Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims

H2020 – 101021801

www.heroes-fct.eu

D5.8 Anti-Grooming Mobile App

Authors: Jesús Alonso López (UCM), Luis Javier García Villalba (UCM), Luis Alberto Martínez Hernández (UCM), Sandra Pérez Arteaga (UCM), Daniel Povedano Álvarez (UCM), Ana Lucila Sandoval Orozco (UCM)

Deliverable nature	Demonstrator (DEM)
Dissemination level	Public (PU)
Version	1.0
Date	30/11/2023

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021801

Document Information

Project Acronym	HEROES
Project Title	Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims
Grant Agreement No.	101021801
Project URL	www.heroes-fct.eu
EU Project Officer	Elina Manova

Deliverable	**Number**	D5.8	**Title**	Anti-Grooming Mobile App		
Work Package	**Number**	WP5	**Title**	Multi-Sectoral and Multi-Disciplinary Strategies to Improve and Reinforce Prevention Programs		
Date of Delivery	**Contractual**		30/11/2023		**Actual**	15/01/2024
Status	Version 1.0				Final	
Nature	DEM		**Dissemination Level**		PU	

Responsible partner	**Name**	Luis Javier García Villalba	**E-mail**	javierv@ucm.es
	Partner	UCM	**Phone**	+34 913947638
Contributing partners				
Reviewers	Pablo Gallegos (IDENER RD), Olivier Huynh (INRIA)			
Security Approval	Julio Hernandez-Castro (UNIKENT)			

Abstract (for dissemination)

Sexual harassment of minors is one of the risks present today on the Internet for minors when using mobile devices. Harassers often identify their potential victims on social networks. Using social engineering techniques, they try to establish contact with them through instant messaging applications. The aim of this tool is to detect grooming attempts at an early stage. For this purpose, a couple of mobile applications have been developed, one to be installed on the child's cell phone and the other on the parent's cell phone.

Keywords	Deep Learning; Federated Learning; Grooming; Mobile devices

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021801. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

Version History

Version	Date	Change Editor	Changes
0.1	09/08/2023	UCM	Structure of the document
0.2	01/11/2023	UCM	Initial draft
0.3	21/11/2023	UCM	UCM internal review
0.4	12/12/2023	IDENER RD	HEROES consortium internal review
0.5	17/12/2023	INRIA	HEROES consortium internal review
0.6	19/12/2023	UNIKENT	SAB Review report
1.0	14/01/2024	UCM	Final version for submission

Table of Contents

List of Figures

List of Tables

Executive Summary

Sexual harassment of minors is one of the risks present today on the Internet for minors when using mobile devices. Harassers often identify their potential victims on social networks. Using social engineering techniques, they try to establish contact with them through instant messaging applications. The aim of this tool is to detect grooming attempts at an early stage. For this purpose, a couple of mobile applications have been developed, one to be installed on the child's cell phone and the other on the parent's cell phone.

1. Introduction

Nowadays, information and communication technologies provide an amazing set of tools that improves the communication process and the exchange of information via the usage of mobile devices, computers etc. This includes all types of users, minors to perform school work and adults in their daily work activities. Such technologies are also used to be in communication with friends, family and work contacts.

Furthermore, minors are exposed on social networks sharing unconsciously sensitive information. This may be used by malicious users to get in contact with them, putting their physical or mental integrity at risk via online child harassment. Online child grooming is defined as the process of approaching, persuading and involving a minor (victim) in sexual activity through the use of digital tools, and has opened up the possibilities for perpetrators to commit this crime on a large scale. The phenomenon of grooming is on the rise, and although there are tools that allow controlling the use of the device or limiting pages that a minor or adolescent can access, it is not enough as it does not allow completely eradicating the process. On many occasions the interaction with the minor starts on social networks such as Facebook or Instagram or even on online video game platforms, and once the adult gains the child's trust, the adult has closer contact with the child.

In order to tackle this problem, HEROES proposes the development of an anti-grooming application (AGApp) to detect and block grooming attempts in early stages on mobile devices of minors or adolescents. The app will have the ability to analyze the multimedia contents of the minor's device to detect those with inappropriate content. An alert will be sent to parents so that they can take appropriate measures.

1.1. Purpose and Scope of the Document

This document presents the Antigroming tool's design. It establishes a solid basis for the planning and execution of the software development by ensuring that the tool's functions are understandable. The tool focuses on early detection and prevention of grooming.

1.2. Objectives

To design an application that allows the detection, identification and blocking of attempts to harass minors at early stages and analysis of multimedia content with sexual content on the minor's device.

1.3. Motivation

Online grooming is a growing and alarming risk faced by children and adolescents in today's digital age. The main motivation is to help minors, adolescents and children not to become victims of grooming and to be able to use technology safely and thus, safeguard their well-being, physical and mental integrity and help them not to fall into dangerous situations. In other tasks of the project HEROES we will complement this approach by educating minors to help them to use technology in a responsible way, contributing to the creation of a safer and more ethical online society.

Creating an anti-grooming tool is an opportunity to contribute to building a safe and secure environment for children online. This tool can play a crucial role in the early detection of inappropriate and dangerous behaviour, allowing for quick. The tool provides parents and guardians with an effective way to protect their children in the digital world. This gives them peace of mind and allows them to take preventative measures to ensure the online safety of their loved ones.

1.4. Structure of the Document

This document is organized as follows: Section 1 presents this document's objectives and motivation, while Section 2 collects information on grooming and work related to what the state of the are solutions as well as the Machine learning models that can be used in our approach. In Section 3 we provide a profuse description of the HEROES' anti grooming tool. Later in Section 4 we describe the application operation is explained. Finally, we draw our conclusions in Section 5.

2. State of the art

2.1. Grooming Process

In a digital world where Information and Communication Technologies (ICT) have developed new forms of social interaction, the use of instant messaging applications (IMA) on mobile devices and communication technologies are extremely useful in the development of different activities such as school homework, professional work and also leisure activities such as communicating with friends and family. Communication at a social and individual level helps in the development of individuals of all ages. The most frequent online social activities among adolescents include sending emails and visiting social networking sites such as Facebook, Twitter and Instagram, while half of adolescents regularly make video calls (e.g. WhatsApp) and upload photos or texts about themselves to the Internet. ICTs provide new opportunities for adolescents to establish and maintain intimate relationships, as well as to explore their sexuality [2]. The use of media by children has helped parents to be in contact with them when they are at school or in case of emergency. However, young people are particularly vulnerable to becoming victims of online violence or abuse [3].

Minors may face several online risks due to their vulnerability and lack of experience in the use of the Internet. This can include as cyberbullying, grooming, inappropriate content on different websites, scams, technology addiction, violence in online games, leaking of confidential information on social networks or unsafe websites due to privacy issues when using these platforms, downloading inappropriate content or viruses and even distraction in learning from their academic responsibilities, Figure 1.

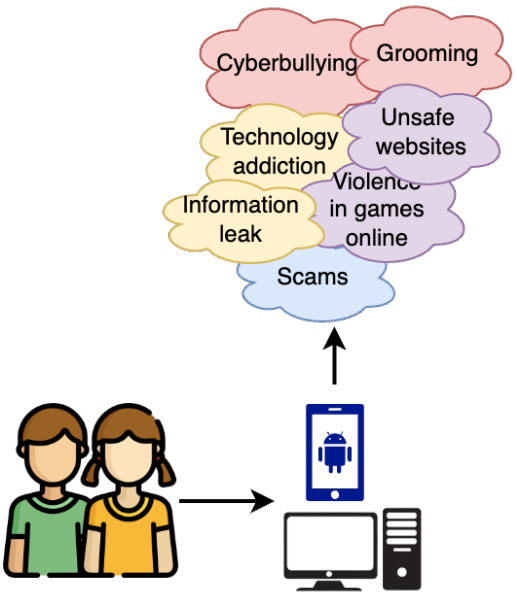


Figure 1: Online risks.

Online grooming is considered to be a relationship based on trust between a child and an adult who uses ICT to seduce and systematically abuse children for sexual purposes. A potential adult abuser befriends a child to gain his or her trust [3]. Grooming is defined as the criminal activity of befriending a child, especially over the Internet, to try to persuade him or her to have a sexual relationship [4].

Grooming is a serious social concern. The media report almost daily on children who have been sexually abused after being persuaded on the Internet. Grooming involves a process of creating sympathy, friendship and manipulation of children in abusive relationships in order to persuade them into personal sexual encounters [5]. Grooming is an umbrella term used to describe a wide range of sexual activities that take place between a child and an older person, in which the child does not fully understand and cannot give consent. Child sexual abuse is not exclusively committed through physical contact (e.g. rape, molestation, masturbation); it can also take place in the form of non-physical contact through the internet or grooming (e.g. production of child pornography, online harassment, exhibitionism) [6].

Grooming is a complex process, in which it can take days, months or years to the offender to gain access to children, gain their trust, maintain the relationship and avoid disclosure by the child [7]. Different victim roles articulate qualitatively different variants of the established components of control deficit and empathy in sexual and violent offending, contributing to the debate about the functioning of these components and having important implications for treatment [8].

Some of the objectives of grooming include:

- Production of images and videos with sexual connotations or activity, intended for the personal consumption of paedophiles or child sexual abuse networks. The request for images or videos of a sexual nature is in itself an abuse. Although sometimes it is the child who sends this content "voluntarily", manipulated in any case by the offender, on other occasions the victim is blackmailed into providing the compromised materials. Ultimately, the perpetrator may carry out physical sexual assaults, compromising the physical and emotional safety of the child.
- Face to face encounters with the child and physical sexual abuse.
- Sexual exploitation and child prostitution.

When grooming is committed, those involved may present some psychological characteristics that may attract the attention of family members, such as anxiety and depression due to the abuse they are subjected to, as well as problems derived from academic performance. A grooming situation seriously affects all areas of a child's daily life, from damage to self-esteem and self-confidence, to decreased concentration and attention in class, to loss of friendships. Victims often do not talk about what is happening because they feel ashamed or guilty or feel that the relationship they have with their perpetrator is real [9].

Through a survey of more than 5,300 young people aged 18 to 20 who had regular access to the Internet as children, WeProtect found that 57 percent of girls and 48 percent of boys had experienced at least one sexual harm online, and in some regions - such as North America, Australia and Western Europe even higher [1], Figure 2.

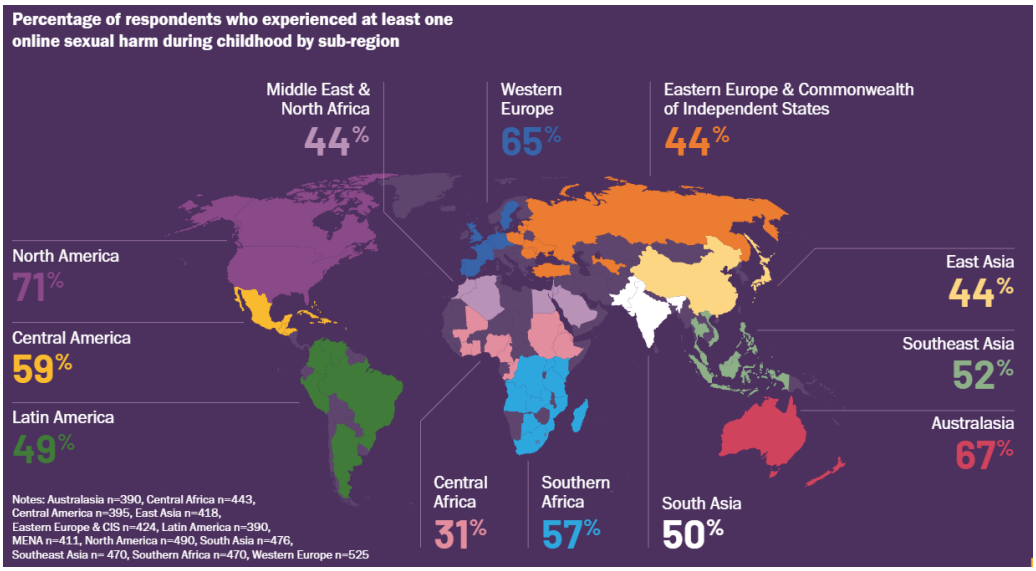


Figure 2: Porcentage online sexual harm during by sub-region [1].

