ver..@,,, Una dama tu corazón!	19.17	11.30	Yes
En el cielo se guardan nuestros secretos,	29.12	51.20	No
Hasme el amor pero de tu vida,	09.31	17.25	No
Aprecia lo que la vida te da, porque no te da dos veces,,,	17.14	18.04	No
Cuando tengas frío búscame,	27.55	25.26	Yes
Aprecia lo que la vida te da, porque no te da dos veces,,,	17.14	18.04	No
Si te estorba la virginidad yo soy experto en curar esos males y estorbos,	11.16	10.79	Yes
A cada PUERCA le llega su Carnaval	14.97	8.11	Yes
Lo que aprendí de Mario Bross es que mientras mas moneditas tengas, es más fácil llegar a la princesa,	13.00	17.53	No
No confío en tus palabras, que se las lleve el viento muy lejos del lugar en el que yo me encuentre,	07.18	09.94	No
Tienes que saber diferenciar para que te quería, para amarte o solo para TIRARTE, Y siempre fuiste lo SEGUNDO,,,	30.55	42.61	No

and semantic relationships between words and documents in a text corpus, it is important to keep in mind that latent semantic analysis is not always able to capture the full context and emotional connotations of a text [16], [17]. Therefore, it becomes necessary to critically read the analysis and consider the full context before drawing conclusions.

Another experiment conducted in this research was with the Ask.fm social network, a question-and-answer-based social platform that allows users to interact anonymously or in an identity-based mode. This platform was launched in 2010 and has become very popular among teenagers and young adults as a way to ask funny, curious, or personal questions to friends and strangers. To validate the algorithm of the Parental Control Multiplatform System, two Ask.fm accounts were created. The first account created has username *mapesystems2*, and is an account that has been created to disseminate messages with pretended harassment, as can be seen in Fig. 5. In this account, the total similarity value of “negative” texts was well above the similarity of “positive” texts, which evidences a large number of texts with presumptive cyberbullying.



Hola bby que hilo usas en esas nalgotas

Hace 7 minutos

que chuchas te importa

Pareces una travesti bien puta

Hace 22 minutos

ok

Cuanto cobras cabrona por tu culo

Fig. 5. Sample messages posted on the Ask.fm social network by the user *mapesystems2*.

The second analyzed account of the Ask.fm social network belonged to the user *mapesystems4344*, which was also created to validate the algorithm of the Parental Control Multiplatform System, and unlike the previous account, its objective consisted of posting messages without “much” presumed harassing content, as can be seen in Fig. 6. Unlike the first analyzed account, in this account, the total value of “positive” text similarity prevails over “negative” text similarity. This indicates that in this account there is a lower amount of texts with cyberbullying.

B. Expert Validation of the Parental Control Multiplatform System

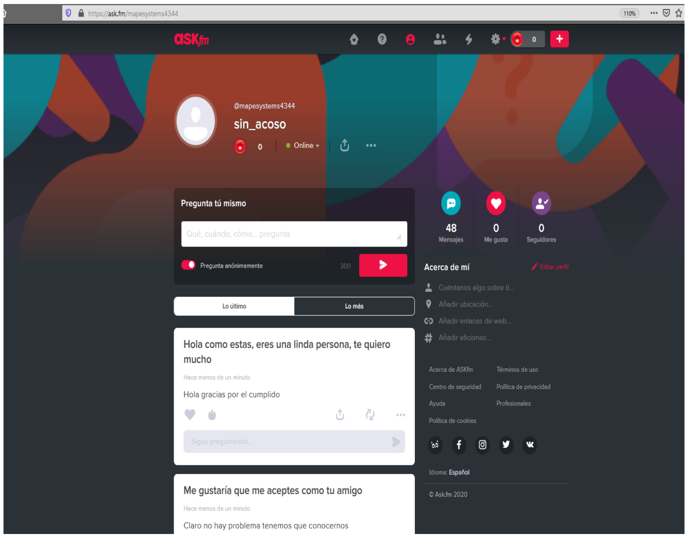
It is important to mention that, for the validation process, the collaboration of psychologists, and specialists in the area of cyberbullying, as well as students and parents or guardians was requested. For the validation of the Web application, first, an explanation of the system’s functionalities was given user registration; social network account creation, validation; analysis, and detection of presumptive cyberbullying; among other functionalities. Once the whole process was explained, the following link https://cloudcomputing.ups.edu.ec/controlParental/ was sent to them so that they could interact with the system and perform the cyberbullying analysis on different social network accounts.

