IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205218 |

Cyber Bullying: Safeguarding Kids from Internet Harassment

Rakshit Patial, Murugan R, Professor

Student of MCA, Dept. of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India

Professor, Dept. of CS&IT, Jain (Deemed-to-be-University), Bengaluru, India

Abstract: As parents, we all want to protect our children from the dangers of online pornography, cyberbullying, and predators. Various current methods focus on limited information gathered from the child's interactions online. Some use a blacklist of prohibited URLs to block access to certain websites, while others analyze the multimedia exchanged between the child and others. However, these approaches may not be foolproof as new URLs can evade the blacklist and individual images, videos, and text may appear harmless when considered on their own. Our proposal suggests a flexible framework that examines material at the Human-Computer Interaction (HCI) level, or user interface, in its completed state. Despite hardware restrictions, Children's Agents for Secure and Privacy Enhanced Reaction (CASPER) seeks to analyze audio signals and screen captures in real-time to make judgments based on all available information. Through the use of deep learning methods for text, audio, and picture processing, CASPER categorizes visual content as either pornographic or neutral. Text can be classifiedas cyberbullying, neutral, or objectionable. We have created a custom dataset with a variety of offensive material for training and assessment purposes. When it comes to text classification, CASPER has demonstrated an average accuracy of 88% and score of 0.85, while its accuracy for pornographic classification is 95%.

I. INTRODUCTION

Ensuring children's safety online is extremely important, especially with the increase in screen time due to school closures and government regulations in western countries. With restrictions limiting interactions with friends and family, children are left to communicate through VoIP or social media, putting them at risk of harmful encounters with unknown individuals. It is crucial to protect children from potential dangers online to safeguard their mental and physical well-being. Providing individuals withresources to protect themselves from online dangers like cyberbullying, pornography, online grooming, and self-harm inducement. This is a widely studied field, both from the psychological standpoint of how these types of dangers affect children's well-being, as well as from a cyber- security perspective, which aims to detect and prevent the occurrence of unwanted content. Individual systems exist that detect unwanted imagery. In this field, there are also advancements that specifically target identifying different kinds of hazards that were previously stated. By evaluating incoming material, Mallmann et al. propose a system that attempts to defend against all kinds of attacks, although it relies on hardware that might not be widely available on all devices. There are procedures in place that restrict access to websites that are manually blocked.

We have developed a simple and flexible system that analyzes all User Interface (UI) outputs to detect inappropriate material aimed for kids. Our system runs on hardware that does not require a graphics card—it just needs a Central Processing Unit, or CPU. Our solution may be utilized on several devices thanks to its design. even though it may sacrifice some accuracy and speed. Our system categorizes content in real-time from both the screen and the audio output simultaneously. By focusing on the information displayed in the UI layer,we are able to effectively identify and filter outunwanted content.

We put our system to the test on a set of browser sessions with both appropriate and improper content. The measure of our performance was the capacity to locate unsuitable regions in the manually labeled dataset. Our work's main contributions are the flexible system architecture we designed and the manually annotateddataset we produced for our image detection algorithm's testing, validation, and training utilizing screenshots. Because the manually annotated photos provideinformation about image classes, this dataset is especially helpful for detecting pornography. We also made modest contributions by creating specializedmodules that handled the analysis of text, graphics, audio, and video from the user interface layer.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205218 |

II. LITERATURE REVIEW

Analysing children's interactions with online platforms to shield them from cyber threats involves a comprehensive strategy encompassing technological, educational, and regulatory components. One prevalent tactic involves the use of parental control software, empowering parents to monitor and limit their children's online activities, including blocking inappropriate content and setting usage restrictions. These tools often employ algorithms to filter content and detect concerning keywords. Additionally, some platforms employ age verification measures to prevent minors from accessing unsuitable material. Educational initiatives are pivotal in equipping children with the skills needed to navigate the digital realm safely. Workshops and courses offered by schools and organizations educate children on topics such as online privacy, cyberbullying, and critical thinking in online contexts. Enhanced digital literacy enables children to identify and address cyber threats more effectively. Moreover, fostering open communication between parents and children about online behaviour is essential for building trust and promoting responsible digital citizenship. Regulatory efforts, such as the Children's Online Privacy Protection Act (COPPA) in the US and the General Data Protection Regulation (GDPR) in the EU, establish guidelines for online privacy and safety. These laws require consent for collecting children's data and mandate privacy protections. Collaboration among stakeholders—including parents, educators, technology companies, and policymakers—is vital for addressing evolving online threats to children. By combining technological tools, educational programs, and regulatory frameworks, society can strive to create a safer digital environment for children to explore and learn. Continuous evaluation and adaptation of strategies are necessary to keep pace with emerging cyber threats and ensure children's protection online.

A. DETECTION OF EXPLICIT IMAGES

Important elements of AI, for instance how A. Detection of explicit images Detection schemes to spot pornographic imagery in a photo depending on whetherthey are feature based as per this taxonomy pornographic content in an image may be detected using any of approaches based on features, regions, or bodily parts. The feature-based (Panda, for example) approaches either concentrate on learning or look for particular traits throughout full images, including local features utilizing SIFT descriptors that can be combined.