According to official statistics, 2% of those who commit sexual offences are women, the majority of whom are child victims. However, victimisation surveys suggest that the actual rate of child sexual abuse perpetrated by women is significantly higher than official statistics, and that it is under-detected and under-reported. Compared to men, relatively little is known about the behaviours and tactics used by women to perpetrate child sexual abuse [2].

The National Institute of Statistics and Geography (Inegi) report that, between October 2019 and November 2020, 21% of the population aged 12 and over who use the internet were victims of cyberbullying, representing

77.6 million people in the country, 40.4 million women and 37.2 million men. During this period, 27% of internet users between the ages of 12 and 17 reported some form of cyberbullying; within this group, more girls than boys were cyberbullied. The situations considered as cyberbullying, in the case of girls, were mainly: Offensive messages (44%); Sexual advances or propositions (35%); Provocations to react negatively (34%); and Contact through false identities (32%) [10].

Grooming statistics in Latin America confirmed 26.3% children knowing another child who has been a victim of grooming, 52.9% of these children are between 11 and 15 years old, and 33.7% are between 7 and 10 years old [11].

Out of all CSAM reports received by the Internet Watch Foundation (IWF), based in the United Kingdom (U.K.) in 2022, 40% of victims appeared to be children 0-10 years of age, and 59% of the victims appeared to be children 11-15 years of age.1 The IWF reported a 60% increase in content depicting pre-pubescent children (ages 7-10 years). Moreover, the IWF reported there was a 129% increase in "self-generated" imagery for children ages 7-10 years of age in 2022 compared to 2021, [12]

2.1.1. Stages of grooming

There are stages and patterns of behaviour that are repeated in the grooming process which are mentioned below [13], [14].

Table 1: Stages of grooming

States	Definition
Friendship forming stage	By attempting to establish a relationship of trust with the child, the offender creates the possibility of sharing sensitive information. The perpetrator requests photos to prove that the young person is really a child through bribery or fraud. To do this, he often poses as someone much younger than the victim. In addition, the offender may give gifts, show empathy, gain the children's trust by appearing to listen to their concerns and establish their loyalty before using that information to blackmail the child.
Relationship-building and victim isolation stage	To trick the victim into believing that the bully cares about their problems and has a relationship with them, they talk about their families, schools, interests, and hobbies. As a result, the abuser isolates the victim from her support system (His/her friends, family, teachers, etc.), leaving her vulnerable. He/She highlights the need to keep things secret in this way.
Risk assessment stage	The perpetrator tries to gauge the level of threat and danger by talking to the minor and always securing his position. He asks the victim if anyone else knows about her relationship and assures her that the boy is alone, that no one else is listening to his conversations, and that no one else has access to the computer or other device he uses.
Conversations about sex stage	In this stage, the abuser uses the concepts of love and care once he feels safe and progressively begins to have sexual conversations trying to familiarize the victim with the sexual topic as well as the terminology.
Requests of a sexual nature stage	The main objective of online grooming is achieved at this point when the victim provides the offender with sexual material, discloses sexual fantasies or the relationship progresses to physical contact under the use of manipulation, threats, blackmail or compulsion.
Conclusion stage	In this stage, the perpetrator approaches the minor to meet face to face and conclude the goal that the predator has.

These aforementioned stages may or may not occur chronologically and may vary depending on the manipulation that the aggressor has with the victim.

2.1.2. Grooming prevention

Online grooming is a long process which most of time starts performing social engineering on minors in order to obtain information about their life, schedules, where they live, etc. The final target for offenders is to have a sexual act. It can be prevented so that the perpetrators do not comply with the objective and thus help minors so that they do not go through such a process of violence.

ICT tools shouldn't be criminalized since they help us perform different tasks and stay in touch, but minors can be taught to navigate safely, be aware with whom to share sensitive information, and so on. also interact with known people and not accept strangers on social networks and the type of information they share on social networks from their daily lives and the safe and responsible use of digital tools.

Generally, victims of grooming do not tell their family members, a trusted person or legal representative what

they are going through. Specialists recommend reporting the facts immediately when someone becomes aware of the abuse since the aggressor may have more victims [15].

The most important thing is to educate minors so that they are aware of the risks and threats that exist in the use of the Internet. Also make teenagers aware of the real cases that happen all over the World and read news about it in the media. Establish a safer age criteria for starting to use devices (computer, tablets, mobile devices) and for accessing different content and services. It is recommended that sex education is taught along with the risks involved in surfing the Internet for minors in order to prevent any type of psychological or physical violence.

In addition, it seems very relevant teaching minors on how to use tools safely, such as configuring privacy options, applications and services and determining what information is accessible. Recommend habits such as not entering unreliable websites, using strong passwords and updating them regularly. Help them to have a critical sense when accepting strangers on social networks, online games and messaging services. Asking themselves whether they know the person physically, who they are, and whether their close environment knows about them and what information they can provide to strangers or people in their environment. Limit the times of use to avoid dependency and conflict with other activities such as study. Be aware of minors' moods and attitudes, ask them directly if they have been harassed at any time or if they know of any cases of this kind in their environment [15], [13].

The most important points that can be put into practice in order to prevent grooming are [9]:

- Establish safe surfing habits by emphasising responsibility and your safety when you go online.
- Establish timetables for use and the place to use these devices, making sure that they are in common spaces and not isolated in their own rooms.
- Caution when conducting online conversations. Sometimes the attacker may be someone you know in person. Therefore, in any online conversation we must be careful when sharing personal information.
- It is advisable not to contact or plan dates with people you do not know in person, as on the internet it is easy for the perpetrator to impersonate a different person by changing their name, age, likes and dislikes, work and personal information so that they have something in common with the victim.
- Talking naturally about love and sexuality with minors and helping to differentiate between healthy and unhealthy relationships.
- Accompany and supervise them, as children's access to the internet should be progressive and supervised by an adult, so that they gradually learn how to use new technologies in a safe and responsible way. For the youngest children, parental control systems can be installed on the devices and applications that have them implemented, thus limiting their use and supervising their activity.

The aforementioned points can be seen in the Figure 3.

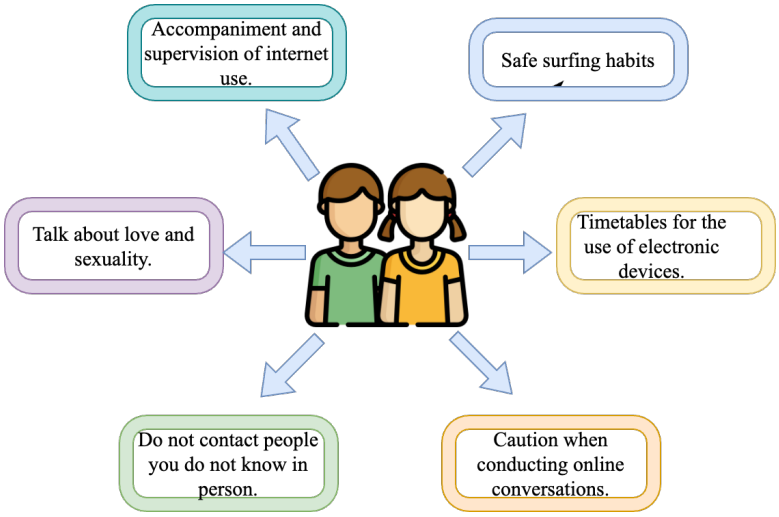


Figure 3: Grooming prevention.

2.2. Detection of Multimedia Content on Mobile Devices

The importance of detecting multimedia content with explicit content on mobile devices is key since minors shouldn't generate nor see sensitive content on their mobile device.

Artificial intelligence algorithms are commonly operated in computers with high computational complexity and processing power for training AI models, making it faster and more agile as it consumes the resources of a computer. When image processing or video classification is performed on a mobile device to identify a person or object, it is done using a lower computational cost algorithm to avoid latency, high memory consumption, high battery consumption and other potential problems. Today, deep learning models are frequently used for image classification and recognition [16].

Mobile models have been used in different fields of knowledge, e.g. to classify images of skin lesions [17], images of skin diseases [18], skin cancer images [19], facial expression recognition [20]. Fields where modelling has been used to improve and automate processes include botany, medicine, manufacturing and digital forensics, among many other areas [21].

The following models **Convolutional Neural Networks (CNN)** were created for use on mobile devices because they have significantly fewer hyper-parameters than computer-oriented models. Their main features are:

- They take up less memory space.
- They can be transferred from the computer to the mobile phone.
- They are light on size and resource usage.
- They meet the resource constraints of mobile phones.
- They meet the speed objectives that users need in an application, without encouraging their mobile device.

2.2.1. MobileNet

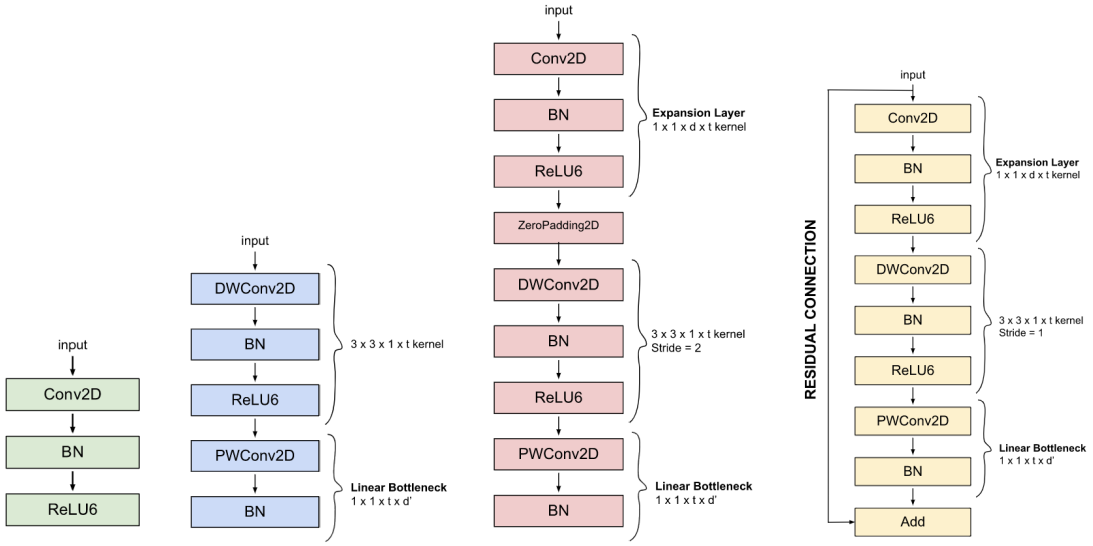
MobileNet is a model that can be deployed on mobile devices to satisfy the needs of Artificial Intelligence in the mobile application market, due to the low amount of parameters required for data training, the low latency in the processing of inferences and the low consumption of computational resources. MobileNet consists of an architecture based on depth-separated convolutions, which allows the model to be quite lightweight and efficient. This model is used for classification, detection, integration and segmentation, and is used in a similar way as other large-scale models [19] [22].

- **MobileNetV1** uses in its architecture **Depthwise Separable Convolutional Layers (DSC)** instead of **Standard Convolutional Layers (Conv)**. Both types of layers are used to obtain the most important

features of the images, these features are then used by the model to classify an image into a class. By using **Conv** the model adds many mathematical operations (multiplications), in the execution of the model training. However, when extracting the most important features from the images, it is not possible to do without them. So the solution for the MobileNetV1 architecture was to replace them with the **DSC** to separate the spatial operations (height and width) from the depth operations, achieving the same results, but with much less mathematical operations and faster, opting to use a kernel of size 3x3 obtaining better results [23].

- **MobileNetV2** This is the second version of the MobileNet model which significantly improves the accuracy and inference time of the model. This update contains a full convolution layer with 32 filters and 19 bottleneck layers and direct access connections [19] [24]. MobileNetV2 uses **DSC** with the same core size as MobileNetV1; *altura* × *anchura* equal to 3x3, the computational cost with respect to **Conv** in operations is also 8 to 9 times lower. It is a new block called Inverted Residual with Linear Bottlenecks [25].
- **MobileNetV3:** This version of the model is based on the EfficiencyNet search method with specific parameter space objectives required for use on mobile devices. It is a lightweight model that allows image classification with reduced inference time and is adaptable to architectures with low computational resources [26] [21].