Once the presentation and validation of the web application were finished, the functionalities available in the mobile application were explained, such as viewing the results of the analyzed accounts, checking account information, and updating user data. After the demonstration, the psychologist and the guardians downloaded[1] the mobile application from the Google Play Store. To assess the effectiveness and adequacy of our mobile and web applications in detecting suspected cyberbullying cases, a group of experts conducted testing. Following this, we distributed a questionnaire to a diverse

[1] At the moment of writing this paper and after being published for several months, the application has been unpublished due to Google’s policies.

TABLE III. SAMPLES OF THE RESULTS OBTAINED BY THE ALGORITHM OF THE PARENTAL CONTROL MULTIPLATFORM SYSTEM WHEN ANALYZING THE @PONTIFEX_ES TWITTER ACCOUNT

QUERY	% SIMILARITY NEGATIVE TEXT	% SIMILARITY POSITIVE TEXT	CYBERBULLYING?
“La oración es el centro de la vida, Si hay oración, también el hermano, la hermana, se vuelve importante, Quien adora a Dios, ama a sus hijos, Quien respeta a Dios, respeta a los seres humanos,” $\#AudienciaGeneral@Pontifex_es, 2012,$	18.02	24.26	No
“La pertenencia a Cristo y el estilo de vida que se deriva de ella no aíslan al creyente del mundo; por el contrario, lo hacen protagonista de un servicio de amor en favor del bien común,” $@Pontifex_es, 2012$	25.12	36.93	No
“¿Una decisión valiente? Destinar el dinero utilizado para las armas a un “Fondo mundial” para acabar con el hambre, Esto evitaría muchas guerras y la emigración de muchos hermanos y hermanas nuestras de los países más pobres, #JornadaMundialAlimentación” (@Pontifex_es, 2012)	14.45	13.73	Yes
“Es tiempo de suscribir un pacto educativo global por y con las jóvenes generaciones, un pacto que comprometa a familias, comunidades, escuelas, universidades, religiones, instituciones, gobernantes, a la humanidad entera, para formar personas maduras, #GlobalCompactOnEducation” @pontifex_2012 ,	14.98	22.37	No
“María, la madre que cuidó a Jesús, también cuida con afecto y dolor materno este mundo herido,” (@Pontifex_es, 2012)	20.41	14.88	Yes
“El mundo es algo más que un problema a resolver, es un misterio gozoso que contemplamos con jubilosa alabanza, #TiempoDeLaCreación #LaudatoSì” (@Pontifex_es, 2012)	05.75	07.87	No



Hola como estas, eres una linda persona, te quiero mucho

Hace menos de un minuto

Hola gracias por el cumplido

Me gustaría que me aceptes como tu amigo

Hace menos de un minuto

Claro no hay problema tenemos que conocernos

Fig. 6. Sample messages posted on the Ask.fm social network by the user *mapesystems4344*.

group of 10 users, including parents, guardians, students, and psychologists. The questionnaire aimed to gather feedback on the application’s features and determine its overall effectiveness. The most relevant results of the survey are presented below.

As evidenced in Table IV, 50% of the surveyed users consider that how the results of the analyses are presented in the web application is understandable and 50% consider that how the results are presented in the application is easy to understand. This shows that all participants understood and comprehended how the information is displayed.