Representations through Convolutional Neural Networks (Convent's). Handcrafted features are required for extracting whole-object details from an image in this context.The primary objective of region-based techniques is to identify segments that exhibit specific attributes ofpornographic videos such as physical bodies. Most ofthe times this can be a skin detector that is based on the o find the pixels in a picture frame that match to human skin, use the Red, Green, and Blue (RGB) model.

While the method may not be as susceptible to variations in backgrounds compared with approaches using features, it suffers from a potential problem; when skin is not accurately detected unjustly categorized as pornography underlies these methods' limitation or ignorance

B. DETECTION OF CYBERBULLYING IMAGES

Authors have scrutinized images with the purpose of non-recognition. Involving the Their approach was to focus more on the sentiment and content of the comments that accompanied the photographs than the images themselves. They take this a step further by checking the continuity of each user that has posted a comment in the image or any other visual method related activity for example if there were many capital letters involved per comment made about it by different users of theirs.' Thus, unlike conventional methods for recognizing operator-defined occurrences including cyber-Bullying among others., this study focuses on how different social cues elicit various effects such as attention Seeking behavior from individuals during real time online interactions while using these sites! Bullying imagery usually shows scenes in which the victim's face is replaced in the original photo by the face of the bullying target in an explicit, violent, disparaging, or otherwise degrading manner. Archives like make an effort to list relevant techniques to stop this attack on the victims by detecting faked imagery using deep learning—more precisely, GANs. Several techniques are presented in particular that address the issue of fabricated imagery, particularly with regard to face switching and recognizing explicit material in images and movies.

C. TEXT CYBERBULLYING DETECTION

Current research indicates an increasing trend in the prevalence of cyberbullying among youthful populations. About 18% of European kids have experienced cyberbullying according to current studies. With regards to the according to data from the 2014 EU Kids Online Report, 20% of children aged 11 to 16 reported experiencing instances of cyberbullying. In his quantitative survey, Tokunaga found out that between 20% and 40% teenagers have fallen victim to cyberbullying attack. There are several methods suggested for picking up cyberbullying. All the previous research analyses have used time-honored Machine Learning (ML) measures to zap the cyberbullying incidents. For cyberbullying, Deep Neural Network based models have recently come into play. It's taken on the approach of a

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205218 |

classification task where each message is separately marked either as bully or not-a-bully using such methods. Various neural network models could help with the detection of cyberbullying. Common models used for this purpose include CNNs, Long Short Term Memory (LSTM), Bidirectional LSTM (BLSTM), and BLSTM with attention, each with increasing levels of neural architectural complexity. While CNNs are typically suited in image and text classification as well as sentiment classification. LSTM networks are used for learning long-term dependencies. Their internal memory is useful for text classification. Bidirectional LSTMs enhance the input information that the network receives by sending information both in forward and backward directions. BLSTM with attention tends to place stronger connections between the model's state at disparate moments (time), lower perplexity and higher burstiness.

D. DETECTION OF ONLINE SEXUAL GROOMING

Online grooming can happen when an adult predator dishonestly befriends a young person through the internet, then persuades them into committing sexual misdemeanors. Online grooming has globally become possible due to large social media platforms whereusers visit for entertainment purposes, as well as gaming sites where players get involved in different levels of digital games aimed at improving their skills on computers among others. These are the platforms with people from all walks of life who share personal information about themselves, their children, whose identities they always conceal from others even within circles of close relatives. It is estimated that 1 out of 5 kids are emailed explicit content before 18 years old but some victims may be minors.

Ways to Prevent from cyberbullying:

1. **Education and Awareness**: For Parents: Teach parents what cyber- bullying entails and how to help their children when the kids fall victims to it. One should always encourage their kids to talk to themfreely about anything they do on the internet. For Children: Raise awareness among kids on digital citizenship; teach them about online etiquette and the results of their actions on the web. Kids should also be helped to understand how harmful it can be to engage in cyber- bullying by encouraging them know where they can receive assistance should they encounter such situations either as victims or bystanders.

2. **Encourage pleasant online behavior**: It is important to teach children to be kind and respectful online, show them empathy and explain to them why it is important to maintain their dignity while relating with others both offline and online. Promote digital empathy and responsibility among people by advocating for affirmative interaction on social media platforms and other such online areas.

3. **Parental Involvement:** Parents should monitor what kids do on the internet by keeping an eye on their surfing habits; they should also put-up specific regulations restricting use of this resource. It is possible to make use of special software programs for controlling system activities and blocking access too bad places. As much as possible, it is advisable that dialogue be open between children themselves or with their parents when discussing such cases. Children also need to be comfortable enough when talking about things bothering them in such forums to parents.

4. **School-Based Interventions**: In order to put a stop to cyberbullying there is need for implementing holistic anti-bullying policies which clearly define this. Staff members in schools should be trained on how best to identify or report cases involving cyberbullying Practically as well as respond on time. The presence of programs like peer support systems and mentorship programs help in creating good relations between students and also encourage them in standing against cyberbullying.