In the Figure 25 you can see the blocks that make up the model and how the residual connections are applied in MobileNetV2.



(a) Conv2D (b) Block 1 (c) Block 2 (d) Block 3

Figure 4: Some of the principal blocks that conform the body of MobileNetV2

MobileNet architecture is based on a simplified architecture that uses depthwise-separable convolutions to construct deep and lightweight neural networks. Depthwise convolution consists of two convolution operations: depthwise convolution and pointwise convolution. Depthwise convolution applies separate convolutions to each channel of the input tensor, i.e., a traditional n × m convolution on a colour image. Subsequently, the product activation maps of the convolution operations are concatenated on the depth axis. A traditional 1 × 1 convolution is then applied to the resulting tensor (pointwise convolution), which combines the channels of the concatenated activation maps. [27].

The MobileNet model is based on depthwise separable convolutions which is a form of factorized convolutions. This convolutions factorize a standard convolution into a depthwise convolution and a pointwise convolution, forming convolutions by filtering and combining. Two simple global hyperparameters are introduced named width multiplier and resolution multiplier, which efficiently trade off between latency and accuracy. that the network is different from the standard convolutional neural network. The 3×3 Depthwise convolution and the

1×1 convolution are calculated as two independent modules, and then perform BN (Batch Normalization) and ReLU (Rectified Linear Unit) activation functions [28].

The unique characteristic of MobileNet is that it uses depthwise separable convolutions which can be thought of standard convolutions split into depthwise convolution and 1 by 1 pointwise convolution [29].

- **Depthwise Convolution**: This layer is where the filtering of the image is performed and the most important features of the image are obtained. The procedure is performed by separating the channels of the input image as three independent matrices of the form $height \times width \times 1$. Each kernel depth layer is repaired and worked on as if they were three independent kernels of the form 3x3x1. When you have the three input channel matrices and the three distinct kernels, you perform scalar multiplications on them. Therefore, each kernel iterates over one of the three channels so that, in total, we will have three kernel-matrix pairs to perform the operations, Figure5, [25].

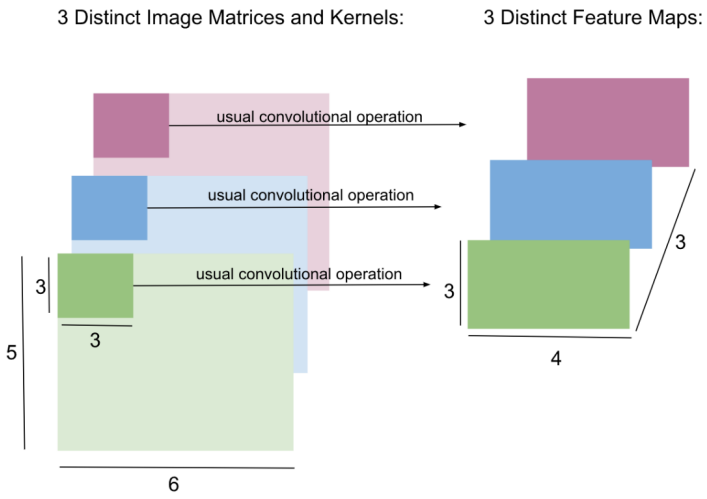


Figure 5: Depthwise Convolution

- **Pointwise Convolution**:Since we want to get the same shape of the output tensor as we got in normal convolution operations, 3x4x1, we must apply this layer, as it deals with the depth operations. What is achieved in this layer is that, by combining the three feature maps, it obtain new features that can be useful for the model to learn. Specifically, this layer uses a kernel of size $1 \times 1 \times$ DEP T H (in DEPTH of the kernel will be equal to 3). The kernel will have to iterate through the height $\times$ width of the feature maps obtained in the Depthwise Convolution Layer (DW CONV) layer in order to traverse all of their pixels and, perform the convolution operation to combine them in each iteration. The spatial dimensions of the kernel is what gives the particular name "pointwise" to this layer, since being 1x1 it is as if it were a point. The process is represented in the Figure 6, and, in Figure 7 it show an example of the convolution operation performed in each iteration to extract each value of the final feature map [25]

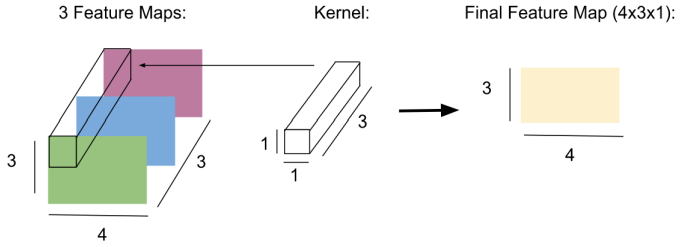


Figure 6: Pointwise Convolution

2.2.2. EfficientNet

EfficientNet was created using MobileNetV2's inverted residual blocks as an architecture type combined with the MnasNet search strategy [26]. These smaller blocks did not exist when MnasNet was created and, by using

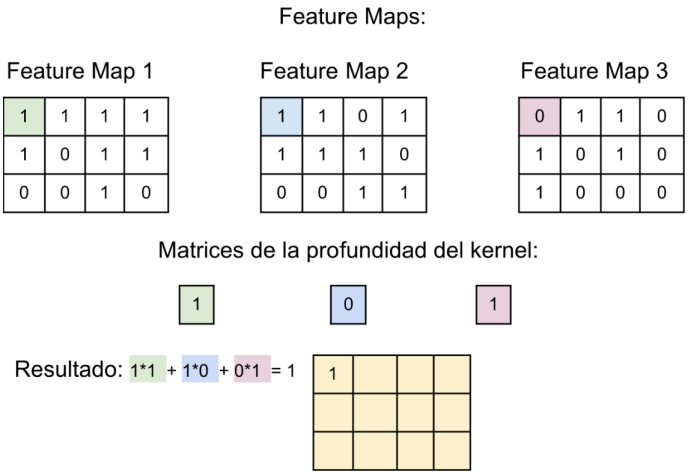


Figure 7: Operation of Pointwise Convolution to extract 1 value of the Final Feature Map

them, the found a significantly improved set of networks. In addition, finding a scalable and reliable set of heuristics to build larger networks gave an initial starting point, which was the key limitation of evolutionary strategies [30].

Using the scaling efficiency of MobileNets and ResNet and the neural architecture are used to design a new neural network and obtain a set of models, called EfficientNets, achieving much better accuracy and efficiency. The EfficientNet model is a **Red Neuronal Convolucional (CNN)** that balances the depth, width and resolution of the network to improve performance, proposing a method which uniformly scales all depth/width/resolution dimensions by a composite coefficient limiting the width, length and resolution of the Convolutional Network to fixed ratios between these parameters. The composite scaling method is justified by the intuition that if the input image is larger, then the network needs more layers to increase the receptive field and more channels to capture more detailed patterns in the larger image [31].

EfficientNet focuses on accuracy and efficiency. Its computational model runs much faster with fewer parameters than other models. It uses model scaling, so in any model there are three types of scaling **Depth Scaling**. This is the most common form of scaling, basically, it involves creating a deeper model. **WidthScaling** refers to the width of the network (i.e. how many channels there are in a resolution layer), the advantage of having a wider model is that it is smaller. **ResolutionScaling** in a larger image is better for the model, but in practice, at high resolutions, for example, there is no significant difference between 500x500 and 560x560. [32].

EfficientNet architecture having the model scaling efficiency is also highly dependent on the reference network. Therefore, to further improve the performance, a new benchmark network has been developed by performing a neural architecture search using the AutoML MNAS framework, which optimises the **on thefloating-point operations per second (FLOPS)** (precision and efficiency). The scaling process improves the performance of the reference model. Therefore, the better the reference model, the better the final performance after scaling. The general method of composite scaling can be applied to other architectures such as ResNet, so the performance of the reference architecture is very important [33]. The resulting architecture uses mobile inverted bottleneck convolution **Mobile inverted Bottleneck Convolution (MBConv)**, similar to that found in the MobileNetV2 and MnasNet architecture, but is slightly larger due to a larger FLOP budget [34] as proposed in [31], Figure 8.

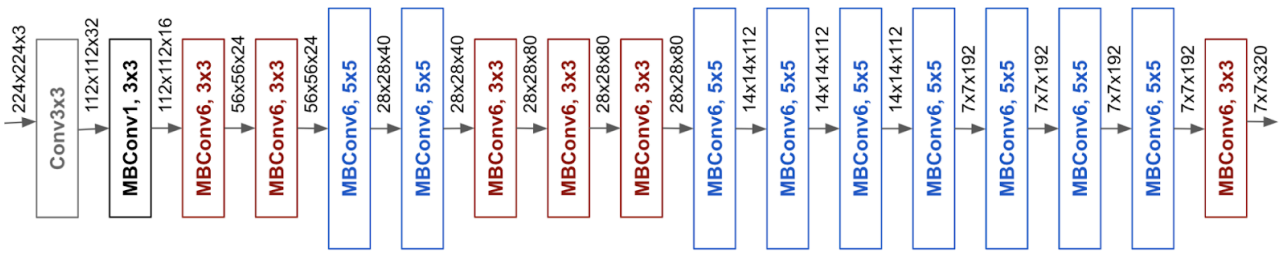


Figure 8: EfficientNet reference network architecture.

EfficientNet added a new scaling technique called composite scaling. This technique uniformly scales the depth, width and resolution dimensions initially. By scaling these dimensions, EfficientNet achieves better performance with fewer parameters and computations. It uses neural architecture search (NAS). NAS is a technique that automates the design of neural networks by searching across a variety of possible architectures. It uses a reinforcement learning-based controller to guide the search process, evaluating different architectures based on their performance on a validation set.

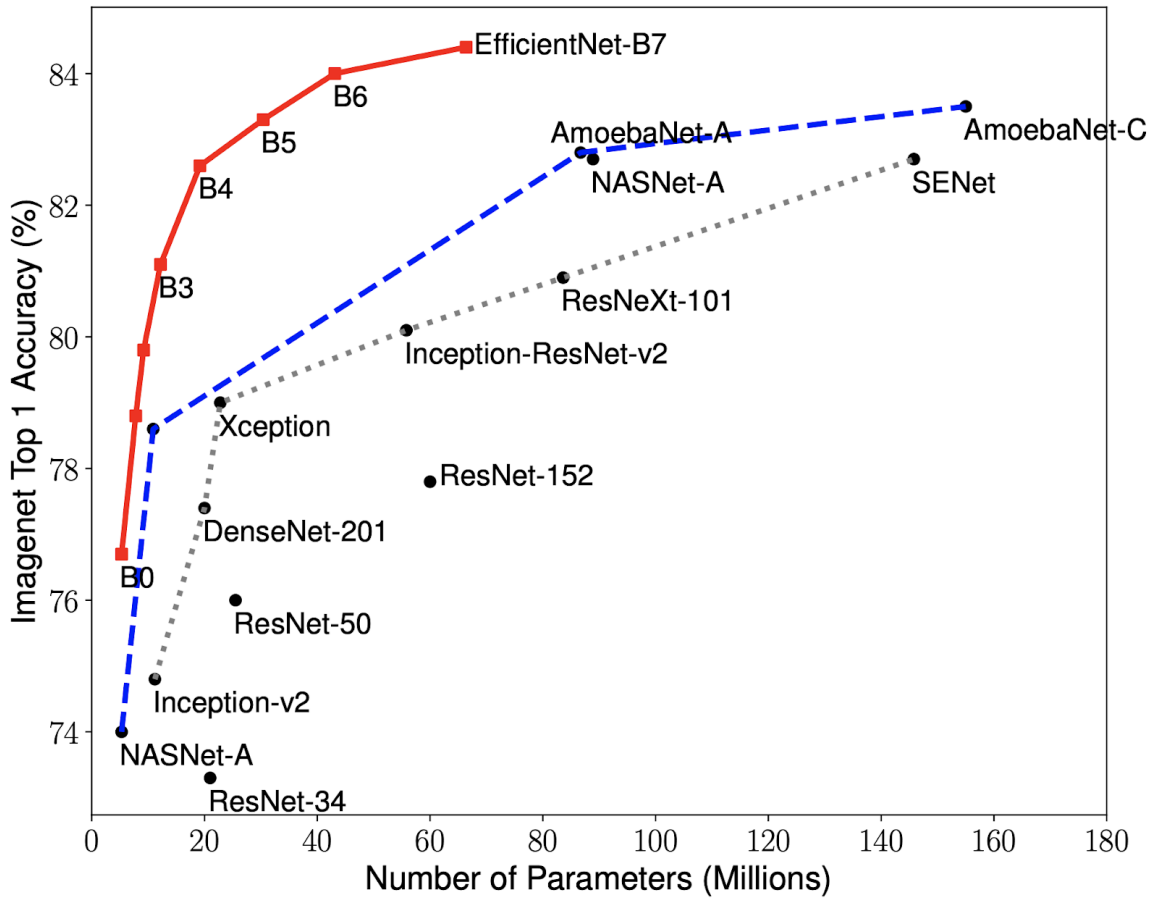


Figure 9: Accuracy of EfficientNet vs the accuracy of other algorithms.