TABLE IV. DOES THE WEB APPLICATION EFFECTIVELY PRESENT THE ANALYSIS RESULTS IN A CLEAR AND COMPREHENSIBLE MANNER?

	Users	Answer
Absolutely understandable	5	50%
Easy to understand	5	50%
Absolutely difficult to understand	0	0%

Furthermore, Table V shows that 60% of the surveyed users consider that the mobile application has an excellent appearance, and 50% consider that it has a good appearance in terms of colors, images, icons, and visibility. This shows that all respondents consider that the mobile application has an adequate appearance and meets their needs.

TABLE V. WHAT DID YOU THINK OF THE APPEARANCE (COLORS, IMAGES, ICONS, VISIBILITY) OF THE MOBILE APPLICATION?

	Users	Answer
Excellent appearance	6	60%
Good appearance	4	40%
Bad appearance	0	0%

In that order, users were asked whether they consider how the results of the analyses are presented in the mobile application to be understandable. According to the results presented in Table VI, 60% of the surveyed users consider it to be understandable and 40% consider it to be easy to understand. This means that all participants understand and can comprehend the presentation of the results.

Table VII, shows that 88.9% of surveyed users consider the security of the application to be excellent and 11.1% consider it to be regular. This means that most of the participants consider that both the web and mobile applications have good security in terms of the information handled, since it is confidential between each user.

TABLE VI. Does the Mobile Application Effectively Communicate the Analysis Results Understandably?

	Users	Answer
Absolutely understandable	6	60%
Easy to understand	4	40%
Absolutely difficult to understand	0	0%

TABLE VII. How Satisfied are you with the Security of the Application?

	Users	Answer
Excellent	9	88.9%
Regular	1	11.1%
Bad	0	0%

Regarding the ease of use of the application to detect presumptive cases of cyberbullying, Table VIII, evidences that 70% consider that both the mobile application and the web are very easy to use and 30% consider that are easy to use. This means that the majority of participants find the applications easy to use.

TABLE VIII. How Satisfied are you with the Ease of use of these Applications?

	Users	Answer
Very easy to use	7	70%
Easy to use	3	30%
Absolutely difficult to use	0	0%

Moreover, when users were asked, how satisfied are they with the reliability of this application? As Table IX shows, 80% consider that it is very reliable to use the applications, while 10% consider that it is not very reliable and the remaining 10% consider that it is not reliable to use the applications. This means that a minimum percentage of surveyed users are not sure about the reliability of the application.

TABLE IX. How Satisfied are you with the Reliability of this Application?

	Users	Answer
Very reliable	8	80%
Unreliable	1	10%
Not reliable	1	10%

Finally, users were asked if they would use this application daily to keep control over the social networks of the adolescents or young people they represent to prevent them from suffering presumptive cyberbullying. Table X, shows that in response to this inquiry, 80% consider that it does meet the objective of helping with cyberbullying issues and 20% consider that it meets the objective of helping with cyberbullying issues regularly.

V. Discussions

The review of the literature on the use of new information and communication technologies to prevent and detect cases of cyberbullying in young people and adolescents demonstrates the current concern to address the problem. The total of the research consulted is mainly focused on finding effective solutions for the detection and prevention of cyberbullying in digital environments, especially in social networks. NLP is one of the most novel technologies for analyzing and understanding contextual content generated online and identifying patterns of cyberbullying, offensive language or abusive content. However, the consideration of the contextual aspect is a very little addressed topic. Therefore, the contributions of the present research demonstrate that understanding the context is a relevant element to accurately detect cases of cyberbullying on digital platforms.

TABLE X. Would you use this Application Daily to Maintain Control Over Your Constituents' Social Networks and Prevent them from Presumptive Cyberbullying?

	Users	Answer
Yes	9	90%
No	1	10%

Tests carried out with the use of two Twitter accounts demonstrated the efficiency of the Parental Control Multiplatform System to extract information from the social network accounts of adolescents, analyze it using the LSA method, and generate results with the percentage of similarity, both in "negative" and "positive" texts, and alert parents or guardians whether or not there is a presumptive case of cyberbullying.