5. **Tech Solutions**: Collaborate with techcompanies to build AI-powered content moderation, reporting mechanisms, and safety tools as part of their online safety awareness campaign. By doing so, it implies working at enhancing the use of applications and online sites leading to guaranteed safety for every user through quality anti-bullying mechanisms.

6. **Support Services:** Children should be able to access support services like guidance counsellors, mental health therapists, and helplines, if they are being cyber bullied and assist parents plus educators by showing them how to get these facilities.

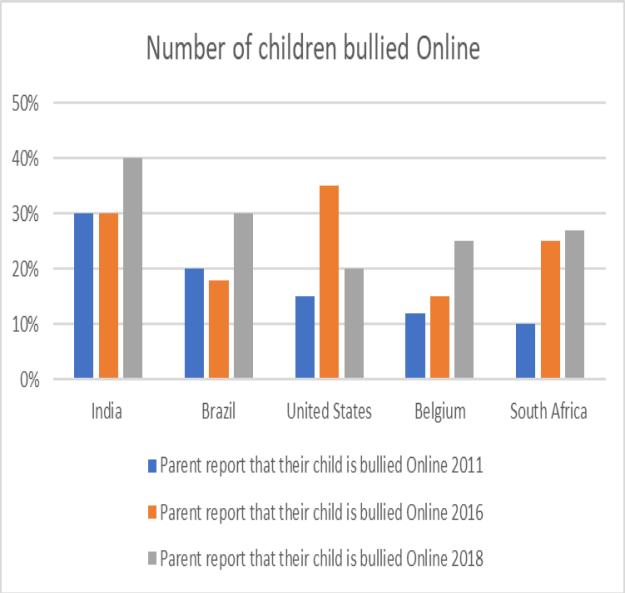
7. **Measures Concerning Law and Policy**: Push and (force) for stricter laws and policies that can handle cyberbullying as well as making those responsible account for their actions. This may range from having an act

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205218 |

➢ Here is the Graph for child cyberbullying across the world.



III. CONCLUSION

In conclusion, in the current digital era, kid cyberbullying is still a widespread and worrisome problem. Even though the internet has many advantages and opportunities, it also provides a venue for cruelty and harm, especially to our impressionable young people. The ways and intensity of cyberbullying are always changing along with technology, thus preventing it will require a proactive, multifaceted strategy. To make the internet a safer place for kids, collaboration between parents, teachers, legislators, and tech firms is essential. This entails teaching young users' empathy, respect, and digital responsibility in addition to enforcing stringent rules and penalties for cyberbullying activity. In addition, it's critical to offer tools and help to both cyberbullying victims and offenders. In addition to being reassured that they are not alone in their experiences, victims need channels for reporting events, as well as access to therapy and support services. In a similar vein, offenders need to be made aware of the repercussions of their behavior and given the chance to get well and alter their ways. Ultimately, we can contribute to ensuring that the internet continues to be a safe and welcoming environment for all kids to study, interact, and grow by realizing the seriousness of child cyberbullying and taking proactive measures to combat it.

REFERENCES

[1] N. AlDahoul, H. Karim, M. Abdullah, M. Fauzi,A. Wazir, S. Mansor, and J. See, ''Transfer detection of YOLO to focus CNN's attention on nude regions for adult content detection,'' Symmetry, vol. 13, no. 1, p. 26, 2020.
[2] S. Avila, N. Thome, M. Cord, E. Valle, and A. de A. Araújo, ''Pooling in image representation: The visual codeword point of view,'' Comput. Vis. Image Understand., vol. 117, no. 5, pp. 453–465, May 2013.
[3] D. Bogdanova, P. Rosso, and T. Solorio, ''Exploring high-level features for detecting cyberpedophilia,'' Comput. Speech Lang., vol. 28, no. 1, pp. 108–120, Jan. 2014.
[4] A. E. Cano, M. Fernandez, and H. Alani, ''Detecting child grooming behaviour patterns on social media,'' in Social Informatics (Lecture Notes in Computer Science). Springer, 2014, pp. 412–427.
[5] A. Chatterjee, K. N. Narahari, M. Joshi, and P. Agrawal, ''SemEval-2019 task 3: EmoContext contextual emotion detection in text,'' in Proc. 13th Int. Workshop Semantic Eval., 2019, pp. 1–10.
[6] M. Dadvar and K. Eckert, ''Cyberbullying detection in social networks using deep learning-based models,'' in Big Data Analytics and Knowledge Discovery (Lecture Notes in Computer Science). Springer, 2020, pp. 245–255.
[7] M. Dadvar, D. Trieschnigg, R. Ordelman, and F. D. Jong, ''Improving cyberbullying detection with user context,'' in Advances in Information Retrieval (Lecture Notes in Computer Science). Springer, 2013,pp. 693–696.
[9] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, ''BERT: Pre training Of deep bidirectional transformers for language understanding,'' 2018, arXiv:1810.04805.
[10] M. Ebrahimi, C. Y. Suen, and O. Ormandjieva, ''Detecting predatory conversations in social media by deep convolutional neural networks,

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details