EfficientNet's NAS process starts with a small-scale model and gradually scales up to find the optimal architecture. This approach ensures that the resulting model is accurate and efficient. The reference architecture is scaled up through compound scaling to obtain a family of EfficientNet models. The final architecture is scaled to different sizes, from EfficientNet-B0 to EfficientNet-B7, each offering a balance between accuracy and computational efficiency [35].

In Table 2, you can see the characteristics of each of the EfficientNet derived models from B0 to B7 where the input size in pixels, the number of parameters and the Accuracy are shown as follows [31], [36].

Table 2: Comparison of features of EfficientNet models.

Version	Input Size (px)	#Params	Accuracy
EfficientNetB0	224 × 224	4,057,253	76.3% / 93.2%
EfficientNetB1	240 × 240	6,582,914	78.8% / 94.4%
EfficientNet-B2	260 × 260	7,777,012	79.8% / 94.9%
EfficientNet-B3	300 × 300	10,792,746	81.1% / 95.5%
EfficientNet-B4	380 × 380	17,684,570	82.6% / 96.3%
EfficientNet-B5	456 × 456	28,525,810	83.3% / 96.7%
EfficientNet-B6	528 × 528	40,973,969	84.0% / 96.9%
EfficientNet-B7	600 × 600	64,113,049	84.4% / 97.1%

EfficientNetB0 allows for smooth scaling to produce larger and larger networks. Roughly speaking, each step of a larger network requires a square amount of computation.

In Figure 9 the high-accuracy regime of EfficientNet-B7 can be observed, which achieves 84.4x top-1 / 97.1x top-5 accuracy on ImageNet, while being 8.4x smaller and 6.1x faster in CPU inference than the previous Gpipe. Compared to the widely used ResNet-50, our EfficientNet-B4 uses similar FLOPS, while improving the top-1 accuracy from 76.3% of ResNet-50 to 82.6% (+6.3%). [37].

2.2.3. EfficientNet-Lite

EfficientNet-Lite, derived from the EfficientNet architecture. EfficientNet-Lite is optimized for edge devices (devices that generate data at the edge of the network and have connectivity (Bluetooth, LTE IoT,...)). This model is suitable to be deployed on resource constrained devices, such as cell phones due to the low number of parameters needed to train the model. [38].

EfficientNet-Lite eliminates compression and excitation networks, and replaces swish triggering functions with ReLU6 triggering to support the quantization required for edge devices [39]. ReLU: (Rectified Linear Units) are a type of linear activation function in the positive dimension, but null in the negative dimension. It replaces all negative values received at the input with zeros.

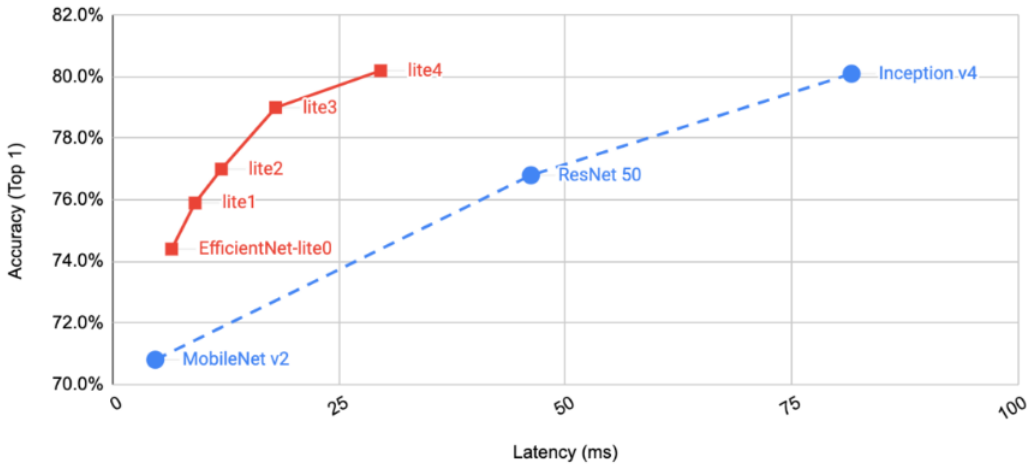


Figure 10: EfficientNet-Lite Latencia (ms) vs Accuracy (Top 1)

EfficientNet-Lite runs on TensorFlow Lite and is designed to deliver performance on mobile CPUs, GPUs and EdgeTPUs, features the power of EfficientNet on edge devices and has five architecture variants (EfficientNet-Lite0 through EfficientNet-Lite4), with Lite0 being the smallest and Lite4 the largest, allowing users to choose from the low latency/model size option (EfficientNet-Lite0) to the high precision option (EfficientNet-Lite4). The largest variant, EfficientNet-Lite4. In which the number of iterations from conv2d layer to conv2d layer RELU6 is different, e.g. 13 iterations for EfficientNet-lite3 and 8 iterations for EfficientNet-lite0. As for the architecture, the higher the number of variants, the more complex and larger it will be [38]. [40].

Figure 10 shows latency and accuracy where the largest variant, EfficientNet-Lite4 quantized with integers only, achieves 80.4% accuracy of ImageNet top-1, while still running in real time. The performance of the EfficientNet-Lite quantized models is shown in comparison to a similar quantized version of some popular image classification models [41].

2.3. Natural Language Processing for Mobiles

Natural Language Processing (NLP) is a field of knowledge that combines artificial intelligence, linguistics, statistics and computing techniques to develop algorithms and systems capable of analyzing, understanding, creating and interpreting human language intelligently expressed through text, speech and symbols. NLP, as a branch of artificial intelligence, uses machine learning to process and interpret text and data. Natural language recognition and generation are types of NLP [42].

NLP is a field of research and development that primarily performs the analysis and generation of written and spoken language, starting with tasks such as cryptanalysis and machine translation. NLP refers to the branch of computer science (and more specifically the branch of AI) that aims to endow computers with the ability to understand human text and spoken words. NLP combines computational linguistics (rule-based modeling of human language) with statistical modeling, machine learning and deep learning. Together, these technologies enable computers to process human language as text or speech data and "understand" its full meaning, as well as the intent and sentiment of the speaker or writer [43].

Human language is full of ambiguities that make it extremely difficult to write software that can accurately determine the intended meaning of text or speech data. Homonyms, homophones, sarcasm, idioms, metaphors, exceptions in grammar and usage, variations in sentence structure: these are just some of the anomalies in human language that take humans years to learn, but developers must program natural language-based applications to master them correctly to recognize and understand from the outset whether these applications are useful or not.

NLP is currently attracting special attention in the academic community. Language technologies are increasingly developed and their use is gradually spreading in professional fields with the aim of discovering, classifying, organizing or searching contents automatically, allowing a more efficient use of time, cost reduction and faster decision making in organizations. NLP applications are used to extract valuable information from unstructured text-based data and to access the extracted information in order to generate a new understanding of this data. NLP examples can be created with Python, TensorFlow and PyTorch [44] [45].

Several NLP tasks decompose human text and speech data in ways that help the computer understand what it is ingesting. Some of these tasks include speech recognition, part of speech tagging, word sense disambiguation, named entity recognition, co-reference resolution, sentiment analysis and natural language generation.

When NLP is used to perform the conversion to text, the processing after transcription is very similar and the purpose remains the same, to understand the meaning of a text or data in order to perform actions on or in response to that text input. The names given to the entities are:

- **Token**:A word or set of words having a common morphological structure.
- **Pooler**: Neural network layer used to compute a representation of all input text.
- **Entity**: Classification that is assigned to a token in which it generalizes into one or more predetermined classes.
- **Tasks *Downstream***: A fine-tuning task that inherits the parameters of the pre-trained model on which it is based.
- **Corpus**: Set of documents on which the model performs various necessary actions.
- ***Dataset***: Data sets structured in tabulated columns, typically used for statistical purposes.

2.4. Federated Learning

Over the past decade, the rise of deep learning has sparked amazing transformations in dozens of industries. It has revolutionized the autonomous car industry, fundamentally changed the way we interact with our devices, and innovated the approach to cybersecurity [46].

Federated learning is a Machine Learning (ML) environment in which different clients collaborating to learn a centralized model while keeping the client's data decentralized [47]. Federated learning or FL (sometimes called collaborative learning) is an emerging method used to train decentralized machine learning models (e.g., deep neural networks) on multiple edge devices, from smartphones to wearable medical devices, vehicles to IoT devices, and more. They collaboratively train (hence the second name) a shared model while keeping the training data local without exchanging it with a central location [48].

In order to ensure user's privacy, when a model is deployed on a mobile device using Federated Learning features, initially the device downloads from a remote server the base model (A), when there is a data that is a candidate for retraining, this model summarizes the changes as a small update to the base model (B) and is sent to refresh the core model via encrypted communication (C). This ensures that no user data, whether private or not, leaves the device in plain text, and that no individual updates are stored in the cloud. (see Figure 11).

Federated learning aims to address growing privacy concerns and enable the adoption of crowd-sourcing techniques (the act of collecting services, ideas or content through the contributions of a large group of people) for data collection. But using federated learning, the sensitive information can be left on the mobile device and doesn't need sharing sensitive information, improving in such a way users' privacy [49].

Federated learning enables smarter models, with lower latency and lower power consumption which helps to take care of device resources while ensuring privacy. This approach has another immediate benefit, that in addition to providing an update to the shared model, the enhanced model on the phone can also be used immediately, driving personalized experiences based on how a user uses the phone [50].

There are three types of Federated Learning [51]:

- **Vertical federated learning**: It applies to situations where data sets share the same sample space but have a different feature space.
- **Horizontal federated learning**: It is proposed for scenarios where the participating customer datasets share the same feature space but have different samples. That is, data containing the same features for each individual.
- **Hybrid federated learning**: It is applied when data sets from different customers not only have different sample spaces, but also different feature spaces.

2.5. Android

Mobile devices have become a great necessity for people in work and personal environments. The Android operating system has become the most widely used worldwide and millions of available applications are available. Android has more than 2,500 million active devices. From 5G phones to tablets [52]. Google revealed that it has 2.5 billion active Android devices in 2019, making it the largest mobile operating system by number of users. On the other hand, Apple has 1.4 billion users across all products, including macOS and iOS devices.

In 2009 and 2020. Android (72.95%) and iOS (26.27%) stand out for their enhanced capabilities and popularity among users. Although there are other smartphone platforms available, the combined market share of Google's Android and Apple's iOS will reach 99% by 2020 [53].

Android has the following features [54]:

- Open profitable platform. It is a free development platform based on Linux and open source.