Unlike the applications developed by [19], [20], [21], [22]. The author in [23], the present research focused on the use of LSA in the Spanish language to achieve greater precision in the analysis of the similarities of texts related to cyberbullying in the context of Ecuadorian adolescents. The research analyzed demonstrates the efforts made by different countries to protect adolescents from online cyberbullying and the scarcity of solutions in Spanish. Thus, it is possible to demonstrate that the use of LSA allows obtaining an appropriate percentage of similarity on alleged cases of cyberbullying in social networks using a knowledge base extracted semi-automatically from social networks such as Twitter.

In summary, the use of Latent Semantic Analysis for detecting cyberbullying in Ecuadorian social media has demonstrated its valuable capabilities, alongside certain inherent limitations in capturing emotional connotations. LSA's strength in identifying explicit aggressive language, as evidenced in high-profile cyberbullying cases, highlights its utility as a tool in initial screening processes. However, our experiments also brought to light the method's challenges in interpreting more nuanced emotional contexts. For instance, the misclassification of contextually complex terms in Pope Francis's account illustrates the need for a deeper understanding of emotional subtleties beyond LSA's word co-occurrence framework. Also, the minimal disparities in negative and positive text percentages in certain cases further underscore the importance of integrating LSA with more context-sensitive methods. Embracing these limitations as opportunities for improvement, LSA can be effectively complemented with advanced, emotionally intelligent algorithms, paving the way for more nuanced and culturally aware cyberbullying detection systems.

The validation, functioning, and operability of the Parental Control Multiplatform System were positively assessed by representatives and experts in the field of psychology. When consulted, they stated that the multiplatform application is a novel tool for identifying possible cases of bullying on social networks. The multiplatform application to detect suspected cyberbullying differs from other existing applications because although they provide parents or guardians with tools to monitor their children's online activity [29], they are not focused on analyzing the online activities of adolescents to detect possible cases of cyberbullying through specific information analysis techniques and the identification of bullying patterns [10].

In terms of functional requirements, parental control applications generally offer monitoring of browsing history, blocking of inappropriate websites, monitoring of messages and phone calls, and setting time limits for the use of devices [19]. Unlike these, our designed application is based on Natural Language Processing using the LSA method, which allows for establishing search patterns, information retrieval, grouping of topics, generating alerts and content recommendations [17], [18].

Regarding the security of the proposed system, it could be demonstrated that it is a secure platform. It is designed to protect users' personal information and comply with privacy and data security standards. Nevertheless, a very small number of users stated that they would not use the application frequently to monitor their children's social network usage. The tests conducted showed that the application does not present potential risks in terms of privacy and data security. One of the major limitations of the apps available for parents and guardians is that they rely on excessive handling of personal information, which becomes a risk factor for the safety of families.

VI. Conclusions

Nowadays, despite the evolution of information and communication technology, very little importance has been given to the negative situations that these advances entail. The most significant issue, and one that is occurring worldwide, has to do with cyberbullying. Although its effects can be devastating, especially for young people and adolescents, there are not many tools or applications aimed at analyzing the activities that adolescents perform on their social networks and determining cases of possible harassment on digital platforms given certain publications, comments, or messages that are inappropriate.

The Parental Control Multiplatform System developed through Natural Language Processing in Spanish had the objective of detecting presumptive cases of cyberbullying in the social networks of the accounts registered in the applications, based on the extraction of information. With the use of data mining, it was possible to generate scripts called *crawlers* to obtain the information, with the respective authorization of the person who owns the account.

The content analysis is performed using the Latent Semantic Analysis method. The creation of a semantic space made it possible to determine the existing similarities between a harassment dataset, which includes positive and negative texts, and the information of each social network, with the purpose of evidencing whether there is alleged cyberbullying.

