# A Survey On The secure Mobile teen: looking at the Secret World of Children

Pratiksha Kadam, Megha shendge, Aishwarya Mandlik, Pooja Rawal, Prof. Supriya Bhosale
Information Technology, D Y Patil College of Engineering, Ambi

**Abstract:** Security and privacy of mobile users could also be a topic of primary importance, given the widespread and growing use of connected smartphones, the great amount of personal data which is able to leak, and thus the shortage of proper controlled environments within the present mobile scenario (for instance, mobile apps and their handling of permissions). During this paper we specialize in a crucial a vicinity of this scenario: usage of mobile by teenagers. We preliminarily report on an ongoing study that for the first time analyzes truth potential risks that children face when using their smartphones. The foremost novelty is to travel beyond the use of questionnaires, which are a typical and handy tool but that introduce bias within the analysis and are limited with regard to the amount of data they're going to collect. Instead we collect data employing a parental control approach: with prior consent of the parents, the smartphones of underage children are controlled and analyzed in disguise, so as that they are actually unaware of the monitoring. This permits to know the important, unfiltered behavior of kids, and to ascertain on the potential risks for privacy and security during their mobile interactions. Here parent add relations account by capturing face, assign deadline supported age. Loved one login by using face and access data. The obtained results, gathered from an honest pool of teens, shade new light on the doubtless dangerous zones that underage children cross on a daily basis, and quantitatively provides a footprint of unsafe activities. the purpose of view of the parents is additionally considered, checking on how their perception about sons and daughters mobile use is accurate, or if there's actually a digital divide that has got to be filled, via awareness, education, dialogues and better privacy tools for the underage generations.

**Keywords:** Machine learning, Face Detection, Android, Time Limit.

## I. INTRODUCTION

Providing education to children is to form a far better communication between parents and them [1]. the youngsters can think and choose on something that they face. the opposite benefits are to form them do the well communicated with another person. Children have started hanging out with their
peers and start to interact with their environment. But now many children are more often played gadgets instead of playing out and socialize with their peers. The negative content can include elements of violence, pornography, crime, and so on. These elements can come from anywhere, such as: video, games, television, and internet. Whether it's considered good or bad, children watch tons of video, and therefore the amount of your time they spend viewing continues to extend [2]. If children spend longer with the gadget it'll cause the individualist nature and lack of sensitivity to the encompassing environment.

## LITERATURE SURVEY

Cyberbullying has been identified as a crucial problem amongst youth within the last decade. This paper reviews some recent findings and discusses general concepts within the world. The review covers definitional issues like repetition and power imbalance, sorts of cyberbullying, age and gender differences, overlap with traditional bullying and sequence of events, differences between cyberbullying and traditional bullying, motives for and impact of cyber victimization, coping strategies, and prevention/intervention possibilities. These issues are going to be illustrated by regard to recent and current literature, and also by in-depth interviews with

nine Swedish students aged 13–15 years, who had some first-hand experience of 1 or more cyberbullying episodes. We conclude by discussing the evidence for various coping, intervention and prevention strategies [1].

Cyberbullying, a contemporary sort of bullying performed using electronic sorts of contact (e.g., SMS, MMS, Facebook, YouTube), has been considered as being worse than traditional bullying in its consequences for the victim. This difference was mainly attributed to some specific aspect that are believed to differentiate cyberbullying from traditional bullying: an increased potential for an outsized audience, an increased potential for anonymous bullying, lower levels of direct feedback, decreased time and space limits, and lower levels of supervision. This studies investigated the relative importance of medium (traditional vs. cyber), publicity (public vs. private), and bully's anonymity (anonymous vs. not anonymous) for the perceived severity of hypothetical bullying scenarios among a sample of Swiss seventh- and eight-graders (study 1: 49 this feminine, mean age = 13.7; study 2: 49 this feminine , mean age = 14.2). Participants ranked a group of hypothetical bullying scenarios from the foremost severe one to the smallest amount severe one. The scenarios were experimentally manipulated supported the aspect of medium and publicity (study 1), and medium and anonymity (study 2). Results showed that public scenarios were perceived as worse than private ones, which anonymous scenarios were perceived as worse than not anonymous ones. Cyber scenarios generally were perceived as worse than traditional ones, although effect sizes were found to be small. These results suggest that the role of medium is secondary to the role of publicity and anonymity when it involves evaluating bullying severity. Therefore, cyberbullying isn't a priori perceived as worse than traditional bullying. Implications of the results for cyberbullying prevention and intervention are discussed[2].

