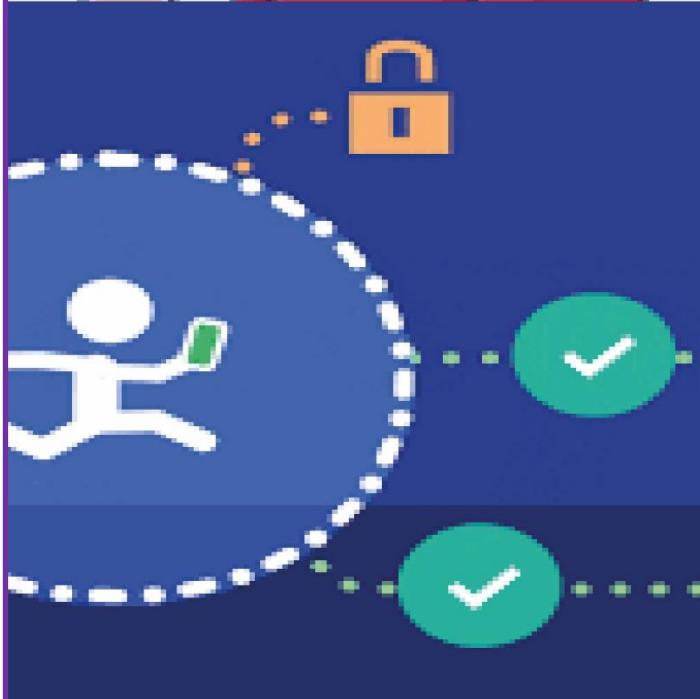
Child Abuse in Digital Space



JANUARY 28

CYGNUSA TECHNOLOGIES
Authored by: Shalin Jain

Online Child Abuse

Online child abuse is a unique form of child abuse also known as “Cyber Molestation” due to its virtual, distanced, and anonymous nature.
This can be categorized into five major categories:

- **Cyber Bullying**
- **Grooming**
- **Sexual Abuse**
- **Adult/ Unappropriated Websites**
- **Online Child Trafficking**

In today’s Generation Virtual Safety is equally important to physical safety. The whole world is digitalized and the young Generation plays a major role in this development. Thus, ensuring their safety should be a primary concern.
AI and ML rule all the major and latest Tech Inventions. Be it Automated Vehicles, Online Shopping Websites, Search Engines, Image-Filters, everywhere. This advanced Technique can be used in this field as well and can make the Internet much safer for Kids.

Basic ML prototypes can be developed which can solve problems in each of the above-mentioned categories such as:

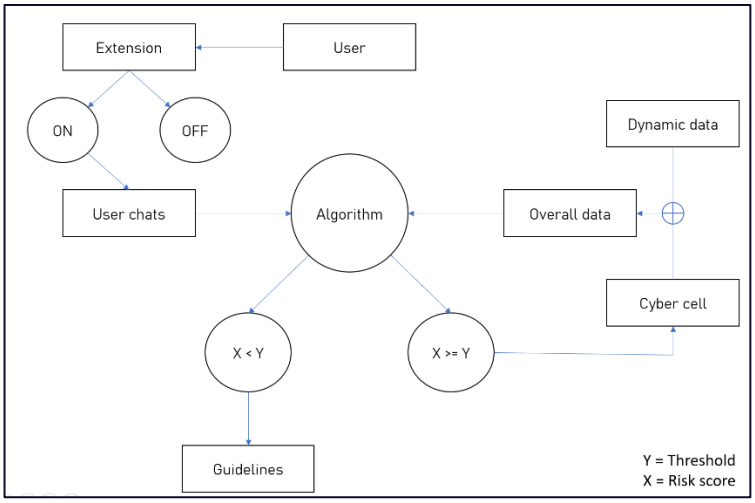
- **Risk Score Detector**
- **Password Randomizer**
- **Image detection Tool**
- **Mental-Age Analyzer**

A full-fledged App/Webpage can be created combing all the above prototypes.

Risk Score Detector:

A chrome extension which can be attached to Messenger, WhatsApp Web Chats on permission. This prototype will analyze the chat and calculate a risk score which can be then used to suggest the user appropriate answers and relatable information.

A threshold can be set so that if the Risk Score is going beyond that, the System will recognize it as **Cyber Bullying** and immediately notify the IP address to the nearest Cyber Cell. This will solve the issue of insecurity which children have and will also improve the knowledge of Kids so that they are prepared for future.

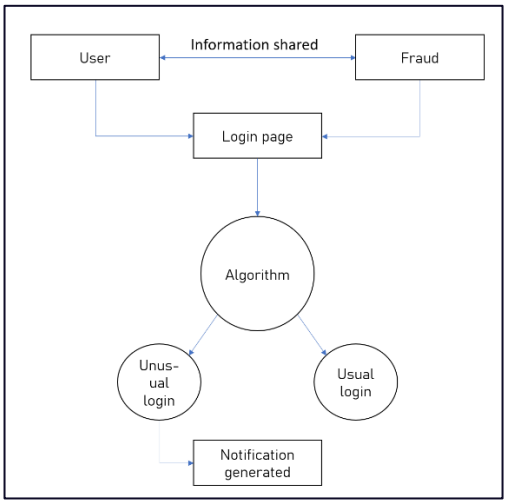


ML Tools and Frameworks used:

This Prototype is **NLP** based and uses Similarity Index such as Cosine Similarity to evaluate the Risk Score. The nltk module will clean up the corpus and then **Naïve Bayes Algorithm** will be implemented for evaluation.