The Parental Control Multiplatform System provides the necessary information to the user. In addition to the analysis, the user is also provided with multimedia content that will allow him/her to have more information about cyberbullying. This is because, for many representatives, this is still a new and unknown topic. The first option is to contact specialists on the subject, such as psychologists, who can provide guidance and have the appropriate knowledge and the necessary tools to cope with this type of situation that could happen to the person they represent. Another option is to view a list of videos on the subject and the last option is to review articles on the Internet.

Cyberbullying is a constantly evolving phenomenon and new technologies and forms of online communication present new challenges for its investigation and prevention. Therefore, there is still much to explore and discover about cyberbullying, especially in relation to newer forms of cyberbullying, such as cyberbullying through online gaming platforms and next-generation social networks. Similarly, it is important to note that cyberbullying has significant impacts on the mental health and well-being of young people, so more research and efforts in prevention and treatment are needed.

Acknowledgment

The authors would like to thank the Cloud Computing, Smart Cities & High Performance Computing Research Group (GIHP4C), and the Computer Science students of the *Universidad Politécnica Salesiana* (UPS) for their collaboration in the development of the study. In addition, they are grateful for the support of the psychology specialists who helped in the validation of the Parental Control Multiplatform System for the prevention of cyberbullying. The parents, guardians, and representatives are thanked for their observations and suggestions for improving the use of the system.

References

[1] G. W. Giumetti and R. M. Kowalski, "Cyberbullying via social media and well-being," Current Opinion in Psychology, p. 101314, 2022.

[2] K. Subaramaniam, R. Kolandaisamy, A. B. Jalil, and I. Kolandaisamy, "Cyberbullying challenges on society: a review," Journal of positive school psychology, vol. 6, no. 2, pp. 2174–2184, 2022.

[3] D. J. Meter, R. Budziszewski, A. Phillips, and T. E. Beckert, "A qualitative exploration of college students' perceptions of cyberbullying," TechTrends, vol. 65, pp. 464–472, 2021.

[4] S.-M. Bae, "The relationship between exposure to risky online content, cyber victimization, perception of cyberbullying, and cyberbullying offending in korean adolescents," Children and youth services review, vol. 123, p. 105946, 2021.

[5] Unicef et al., "Una mirada en profundidad al acoso escolar en el ecuador," Violencia entre pares en el sistema educativo. Obtenido de: https://www. unicef. org/ecuador/acoso_escolar. pdf, 2015.

[6] G. A. León-Paredes, W. F. Palomeque-León, P. L. Gallegos-Segovia, P. E. Vintimilla-Tapia, J. F. Bravo-Torres, L. I. Barbosa-Santillán, and M. M. Paredes-Pinos, "Presumptive detection of cyberbullying on twitter through natural language processing and machine learning in the spanish language," in 2019 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), Nov 2019, pp. 1–7.

[7] D. A. Andrade-Segarra, G. A. Le et al., "Deep learning-based natural language processing methods comparison for presumptive detection of cyberbullying in social networks," International Journal of Advanced Computer Science and Applications, vol. 12, no. 5, 2021.

[8] N. B. Alotaibi, "Cyber bullying and the expected consequences on the students' academic achievement," IEEE Access, vol. 7, pp. 153 417–153 431, 2019.

[9] ——, "Cyber bullying and the expected consequences on the students' academic achievement," IEEE Access, vol. 7, pp. 153 417–153 431, 2019.

[10] G. Wang, J. Zhao, M. Van Kleek, and N. Shadbolt, "Protection or punishment? relating the design space of parental control apps and perceptions about them to support parenting for online safety," Proceedings of the ACM on Human-Computer Interaction, vol. 5, no. CSCW2, pp. 1–26, 2021.

[11] E. L. Helfrich, J. L. Doty, Y.-W. Su, J. L. Yourell, and J. Gabrielli, "Parental views on preventing and minimizing negative effects of cyberbullying," Children and Youth Services Review, vol. 118, p. 105377, 2020.

