IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 21, 2021, accepted August 2, 2021, date of publication August 9, 2021, date of current version August 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3103459

A Systematic Review of Computer Science Solutions for Addressing Violence Against Women and Children

DALIA ANDREA RODRÍGUEZ[1], ARNOLDO DÍAZ-RAMÍREZ[1], (Member, IEEE), JESÚS ELÍAS MIRANDA-VEGA[1], LEONARDO TRUJILLO[2], AND PEDRO MEJÍA-ALVAREZ[3]

[1]Department of Computer Systems, Tecnológico Nacional de México/IT Mexicali, Mexicali, Baja California 21376, Mexico
[2]Department of Electrics and Electronics, Tecnológico Nacional de México/IT Tijuana, Tijuana, Baja California 22430, Mexico
[3]Cinvestav Guadalajara, Zapopan, Jalisco 45017, Mexico

Corresponding author: Arnoldo Díaz-Ramírez (adiaz@itmexicali.edu.mx)

This work was supported in part by the Tecnológico Nacional de México and in part by the National Council of Science and Technology (CONACyT).

ABSTRACT Violence against women and children is a public health issue of pandemic proportions. It is estimated that one in every three women worldwide has experienced physical, emotional, or sexual violence. Similarly, each year one out of two children are victims of some form of violence including domestic aggression and bullying. Due to the widespread use of the Internet and social media, women and children are now vulnerable to other types of violence such as cyber-bullying and online sexual or emotional harassment. To help alleviate this social problem, the use of computer science and related technologies has been leveraged in recent years. The Internet of Things, artificial intelligence, ubiquitous and mobile computing, pattern recognition, cloud computing and similar technologies, have been used to formulate solutions to detect and prevent violent acts against women and children. In this paper, a systematic review of some of the efforts that can help address the problem of violence against women and children is presented. This paper describes the current state-of-the-art of these contributions and identifies trends, architectures, technologies, and current open challenges. The survey was developed using a literature review of academic documents published from 2010 to 2020. The contributions were categorized into four application domains: online detection, offline detection, safety, and education. These contributions were further categorized based on the computer science approaches and technologies used: artificial intelligence, Internet of Things, and digital serious games.

INDEX TERMS Artificial intelligence, Internet of Things, machine learning, ubiquitous computing.

I. INTRODUCTION

Violence is defined by the Violence Prevention Alliance (VPA), a network of the World Health Organization (WHO), as ''the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation.'' Violence can be inflicted upon anyone, but women and children are at particular risk of becoming victims. About one in every three women worldwide have experienced physical or sexual intimate partner violence (IPV) or non-partner sexual violence during their lifetime [1]. Similarly, estimates indicate that one out of two children worldwide suffer from some form of violence each year [2]. Violence against women (VAW) and violence against children (VAC) are major public health concerns in need of any form of intervention.

IPV is one of the most common forms of VAW [3]. 30% of women who have been in a relationship report that they have experienced physical or IPV during their lifetime; 38% of femicides happen at the hands of an intimate partner or ex-partner [1]. Men are the most common perpetrators of IPV; some factors that lead to IPV against women include social norms such as male dominance and the belief that men have a right to beat their female partner [3]. Therefore, gender inequality and discrimination foster VAW. It is necessary to address these issues to prevent VAW.

Violence experienced by women often goes unreported. Less than 40% of women seek help of any sort or report the crime to the authorities [4]. In Mexico, the percentage of women who do not report violent acts is 88% [5].

The associate editor coordinating the review of this manuscript and approving it for publication was Feng Lin.

Also, 49.3% do not report because they think that the violence that they suffered was not significant [5], highlighting that women believe that it is acceptable to commit violence against them. Lawmakers appear to support this belief, given that one in four countries have no laws protecting women from domestic violence (DV) [4]. However, VAW may lead to injuries, unintended pregnancies, sexually transmitted diseases, and death. Victims experience anxiety and eating disorders, sleep difficulties, and suicidal behavior [1]. In particular, women who have suffered IPV are almost twice as likely to suffer from depression and drinking problems [1]. The consequences of VAW are indeed significant. Therefore, it is necessary to teach women and society that all forms of violence are unacceptable. Furthermore, it is vital to provide women with appropriate protection and methods to seek help.

Adult women are not the only victims of VAW. About 120 million girls and young women under the age of twenty have suffered some form of forced sexual contact, and underage girls are more likely to suffer from sexual abuse than underage boys [2]. IPV and child maltreatment can co-occur within the same household [6]. In particular, 300 million children between the ages of two and four regularly suffer physical or emotional violence at the hands of parents or caregivers, and one in four children aged under five live with a mother who is a victim of IPV [2]. As a result, children who experience maltreatment are at a higher risk of repeating the cycle of IPV as adults, with men as perpetrators and women as victims [2]. Other forms of VAC include bullying, which affects one in three students between the ages of eleven and fifteen each month, and at least 20% of adolescents aged between thirteen and eighteen experience dating violence [3]. Given the correlations between VAW and VAC, it is necessary to address VAW and VAC simultaneously.