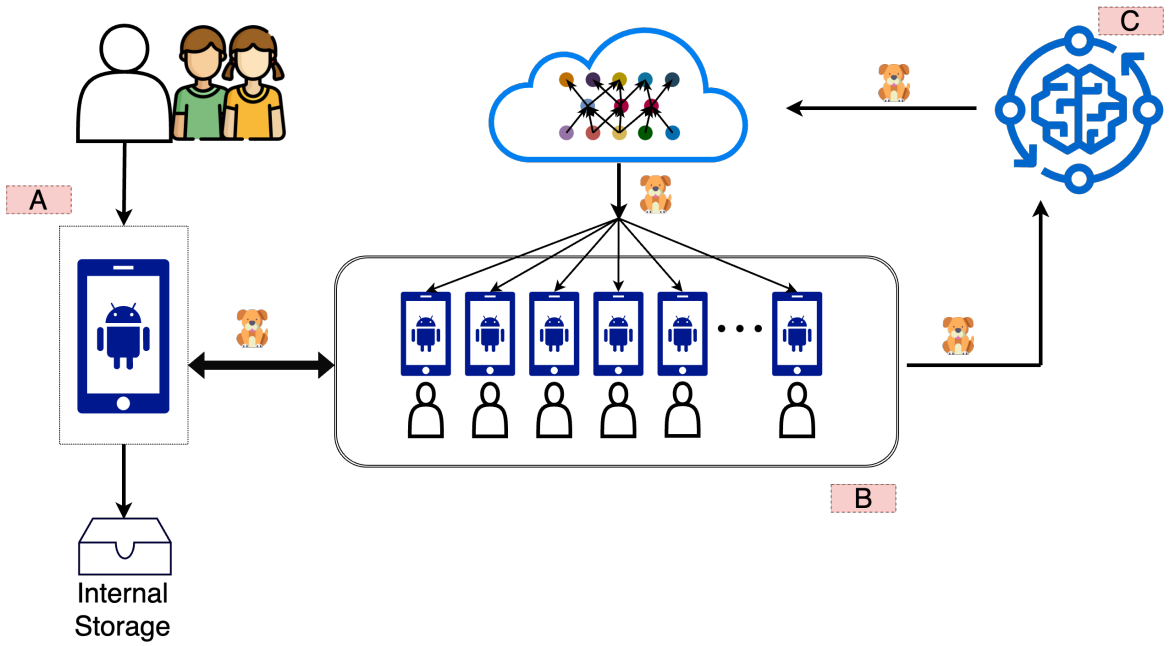


Figure 11: Functioning of Federated Learning.

- Adaptable to any type of hardware, as it can be used in different devices such as watches, glasses, TV, home appliances, among others.
- Assured portability, it helps the applications to be executed in any type of CPU because the final applications are developed in java.
- Internet-inspired component-based architecture, allowing the same application to run on a watch or a TV.
- Highly configurable and allows you to fully control your privacy settings. Each application has a set of permissions that limit the range of action, allowing the user to grant or withdraw permissions.

Android is a Linux-based mobile operating system with different layers, [53][55], as shown in Figure 12 :

- **kernel**: It supports and manages core system services like process, memory, security, network, etc.
- **Hardware abstraction layer (HAL)**: It provides standard interfaces that expose the hardware capabilities of the device. The HAL consists of several library modules and each of these implements an interface for a specific type of hardware component. It acts as an interface to communicate the Android application/framework with hardware-specific device drivers, such as camera, Bluetooth, etc. HAL is hardware specific and the implementation varies from vendor to vendor.
- **Android runtime**: For devices running Android 5.0 (API level 21) or later, each app runs its own processes with its own instances of the Android Runtime (ART). The ART is written to run multiple virtual machines on low-memory devices executing DEX files, a bytecode format designed especially for Android and optimized to occupy minimal memory space.

  ART is introduced as a new runtime environment in newer Android versions (version 5.0 onwards). During app installation, it uses ahead-of-time (AOT) and just-in-time (JIT) compilation, which compiles the Dalvik bytecode into native binaries (ELF format). This optimizes garbage collection and power assumption and achieves high runtime performance.
- **Native Libraries**: Core system services and different components of Android like ART and HAL are built from the native libraries, which are written in C/C++. There are different libraries, which provide support in building user interface application framework, drawing graphics and accessing database. Many core Android system components and services, such as ART and HAL, are based on native code that requires native libraries written in C and C++.

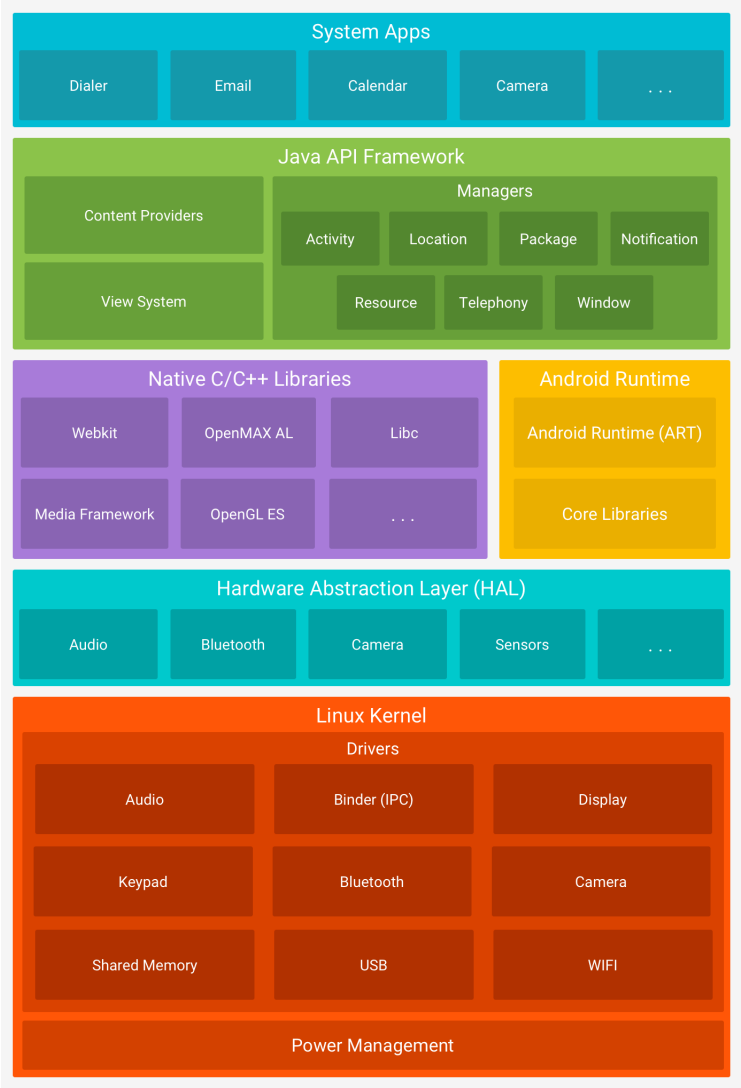


Figure 12: Android architecture.

- **Application framework**: Android SDK provides tool and API libraries to develop applications on Android java. This framework is known as Android Application Framework. Important features are database for storing data, support for audio, video and image formats, debugging tools, etc.
- **Applications**: Apps are at the top layer of the Android stack. It consists of native and third-party apps, such as web browser, email, SMS messaging, etc., that are installed by the user. There are some exceptions, such as the System Settings app. System apps function as apps for users and provide key capabilities that developers can access from their own apps.

Android's architecture is designed to be modular and open, allowing developers to easily customize the platform to meet their needs. Android's flexibility contributes to its popularity and the variety of devices running this operating system.

The Linux kernel in Android protects users by restricting user access to system resources and preventing resource exhaustion.The iOS security model is more restrictive compared to Android. iOS is a closed system, where developers can develop their own applications but their source code is not published, as in the case of Android.

Earlier versions of Android provide full disk encryption (FDE). Recent versions of Android support hardware encryption, also known as trusted execution environment (TEE) and file-based encryption (FBE). In FBE, different files are encrypted with different keys so that they can be unlocked independently [53]. Google has implemented various security measures in Android, such as app scanning in the Play Store, regular security

updates and the Google Play Protect feature, which protects against malicious apps.

2.6. Comparison with similar proposals

Some applications that perform monitoring of a particular application for children's Internet browsing re parental control applications. Parental control apps are tools that allow parents to set controls over minors' Internet and mobile device usage. These apps can help prevent children from accessing inappropriate content online and limit the time they spend on electronic devices [56]. This includes from mobile devices, to consoles or even applications such as Netflix, YouTube or Amazon Prime Video.

Some of the features that parental control applications have include [57]:

- **Call blocking**: Prevent unknown numbers not stored on your mobile device from calling you.
- **Time management**: Blocking the cell phone screen at bedtime, during meals or school hours.
- **Activity log**: As a browsing history, these tools keep a record of the applications you use, websites you visit, etc.
- **Emergency button**: This is less common, but some parental control tools offer an emergency button for the child in case any problems occur.

The reasons for activating parental controls are to protect minors from inappropriate content on the Internet, to block certain websites or specific search categories, to limit the downloading of dangerous or unwanted files, to keep devices safe from viruses, for example.

Some of the best parental control apps available on the market include FamiGuard, Vodafone Secure Net Family, Eyezy, mSpy, Kids Place, Qustodio, Confidant, Norton Family, Kaspersky Safe Kids, and Bark. These applications allow parents to block applications, calls, web pages, and entire devices, as well as monitor the location and online activity of minors. It is important to note that these applications should be used properly and not as a method of spying [58], [59].

There are three types of controls in particular:

- Network level controls are set at the hub or router and apply to all devices connected to that hub or router (covering the entire home).
- Device level controls are configured on the device itself, such as a smartphone, and will be applied regardless of how and where the device is connected to the Internet.
- Application controls are set on the platform or application being used. Examples of this would be the settings applied to Google or YouTube.

2.6.1. Parental control applications

Google SafeSearch

Provides users with the ability to change browser settings to filter explicit content from search results. As an owner, you can help Google understand the nature of the website you are visiting and the content by following the steps outlined in this guide. In this way, it helps to apply SafeSearch filters on the website used. This is used to filter pages that contain images or videos that include nude breasts or genitalia. It is also designed to filter pages with links, pop-ups or advertisements that display or lead to explicit content, Figure 13.

Search results with explicit content include content such as: images of nudity, graphic sex acts or sexually explicit material, violent or gory content, photos of realistic sex toys, escort services or sex dating [60], [61].

SafeSearch settings can be changed depending on the administrator for example:

- If you manage your own Google account, you can manage your SafeSearch settings.

- If a guardian assists a minor in managing the Family Link app account, SafeSearch settings can be managed.
- If you are signed in to a Google Workspace for Education account and are under the age of 18, or are associated with a K-12 institution, the administrator can modify your SafeSearch settings.
- Administrators of a device or network can block SafeSearch under "Filter".

Figure 13: Aplication Google SafeSearch.

Family Link de Google

Google Family Link is a family parental controls service that allows parents to manage and monitor their children's devices. It enables parents to set restrictions on content, approve or disapprove apps, and manage screen time. The service requires Google accounts and is available in 38 countries, including the United States, Australia, and Japan. Family Link also provides features such as content restrictions, GPS locating, and "bed-time" phone restrictions. It allows parents to manage their child's Google Account settings, apps on supervised devices, and view and manage permissions for websites and apps. Family Link is designed to help parents understand how their children are using their devices and to make meaningful choices about their child's data and privacy. The service is available as an app and is compatible with Android and iOS devices. Overall, Google Family Link offers a range of tools to help parents set screen time limits, filter content, and better understand how their families spend time online [62], [63], see Figure14 .

Figure 14: Aplication Family Link de Google.

FamiGuard

FamiGuard is a parental control application that allows parents to set controls over children's Internet and mobile device usage. The application allows parents to restrict content, approve or disapprove applications, set time limits and more. It also allows parents to monitor their children's location and online activity. FamiGuard is one of the popular parental control applications available on the market [58].

The app is available on Google Play and can be installed on parents' and children's devices. Parents can follow the on-screen installation steps to complete the registration process and start monitoring children's devices from the FamiGuard dashboard.

It is important to keep in mind that monitoring of minors' devices should be used openly and honestly in partnership with minors, not as a stealth spying method, Figure 15.

mSpy

MSpy is a brand of mobile and computer parental control monitoring software for iOS, Android, Windows, and macOS. The app allows users to monitor and log activity on the client device. It was launched as a product for mobile monitoring in 2010 by a London-based tech company. The application initially allowed parents

Figure 15: Aplication FamiGuard.

to monitor smartphones and later expanded to include monitoring of computers running Windows and Mac. However, it's important to note that mSpy has faced criticism and controversy, including data breaches and concerns about its potential for misuse. The app has been noted for its inconspicuous operation, raising concerns about potential illegal use. Additionally, some of its features only work on devices that have been rooted or jailbroken, which can compromise the security of the device. While the app offers a range of monitoring features, its installation and setup can be complex, requiring technical expertise and potentially compromising the security of the monitored device. Therefore, it's essential for users to carefully consider the implications and potential risks before using mSpy or similar monitoring software, Figure 16, [64].