[12] S. Ali, M. Elgharabawy, Q. Duchaussoy, M. Mannan, and A. Youssef, "Betrayed by the guardian: Security and privacy risks of parental control solutions," in Annual Computer Security Applications Conference, 2020, pp. 69–83.

[13] M. S. M. Suhaimin, M. H. A. Hijazi, R. Alfred, and F. Coenen, "Natural language processing based features for sarcasm detection: An investigation using bilingual social media texts," in 2017 8th International conference on information technology (ICIT). IEEE, 2017, pp. 703–709.

[14] T. Kanan, O. Sadaqa, A. Aldajeh, H. Alshwabka, S. AlZu'bi, M. Elbes, B. Hawashin, M. A. Alia et al., "A review of natural language processing and machine learning tools used to analyze arabic social media," in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). IEEE, 2019, pp. 622–628.

[15] J. Minango, A. Flores, M. Zambrano, W. Paredes Parada, and C. Tasiguano, "Radar probability of detection in multipath environments," Trends in Artificial Intelligence and Computer Engineering: Proceedings of ICAETT 2022, pp. 91–103, 2023.

[16] D. Jurafsky and J. Martin, "Computational linguistics and speech recognition, 2000," 2000.

[17] J. Daniel, M. James H et al., Speech and language processing: An introduction to natural language processing, computational linguistics, and speech recognition. prentice hall, 2007.

[18] G. A. León-Paredes, L. I. Barbosa-Santillán, and J. J. Sánchez-Escobar, "A Heterogeneous System Based on Latent Semantic Analysis Using GPU and Multi-CPU," Scientific Programming, vol. 2017, p. 19, 2017.

[19] M. F. Wyne, J. Sood, C. Kempton, and T. Dao, "Safeguard: A web-based application to guard against cyberbullying." Journal of Education and Learning, vol. 10, no. 4, pp. 63–69, 2021.

[20] S. Shrimali, "A natural language processing and machine learning-based framework to automatically identify cyberbullying and hate speech in real-time," in 2022 IEEE MIT Undergraduate Research Technology Conference (URTC). IEEE, 2022, pp. 1–5.

[21] S. Afrifa and V. Varadarajan, "Cyberbullying detection on twitter using natural language processing and machine learning techniques," International Journal of Innovative Technology and Interdisciplinary Sciences, vol. 5, no. 4, pp. 1069–1080, 2022.

[22] B. Bhatia, A. Verma, Anjum, and R. Katarya, "Analysing cyberbullying using natural language processing by understanding jargon in social media," in Sustainable Advanced Computing: Select Proceedings of ICSAC 2021. Springer, 2022, pp. 397–406.

[23] J. M. A. Soto, H. Á. Gonzales, and V. B. Saines, "Uso de una herramienta de nlp aplicada a la detección del ciberacoso en twitter," Innovación y Software, vol. 3, no. 2, pp. 81–90, 2022.

[24] D. Van Bruwaene, Q. Huang, and D. Inkpen, "A multi-platform dataset for detecting cyberbullying in social media," Language Resources and Evaluation, vol. 54, pp. 851–874, 2020.

[25] R. Slonje, P. K. Smith, and A. Frisén, "The nature of cyberbullying, and strategies for prevention," Computers in human behavior, vol. 29, no. 1, pp. 26–32, 2013.

[26] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[27] M. Eyuboglu, D. Eyuboglu, S. C. Pala, D. Oktar, Z. Demirtas, D. Arslantas, and A. Unsal, "Traditional school bullying and cyberbullying: Prevalence, the effect on mental health problems and self-harm behavior," Psychiatry research, vol. 297, p. 113730, 2021.

[28] S. Hinduja and J. W. Patchin, Bullying beyond the schoolyard: Preventing and responding to cyberbullying. Corwin press, 2014.

[29] M. Anderson, "Parents, teens and digital monitoring," 2016.