Password Randomizer:

Fake Calls and Online Frauds have increased exponentially in the past decade and young girls and boys are the easiest targets for these frauds. They manipulate their minds with greed and steal their confidential passwords. This Randomizer will randomly change the passwords of the Social Media Accounts and other accounts if it detects an unusual login pattern and then notify the parents as well. This simple application can safe guard accounts with a very high Efficiency and the random passwords will be messaged to both parents and children so that they can later review the pattern and act accordingly.



ML Tools and Frameworks used:

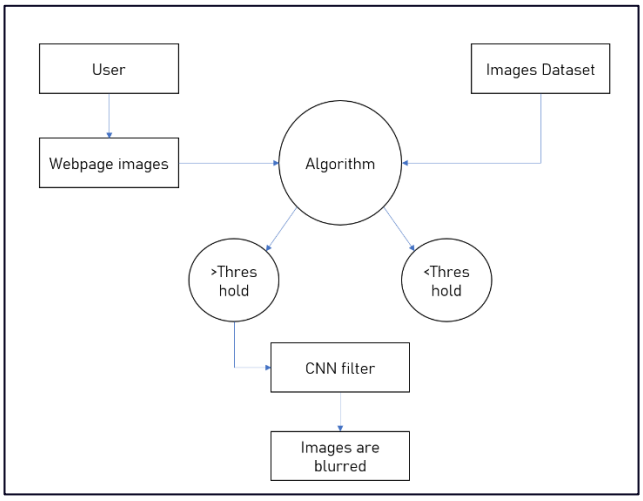
A **shallow Neural network** will be formed which store the parameters and give an encoding to the daily Login Pattern. We will then use **SVM** to do an Anomaly Detection and if we find an encoding which is completely breaching the rest, an alert will be sent.

Image Detection Tool:

This Prototype can be used as an extension with any browser. This will scan the webpage while surfing and detect inappropriate and unsafe images and videos from the webpage. The items detected will then be blurred using CNN filters. As a result, general guidelines related to Online child abuse will pop up, so that the child can be more aware about such cases.

This way the privacy of the child is also not breached and they are away from the Dark web as well.

A global Counter for each website will be maintained, so if some website crosses the limit, the cyber cell can be informed and required changes can be done in the login and security policies of that website.



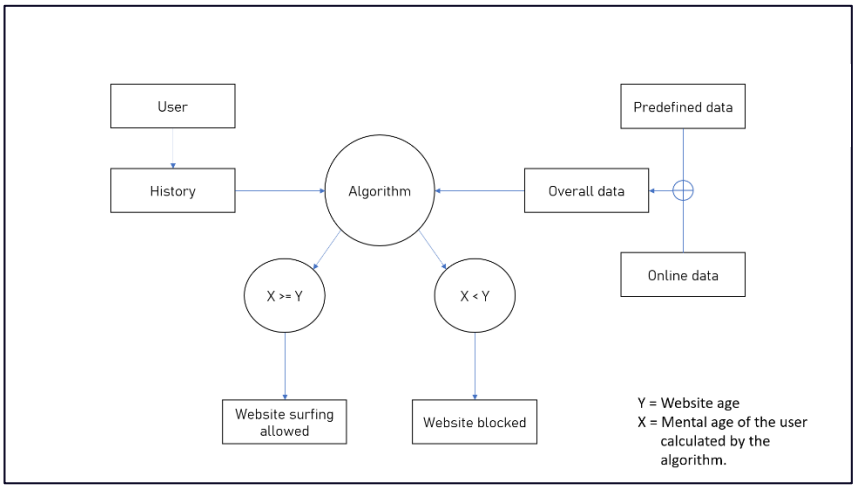
ML Tools and Frameworks used:

A **convolution Neural Network (CNN)** is formed which searches for Images in a Webpage and compare them with a pre-defined dataset and if a certain image crosses the threshold, it will use the Blur Filter and convert the Image into a blurry one and then give warnings/red alert Notifications on User's mail/number.

Mental-Age Analyzer:

This tool will render the Search History of the user and analyze the pattern of the search with user's permission and then based on its results, it will predict a Mental Age of that user and restrict websites accordingly. This prototype will reduce the frequency of children accessing the adult sites and malicious webpages. This will work as child lock basically, but it is dynamic in nature and locks sites according to mental age with a certain threshold for physical age as well.

It will also suggest guidelines and useful websites for that certain age level and also keep a count of such websites, but rather than sending messages to the parents it will give warnings to children and explain them the negative side of this internet.



ML Tools and Frameworks used:

A dense Neural Network which will render the Search History and predict a Mental Age(x) using the Cyber Cell Database*. Using **Collaborative and Content-based Filtering** several Guidelines and Webpages are recommended to the user. A database of all Major websites is created and a mental age(y) is predicted for each of the using Comment Section and its daily audience. “x” is then compared with “y” and restriction are imposed on several websites.

> ***“All prototypes will be developed keeping in mind the Privacy of the child and their freedom of Search since we want to educate the children and make them aware of Online Child Abuse and keep them safe without imposing highly strict Laws.”***

COMBINED APPLICATION:

A full-fledged App/ Webpage is developed which incorporate all the above features all together and also contains all general guidelines from Indian Government. Cyber Units Phone Numbers, in-shorts, Updates about latest cases, etc.
Feedback form at the end will help us collect more data which will improve the efficiency of all our Prototypes.