We present an approach to the detection and identification of human faces and describe a working, near-real-time face recognition system which tracks a subject's head then recognizes the person by comparing characteristics of the face to those of known individuals. Our approach treats face recognition as a two-dimensional recognition problem, taking advantage of the very fact that faces are are normally upright and thus could also be described by alittle set of 2-D characteristic views. Face images are projected onto a feature space ("face space") that best encodes the variation among known face images. The face space is defined by the "eigenfaces", which are the eigenvectors of the set of faces; they are doing not necessarily correspond to isolated features like eyes, ears, and noses. The framework provides the power to find out to acknowledge new faces in an unsupervised manner[3].

Parental control software enables parents to support risk-management of their children's digital media use. However, tools to support online opportunities are left unexplored. This paper presents an explorative inquiry into stakeholder values associated with parental software for young children, employing a Value Sensitive Design approach. By studying values, we aim to illuminate design of parental software solutions that are aware of the problems families find most vital. We engaged in value exploration of corporate and parental values, and conducted a workshop with the company stakeholders to align stakeholder values. The results highlight the importance of values like 'control for safety' and 'involvement' within the development of parental software for young children. The contribution of this paper lies within the understanding of stakeholder needs and values concerning software tools that balance online risks and opportunities for young children [4].

We present an approach to content control where parents and youngsters collaboratively configure restrictions and filters, an approach that focuses on education instead of simple rule setting. We conducted an initial exploratory qualitative study with results highlighting the importance that oldsters place on avoiding inappropriate content. Building on these findings, we designed an initial prototype which allows parents and youngsters to figure together to pick appropriate applications, providing a chance for folks to teach their children on what's appropriate. A second qualitative study with parents and youngsters within the six to eight year-old age bracket revealed a positive response to the present approach. Our results suggest that oldsters felt that this approach helped facilitate

discussions with their children and made the education more enjoyable and approachable, which children may have also learned from the interaction additionally, the approach provided some parents with insights into their children's interests and understanding of their notions of appropriate and inappropriate content [5].

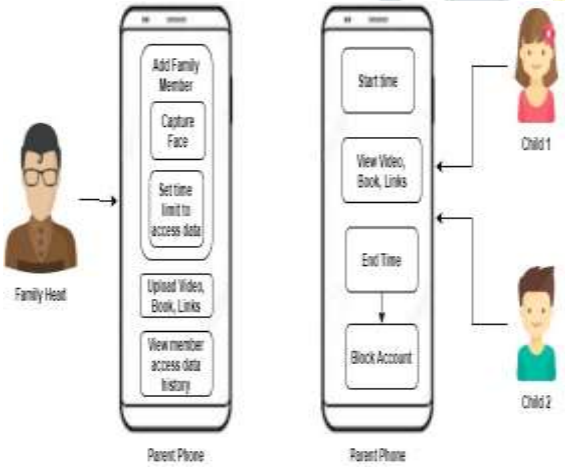
## II. PROPOSED SYSTEM:

During this paper, family head voice and login to the smartphone. Family head have all authority for access smartphone, like add loved one by using face, and regulation, on the idea aged family head set time interval for members. When member login then first capture member face by using voila Jones and LBPH algorithm that detect face and recognize face. Then deadline start for the member, access data that are uploaded by head, when time; limit ends system automatically block member account.

## III. ADVANTAGES:

◦ This system track all children access data.

◦ By providing deadline to the youngsters for access data. System Architecture:




## IV. ALGORITHM DETAILS

Viola-Jones

1. Initialize the weights
2. Normalize the weights
3. Select the best weak classifier (based on the weighted error)
4. Update the weights based on the chosen classifiers error
5. Repeat steps 2–4 T times where T is the desired number of weak classifiers

## CONCLUSION

In this paper, we study for the primary time had a glance at the access control of youngsters for the mobile context, fixing the essential focus points of interest, and a strategy to securely collect the relevant data and analyze it. in out project family head voice and login to the smartphone. family head have all authority for access smartphone, like add loved one by using face, and regulation , on the idea aged family head set time interval for members. When member login then first capture member face by using voila Jones and LBPH algorithm that detect face and recognize face. then deadline start for the member, access data that are uploaded by head, when time ;limit ends system automatically block member account. Our system are more efficient that existing systems.

## REFERENCES:

[1] Robert Slonje Peter K.Smith Ann Frisen, " The nature of cyberbullying, and strategies for prevention ", Volume 29, Issue 1, January 2013, Pages 26-32.

[2] Hind Baqeel, Saqib Saeed, "Face detection authentication on Smartphones: End Users Usability Assessment Experiences ", 978-1-5386-8125-1/19/$31.00 ©2019 IEEE

[3] Matthew A. Turk and Alex P. Pentland "Face Recognition Using Eigenfaces", DOI: 10.1109/CVPR.1991.139758

[4] Bieke Zaman "A value sensitive design approach to parental software for young children", https://doi.org/10.1145/2771839.2771917

[5] E. Young "Involving children in content control: a collaborative and education-oriented content filtering approach", DOI:10.1145/2556288.2557128