Figure 16: Aplication mSpy.

3. Description of the Tool

HEROES proposes an anti-grooming application (AGApp) to detect and block any grooming attempts at an early stage on mobile devices belonging to children or teenagers. The app will have the ability to analyse multimedia content and an alert will be sent to the guardian to analyse them and indicate what action to take.

3.0.1. Child's Application

The child application is based on IA the analysis of multimedia files for grooming detection. It will help to maintain the privacy of their confidential information and physical integrity. The application will be installed on the device of minors taking into account the age of each minor, to display a consent that must be approved by the minor to accept the use of the application on their device.

3.0.2. Parents' Application

The second application corresponds to the parent or guardian who will receive an alert from the child's application if an attempt to grooming is detected. The parent or guardian will have the ability to determine whether the alert is true or false and will be responsible for sending an alert for action.

4. Manuals

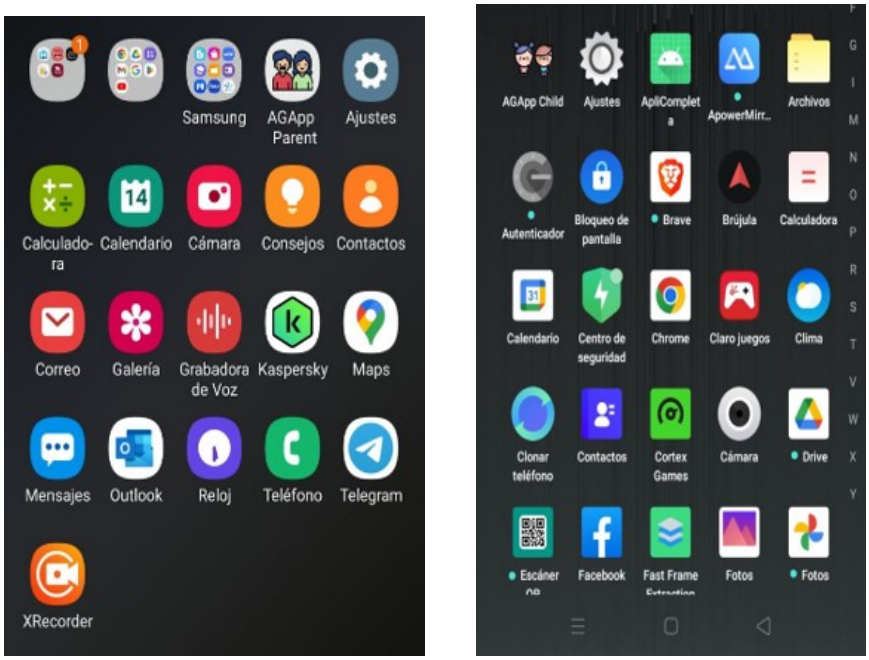
This section provides the installation and basic usage manual of the proposed applications for the Anti-Grooming tool. These manuals will serve as a resource for the correct utilisation of the Anti-Grooming tool to ensure its effectiveness in terms of early grooming attempts detection. The installation manual describes the step-by-step installation process of the tool, proposing a method for a seamless and error-free integration in the detection and processing of possible grooming messages. The user manual provides comprehensive guidance on how to use the tool effectively.

4.1. User Manual

The user manual provides a complete guide to effectively use the Anti-Grooming tool. This information will help to understand the data generated and the results of the tool.

The first step of the setup is to obtain the application by direct download of the APK. And it should be installed on the device of the parent and the child as shown in Figures 17(a) and 17(b).

For the applications to work correctly, the appropriate permissions for the correct functioning of the tool must be activated manually or when the application requests them.



(a) Installation of Parents app

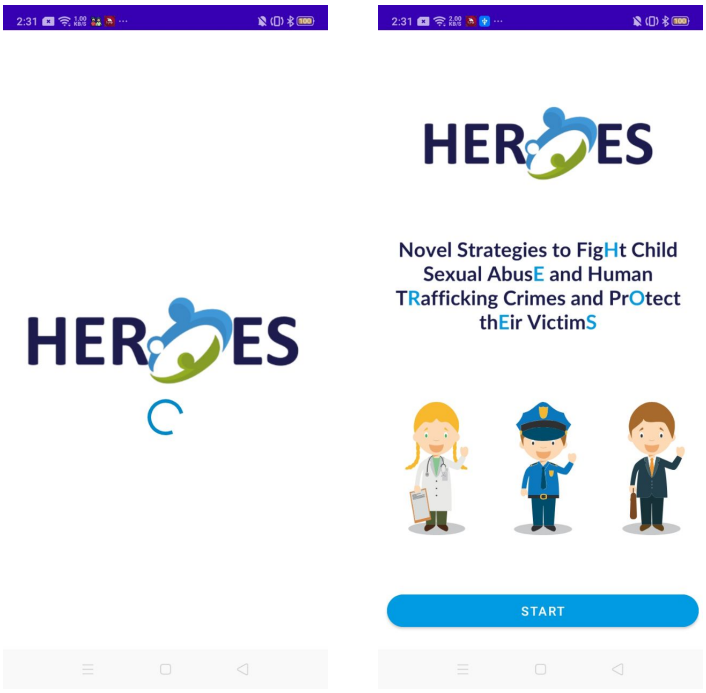
(b) Installation of Minor's app

Figure 17: Base Tool Applications

4.1.1. User Creation

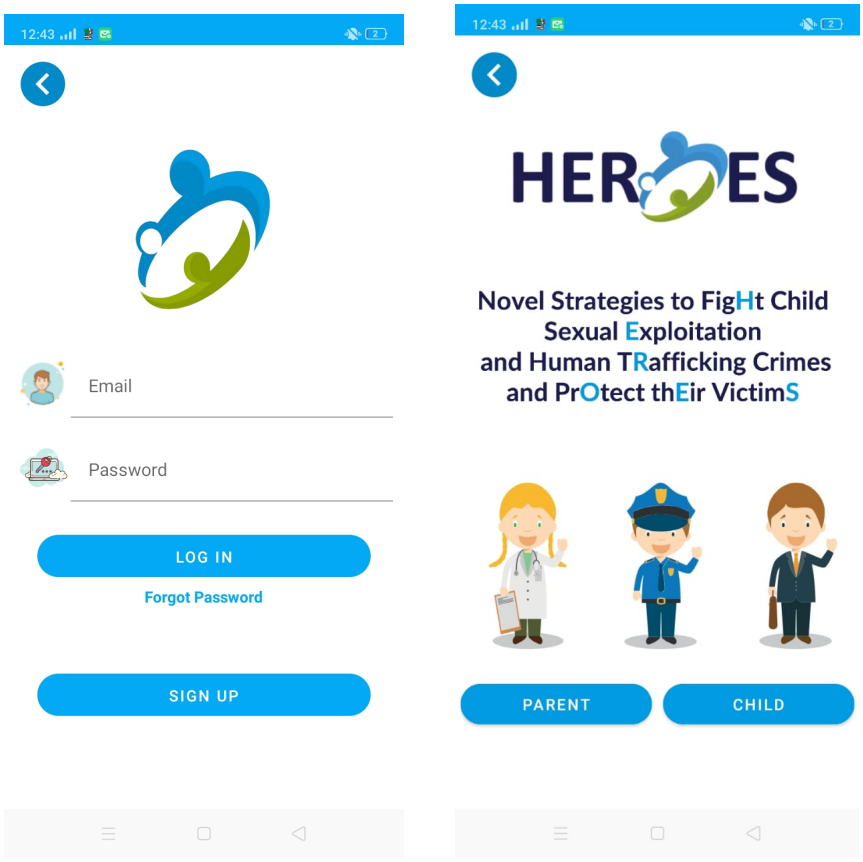
When the application is started for the first time, two welcome screens with the name of the HEROES project are presented (Figures 18(a) and 18(b)). While these screens are displayed, the base folders of the application are created.

When the button is pressed *"Start"*, the login screen appears, with the possibility to create new users by clicking on the button "*Sign Up*" (Figure 19(a)). For the registration of a new user, the type of user to be created will be requested (Figure 19(b)), depending on whether it is a child or a parent or guardian the creation options vary.



(a) Welcome Screen (b) Main Application Screen

Figure 18: Base Tool Applications



(a) User Login (b) User Type Selection

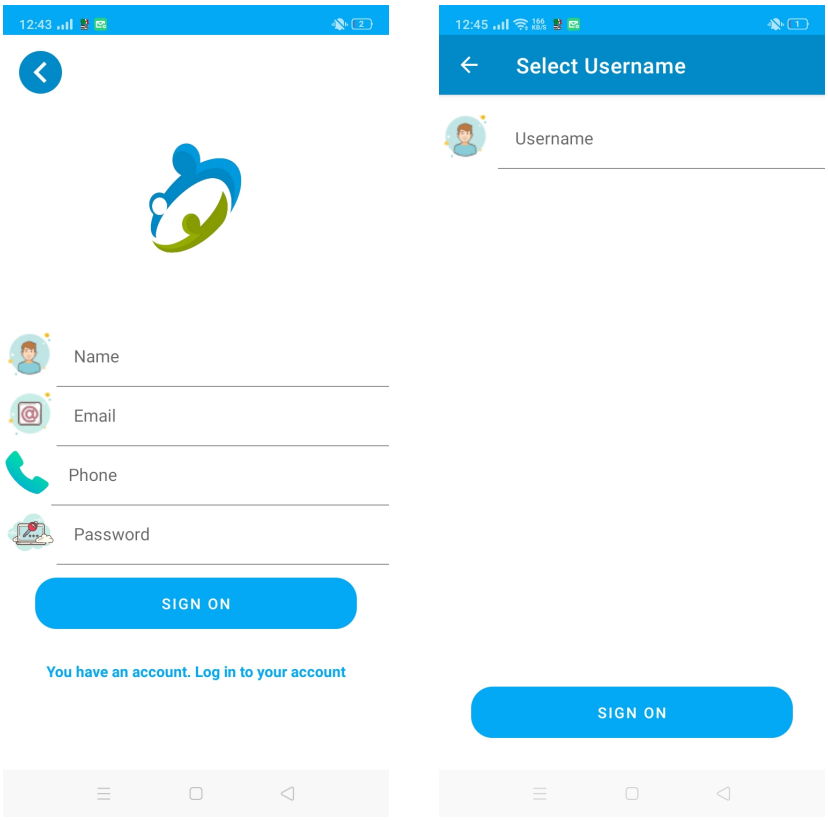
Figure 19: Base Tool Applications

At this point it is recommended that the parent's user is created first, since in a later screen, when the child's account is generated, the parent's email will be requested to associate the child and verify if it is a valid user in

order to validate that users are not created arbitrarily in the application.

Once the user type is selected (if it is the first time interacting with the application or the accounts will be created for the first time, it is recommended that the parent user are generated in first place), the user will be sent to the registration screen where basic data will be requested for the creation of the account and user login such as the *name*, *Email*, *Telephone* and a *password* that meets the minimum security requirements (at least one uppercase, one lowercase, one digit and one special character) (Figure 20(a)).

The user and password entered must be remembered as they will be used later. Once the base data has been entered, a username will be requested to identify the user (Figure 20(b)).



(a) User Creation (b) Username selection

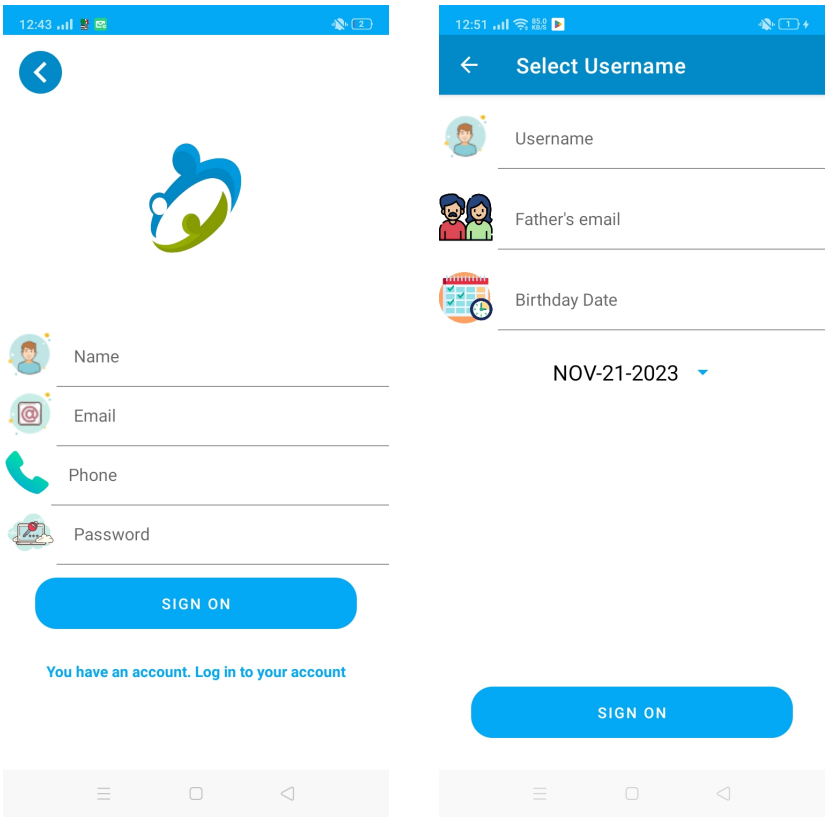
Figure 20: Parent or Guardian User Registration

Upon the creation of user of type "*Parent*", users of the type "*Child*" can be created. The same basic user data will be requested, *name*, *Email*, *Phone* y un *password* that meets the minimum security requirements (at least one uppercase, one lowercase, one digit and one special character). Then the process request a "*username*", the father's email address for information exchange and date of birth (Figure 21(b) and 21(a)), which will be used to determine whether consent from the minor is required for the application to run on his or her device.

As many child accounts can be created as necessary, however, it is recommended to create a single account for each device so that the application's functions are customised and alerts correspond to the correct device.

Furthermore, it will be possible to create more than one user of the type "*Parent*" and can be associated with a user "*Child*" previously associated with another user of type "*Parent*" This will allow another person to administer the same user who is in their care, however, it will be necessary to enter the email address of the "*Parent*" user who generated the child's account in order to link it.

Once the registration of the User of type *Child*is successful, a screen will be displayed indicating that you must log in to the minor's application to finish the process. You click on *Log Out* to log out and log in as a parent.



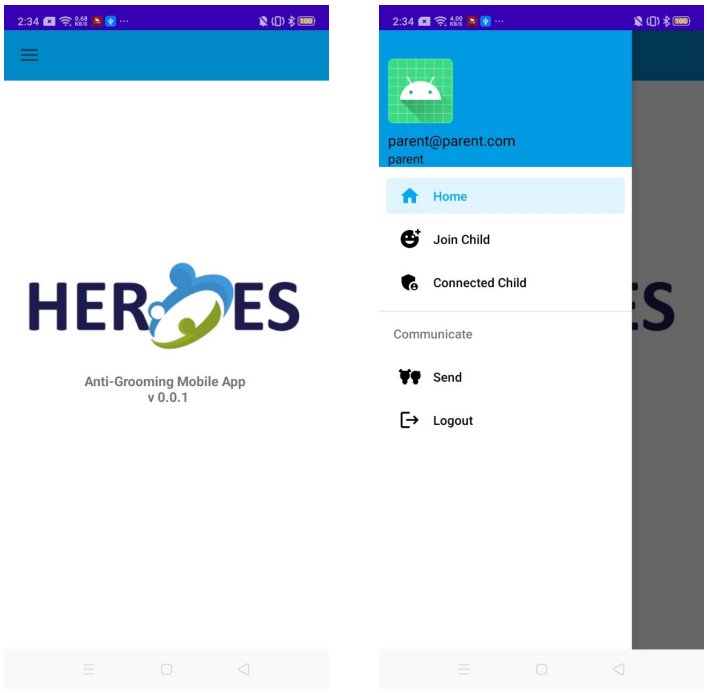
(a) Child User Creation (b) Selection of the Child's username

Figure 21: Minor User registration

4.1.2. User Login

In the Figure Login 19(a) the user's username and password of type *Parent* previously generated are are entered and the main screen of the user shown in Figure 22(a) will open. The basic user information will be displayed in the drop-down menu, Figure 22(b). In addition, the following buttons will be displayed for the user to interact with the application, which will be detailed in the following subsections:

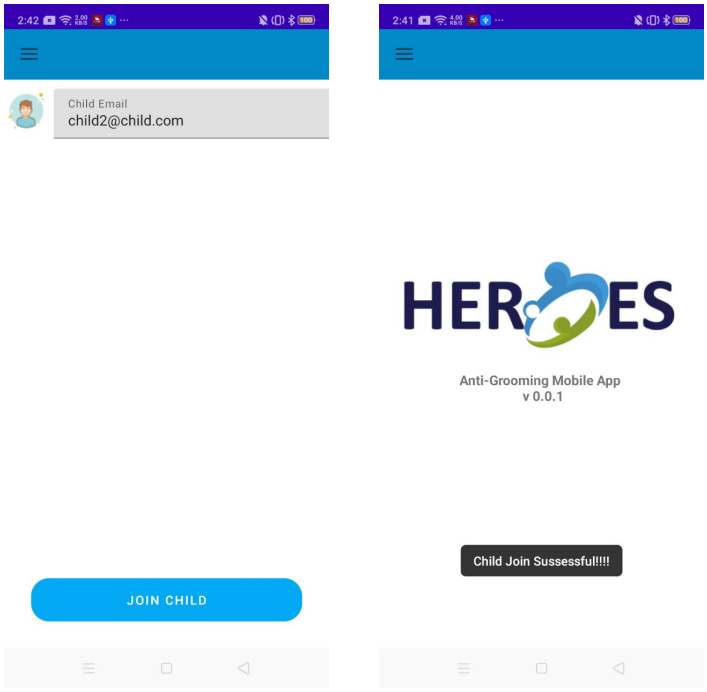
- **Home**: The main screen of the user session is displayed:
- **Join Child**: It will allow you to link accounts of the type *Child* to user.
- **Connected Child**: Allows you to interact with linked users:
- **Send**: Allows you to send a text message to the minor:
- **Logout**: Log out of the user.



(a) Main User Screen (b) Child username selection

Figure 22: Basic User Information

4.1.3. Linking and interaction with New Users



(a) User Linking (b) Successfully linked user

Figure 23: Linking Users

The button "*Join Child*" will allow linking a new user to the profile of the "*Parent*" using only the email of the account you want to link, Figure 23(a). If the user was able to join, it will display a legend indicating that the user joined successfully. (Figure 23(b)).

The application will allow you to link all the necessary users, however once joined, the application will need the

user who created the accounts to confirm or enter their email in order to validate that they are a valid user.

By clicking on the button "*Connected Child*" the users configured in the system are displayed (Figure 24).

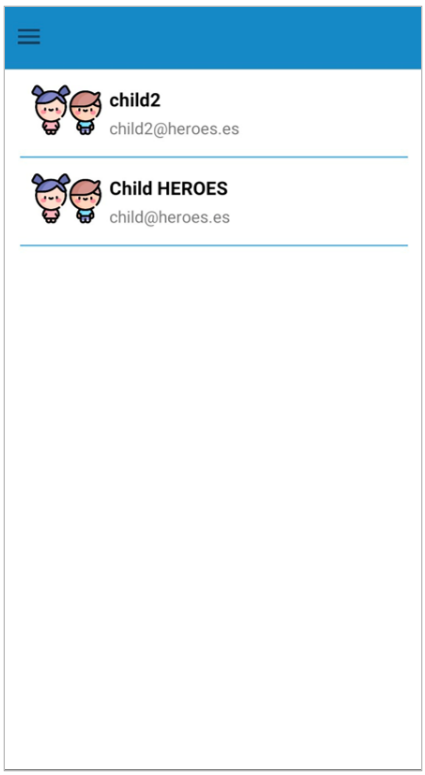
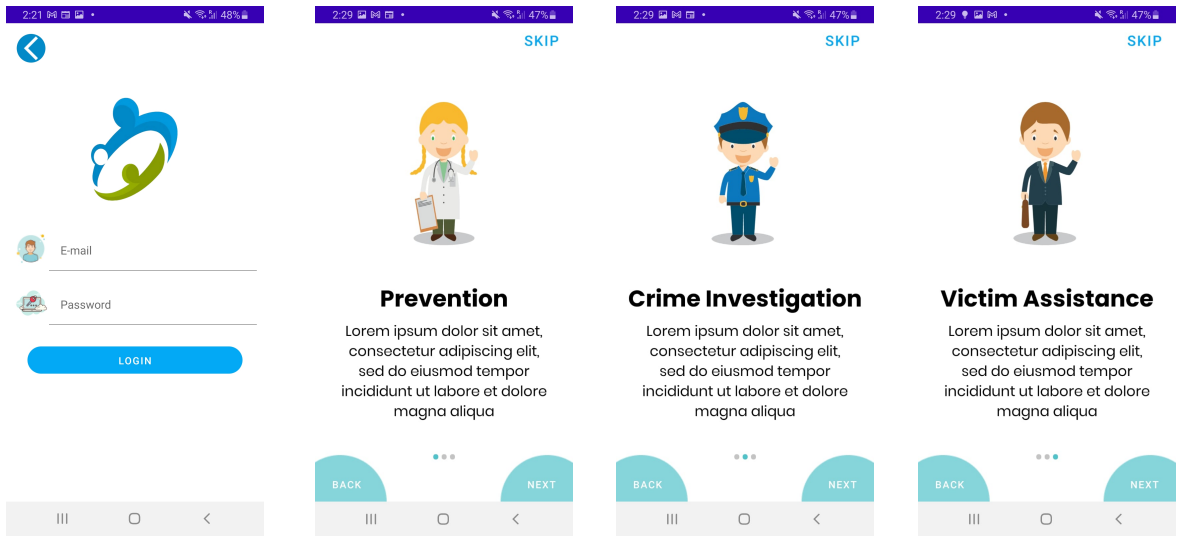


Figure 24: Users online

4.1.4. Child Application

Once the users have been generated correctly, they log in to the application on the minor's device and the services will automatically start and information regarding the protection of minors will be displayed to avoid falling into a case of grooming.



(a) Main Screen child Application

(b) Screen 1 child Application

(c) Screen 2 child Application

(d) Screen 3 child Application

Figure 25: Child Application Screens

5. Conclusions

The threat of grooming, a criminal act involving the manipulation and harassment of minors by adults for sexual purposes, has intensified in the digital age, exacerbated by the increased use of mobile devices. Although tools have been developed to control access and use of these devices by minors, the complexity of grooming has proven to be a challenge that goes beyond conventional solutions.

HEROES' proposal, in the form of the Anti-Grooming Tool (AGApp), represents an advanced and proactive approach to tackle this growing problem by enabling early detection and blocking of possible criminal attempts and also seeks to prevent situations of imminent danger.

The AGApp's ability to analyze images and videos directly on the child's device effectively solves the dilemma between the need to protect privacy and the urgency to detect potentially dangerous content. This ensures that the child's information does not leave the device, mitigating information security issues.

Direct communication with the guardian through alerts establishes an effective and rapid channel for responsible adults to take appropriate action. This approach not only allows for immediate intervention in critical cases, but also facilitates a deeper understanding of the situation, enabling tutors to address the issue in an informed and educational manner.

In short, the HEROES proposal highlights the need to address online grooming not only as a safety issue, but also as a social and educational issue. The AGApp represents a step forward towards protecting the integrity of minors in the digital environment, taking advantage of technology in an ethical and proactive way. However, it highlights the importance of effective implementation and ongoing adaptability to meet the constantly evolving challenges associated with grooming in the digital age.

As future work, it is planned to expand the functionalities of the anti-grooming tool with other technologies in order to protect more users and reach the largest number of target audiences.

References

[1] "Global threat assessment 2021 shows dramatic increase in online child sexual exploitation and abuse," https://www.end-violence.org/articles/global-threat-assessment-2021-shows-dramatic-increase-online-child-sexual-exploitation, accedido: 2023-09-20.

[2] L. E. Kaylor, G. M. Winters, and E. L. Jeglic, "Exploring sexual grooming in female perpetrated child sexual abuse," *Journal of child sexual abuse*, vol. 31, no. 5, pp. 503–521, 2022.

[3] M. P. Hernández, K. Schoeps, C. Maganto, and I. Montoya-Castilla, "The risk of sexual-erotic online behavior in adolescents–which personality factors predict sexting and grooming victimization?" *Computers in human behavior*, vol. 114, p. 106569, 2021.

[4] A. C. Wood and J. M. Wheatcroft, "Young adult perceptions of internet communications and the grooming concept," *Sage open*, vol. 10, no. 1, p. 2158244020914573, 2020.

[5] E. L. van Gijn-Grosvenor and M. E. Lamb, "Online groomer typology scheme," *Psychology, Crime & Law*, vol. 27, no. 10, pp. 973–987, 2021.

[6] Y. Y. Lim, S. Wahab, J. Kumar, F. Ibrahim, and M. R. Kamaluddin, "Typologies and psychological profiles of child sexual abusers: An extensive review," *Children*, vol. 8, no. 5, p. 333, 2021.

[7] M. Gámez-Guadix, P. De Santisteban, S. Wachs, and M. Wright, "Unraveling cyber sexual abuse of minors: Psychometrics properties of the multidimensional online grooming questionnaire and prevalence by sex and age," *Child Abuse & Neglect*, vol. 120, p. 105250, 2021.

[8] D. Canter and D. Youngs, "Sexual and violent offenders' victim role assignments: A general model of offending style," *Journal of Forensic Psychiatry & Psychology*, vol. 23, no. 3, pp. 297–326, 2012.

[9] "Grooming," https://www.incibe.es/menores/tematicas/grooming, accedido: 2023-09-20.

[10] "Grooming, la pandemia cibernética que pone en peligro a la infancia," https://www.eleconomista.com.mx/arteseideas/Grooming-la-pandemia-cibernetica-que-pone-en-peligro-a-la-infancia-20220428-0121.html, accedido: 2023-09-20.

[11] "Grooming," chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.eset-la.com/microsites/proteccion-infantil/descargar/grooming_chicos_eset.pdf, accedido: 2023-09-20.

[12] "Child sexual abuse material: Model legislation and global review, 10th edition, 2023," https://www.icmec.org/child-pornography-model-legislation-report/, accedido: 2023-09-20.

[13] "Grooming qué es, cómo detectarlo y prevenirlo," https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo, accedido: 2023-09-20.

[14] S. Candra, F. Gunawan, L. Ashianti, and B. Soewito, "Detecting online child grooming conversation," in *Conference: 2016 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS). https://www. researchgate. net/publication/317692642_Detecting_online_child_grooming_conversation*, 2016.

[15] "Guía s.o.s. contra el grooming," chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf, accedido: 2023-09-20.

[16] S. Pérez Arteaga, A. L. Sandoval Orozco, and L. J. García Villalba, "Analysis of machine learning techniques for information classification in mobile applications," *Applied Sciences*, vol. 13, no. 9, p. 5438, 2023.

[17] S. S. Chaturvedi, K. Gupta, and P. S. Prasad, "Skin lesion analyser: an efficient seven-way multi-class skin cancer classification using mobilenet," in *Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2020*. Springer, 2021, pp. 165–176.

[18] J. Velasco, C. Pascion, J. W. Alberio, J. Apuang, J. S. Cruz, M. A. Gomez, B. Molina Jr, L. Tuala, A. Thio-ac, and R. Jorda Jr, "A smartphone-based skin disease classification using mobilenet cnn," *arXiv preprint arXiv:1911.07929*, 2019.

[19] A. Wibowo, C. A. Hartanto, and P. W. Wirawan, "Android skin cancer detection and classification based on mobilenet v2 model," *International Journal of Advances in Intelligent Informatics*, vol. 6, no. 2, pp. 135–148, 2020.

[20] P. Sreelakshmi and M. Sumithra, "Facial expression recognition robust to partial occlusion using mobilenet," *International Journal of Engineering Research & Technology (IJERT)*, vol. 8, no. 6, pp. 1387–1391, 2019.

[21] J. Huang, L. Mei, M. Long, Y. Liu, W. Sun, X. Li, H. Shen, F. Zhou, X. Ruan, D. Wang *et al.*, "Bm-net: Cnn-based mobilenet-v3 and bilinear structure for breast cancer detection in whole slide images," *Bioengineering*, vol. 9, no. 6, p. 261, 2022.

[22] GitHub, "Mobilenet," https://github.com/tensorflow/tfjs-models/tree/master/mobilenet, accessed: 2023-01-08.

[23] s. Ozturk, U. Ozkaya, B. Akdemir, and L. Seyfi, "Convolution kernel size effect on convolutional neural network in histopathological image processing applications," in *2018 International Symposium on Fundamentals of Electrical Engineering (ISFEE)*. IEEE, 2018, pp. 1–5.

[24] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "Mobilenetv2: Inverted residuals and linear bottlenecks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 4510–4520.

[25] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," *ArXiv*, vol. abs/1704.04861, 2017.

[26] B. Koonce, *MobileNetV3*. Berkeley, CA: Apress, 2021, pp. 125–144. [Online]. Available: https://doi.org/10.1007/978-1-4842-6168-2_11

[27] E. Díaz-Gaxiola, Z. E. Morales-Casas, O. Castro-López, G. Beltrán-Gutiérrez, I. F. V. López, and A. Y. Rendón, "Estudio comparativo de arquitecturas de cnns en hojas de pimiento morrón infectadas con virus phyvv o pepgmv." *Res. Comput. Sci.*, vol. 148, no. 7, pp. 289–303, 2019.

[28] J. Liao, L. Cai, Y. Xu, and M. He, "Design of accelerator for mobilenet convolutional neural network based on fpga," in *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, vol. 1. IEEE, 2019, pp. 1392–1396.

[29] D. Sinha and M. El-Sharkawy, "Thin mobilenet: An enhanced mobilenet architecture," in *2019 IEEE 10th annual ubiquitous computing, electronics & mobile communication conference (UEMCON)*. IEEE, 2019, pp. 0280–0285.

[30] D. Categorization and B. Koonce, "Convolutional neural networks with swift for tensorflow."

[31] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *International conference on machine learning*. PMLR, 2019, pp. 6105–6114.

[32] S. S. Keh, "Semi-supervised noisy student pre-training on efficientnet architectures for plant pathology classification," *arXiv preprint arXiv:2012.00332*, 2020.

[33] "Introduction to efficientnet," https://www.scaler.com/topics/deep-learning/efficientNet/, accessed: 2023-01-10.

[34] "Efficientnet: Improving accuracy and efficiency through automl and model scaling," https://ai.googleblog.com/2019/05/efficientnet-improving-accuracy-and.html, accessed: 2023-01-10.

[35] "Efficientnet: Un enfoque revolucionario para el reconocimiento y análisis de imágenes," https://ts2.space/es/efficientnet-un-enfoque-revolucionario-para-el-reconocimiento-y-analisis-de-imagenes/, accessed: 2023-01-10.

[36] S.-L. Yi, X.-L. Yang, T.-W. Wang, F.-R. She, X. Xiong, and J.-F. He, "Diabetic retinopathy diagnosis based on ra-efficientnet," *Applied Sciences*, vol. 11, no. 22, p. 11035, 2021.

[37] "Efficientnet: Improving accuracy and efficiency through automl and model scaling," https://blog.research.google/2019/05/efficientnet-improving-accuracy-and.html, accessed: 2023-01-10.

[38] D. H. Fudholi, S. Rani, D. M. Arifin, and M. R. Satyatama, "Deep learning-based mobile tourism recommender system." *Scientific Journal of Informatics*, vol. 8, no. 1, pp. 111–118, 2021.

[39] M. N. Ab Wahab, A. Nazir, A. T. Z. Ren, M. H. M. Noor, M. F. Akbar, and A. S. A. Mohamed, "Efficientnet-lite and hybrid cnn-knn implementation for facial expression recognition on raspberry pi," *IEEE Access*, vol. 9, pp. 134 065–134 080, 2021.

[40] "Higher accuracy on vision models with EfficientNet-Lite, howpublished = https://blog.tensorflow.org/2020/03/higher-accuracy-on-vision-models-with-efficientnet-lite.html, note = Accessed: 2023-04-10."

[41] T. Blog, "Higher accuracy on vision models with efficientnet-lite," https://blog.tensorflow.org/2020/03/higher-accuracy-on-vision-models-with-efficientnet-lite.html, accedido: 2023-01-15.

[42] G. Cloud, "¿qué es el procesamiento del lenguaje natural?" https://cloud.google.com/learn/what-is-natural-language-processing?hl=es, accedido: 2023-04-18.

[43] IBM, "What is natural language processing (nlp)?" https://www.ibm.com/topics/natural-language-processing, accedido: 2023-04-18.

[44] L. A. Martínez Hernández, A. L. Sandoval Orozco, and L. J. García Villalba, "Analysis of digital information in storage devices using supervised and unsupervised natural language processing techniques," *Future Internet*, vol. 15, no. 5, p. 155, 2023.

[45] J. Li, A. Sun, J. Han, and C. Li, "A survey on deep learning for named entity recognition," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, pp. 50–70, 1 2022.

[46] M. T. Review, "Aprendizaje federado: la nueva arma de ia para asegurar la privacidad," https://www.technologyreview.es//s/11017/aprendizaje-federado-la-nueva-arma-de-ia-para-asegurar-la-privacidad, accedido: 2023-04-18.

[47] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, and Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications," *Information Processing & Management*, vol. 59, no. 6, p. 103061, 2022.

[48] altexsoft, "Federated learning: The shift from centralized to distributed on-device model training," https://www.altexsoft.com/blog/federated-learning/, accedido: 2023-04-18.

[49] Visionair, "Implementing federated learning in android," https://vision-air.github.io/federated.html, accedido: 2023-04-18.

[50] G. Research, "Federated learning: Collaborative machine learning without centralized training data," https://blog.research.google/2017/04/federated-learning-collaborative.html, accedido: 2023-04-18.

[51] H. Zhu, H. Zhang, and Y. Jin, "From federated learning to federated neural architecture search: a survey," *Complex & Intelligent Systems*, vol. 7, no. 2, pp. 639–657, 2021.

[52] Android, "Qué es android," https://www.android.com/intl/es-419$_m$x/$what - is - android/, accedido : 2023 - 04 - 18.

[53] S. Garg and N. Baliyan, "Comparative analysis of android and ios from security viewpoint," *Computer Science Review*, vol. 40, p. 100372, 2021.

[54] J. T. Gironés, *El gran libro de Android*. Alpha Editorial, 2019.

[55] A. Developers, "Arquitectura de la plataforma," https://developer.android.com/guide/platform?hl=es-419, accedido: 2023-04-18.

[56] Ayudaley, "Las mejores apps de control parental para android e iphone," https://ayudaleyprotecciondatos.es/2021/06/23/control-parental/, accedido: 2023-04-18.

[57] C. Claro, "Herramientas de control parental: qué son y sus características," https://www.eldiario.es/consumoclaro/herramientas-control-parental-son-caracteristicas$_{18}$201814.*html*, *accedido* : 2023 − 04 − 18.

[58] E. Mundo, "Las apps y herramientas de control parental que protegerán a tus hijos en la red," https://saposyprincesas.elmundo.es/ocio-en-casa/apps-videojuegos/mejores-apps-gratuitas-control-parental/, accedido: 2023-04-18.

[59] E. P. de España, "Las 10 mejores apps de control parental ¡y gratis!" https://www.epe.es/es/sociedad/20220919/10-mejores-apps-control-parental-75637206, accedido: 2023-04-18.

[60] S. google, "Cómo filtrar o desenfocar resultados con contenido explícito con safesearch," https://support.google.com/websearch/answer/510?co=GENIE.Platformaccedido: 2023-04-18.

[61] G. S. Central, "Safesearch y tu sitio web," https://developers.google.com/search/docs/crawling-indexing/safesearch?hl=es-419, accedido: 2023-04-18.

[62] G. F. Link, "Help keep your family safer online," https://families.google/familylink/, accedido: 2023-04-18.

[63] G. F. F. Help, "Get started with family link," accedido: 2023-04-18. [Online]. Available: https://support.google.com/families/answer/7101025?hl=en&sjid=6792812314255583162-NC

[64] S. Detectives, "mspy review 2023: Is this parental control app any good?" https://www.safetydetectives.com/best-parental-control/mspy/, accedido: 2023-04-18.