The prevalence of VAW and VAC has led to a growing interest in addressing these issues from a computer science (CS) and engineering perspective. Technological contributions using CS and related techniques assist in the detection of potential cases of VAW and VAC, such as peer violence, IPV, and child sexual abuse (CSA). Given that the majority of cases of VAW are not reported, and 60% of cases of sexual VAC has a five-year delay in disclosure [7], technological solutions may be a valuable tool to assist practitioners in identifying victims of abuse. CS can be used to detect and prevent pedophilia by monitoring the influx of media files depicting CSA [8]. CS can also aid in the detection of social media posts that are discriminatory or hateful towards women and girls [9], a task that may be time-consuming or emotionally taxing for those in charge of removing said content.

CS is also being used to provide education on the subject of VAW and VAC. CS can provide tools to educate healthcare workers on how to improve the identification of victims of abuse [10]. Therefore, victims of abuse who are reluctant to speak up can get the help that they need. These educational tools can also help to educate children or adults on the topic of healthy friendships [11] and romantic relationships [12]. CS solutions to VAW and VAC may help foster a society where women and children can be heard and supported.

CS is also being incorporated into safety tools for women and children. These tools may detect when a woman or child is involved in a dangerous situation and, in response, provide help for victims in real-time [13]. These tools may help to stop violent situations from further escalating.

As seen in previous paragraphs, CS and related technologies have the potential to address VAW and VAC. This paper aims to describe the current state-of-the-art contributions to stopping VAW and VAC within these fields; it also seeks to identify trends, architectures, technologies, and open challenges. To the best of our knowledge, there is no other paper that offers a systematic review on contributions concerning VAW and VAC from the perspective of CS and engineering. This paper aims to fill in this gap in the literature and guide researchers interested in addressing VAW and VAC from a CS and engineering point of view. A systematic literature review protocol was pre-defined using [14] as a guideline to provide a thorough and unbiased review.

The paper is structured as follows. Section 2 discusses the planning of this review. In Section 3, introduces the methodology for data extraction. Section 4 describes and categorizes the most important proposals found in the literature. Section 5 presents a discussion of the analysis of the review. Finally, Section 6 is for conclusions.

II. PLANNING

This section introduces the protocol for conducting this systematic literature review. The stages included are: specifying the research questions, primary study search, study selection criteria, study quality assessment procedures, and data extraction strategy. The two research questions that motivated this study were:

1) What are the main application domains related to VAW and VAC that are addressed using CS and engineering technologies?
2) What specific CS and related approaches and technologies do researchers implement to address the problems of VAW and VAC?

A systematic Internet search using search engines and academic digital libraries was performed between September to December 2020, to collect studies for this paper. The search engines and digital libraries described in Table 1 were chosen for study extraction due to their impact in covering a variety

TABLE 1. Information sources used to find studies.

Source	Type	URL
ACM	Digital library	https://dl.acm.org/
AAAI Press	Digital library	https://aaai.org/
IEEE	Digital library	https://ieeexplore.ieee.org/
IOS Press	Digital library	https://iospress.nl
ScienceDirect	Digital library	https://www.sciencedirect.com/
Springer	Digital library	https://link.springer.com/
dblp	Digital library	https://dblp.org/
PubMed	Search engine	https://pubmed.gov

of scientific and technological topics, including those closely related to the objective of this paper.

The next step in the search strategy was to obtain potentially relevant primary studies from each of the information sources in Table 1. Two groups of keywords, as defined in Table 2, were created using the research questions as guidelines. Group 1 includes words associated with CS and related technologies, while Group 2 contains terms related to VAW and VAC. At least one term from Group 1 and at least one term from Group 2 was combined into search strings using Boolean ANDs and ORs.

TABLE 2. Search terms.

Group 1	Group 2
Engineering, Computer science, CS, Internet of things, IoT, Artificial intelligence, AI, Machine learning, ML, Deep learning, DL, Serious game, SG	Women violence, violence against women, women abuse, VAW, woman violence, abuse against women, misogyny, misogynous, misogynist, sexism, sexist, gender-based violence, women hatred, women hate speech, child abuse, child sexual abuse, CSA, child physical abuse, IPV, intimate partner violence, child pornography, adolescent violence, dating violence, peer violence, school bullying, bullying children, children abuse, abuse of children, abuse of women, child maltreatment, domestic violence, abuse of children

Only the studies that met the following criteria were considered as potentially relevant:

- Papers published in peer-reviewed journals, peer-reviewed conference or workshop proceedings, or book chapters.
- Papers published in English.
- Papers with a date of publication between and including the years 2010 and 2020.

Potentially relevant studies were assessed for actual relevance using the following inclusion criteria:

- The title and abstract of the paper were read. If the abstract failed to mention either VAW or VAC or similar concepts, as well as the use of CS or related technologies, it was discarded.

The paper was read in its entirety and selected for inclusion if it met the following quality assessment:

- The paper addresses the issues of VAW or VAC from a CS or engineering perspective.
- The paper provides details of the design or architecture used to implement the proposed model.
- The paper describes related works that inspired the proposed model.

III. GUIDELINES FOR GRAPHICS PREPARATION AND SUBMISSION

A. DATA EXTRACTION

The objective of this stage is to extract studies for our paper using the protocol defined in the previous section. Queries made up of words or phrases from Table 2 were passed onto the information sources in Table 1 using a search format as described previously. The initial search was limited to reading the title and abstract of the studies that were recovered.

TABLE 3. Form used to extract data for each study.

Data retrieved	Description
Title	Title of the study
Year	Year of publication
Authors	Names of the people who contributed to writing the study
Countries	Countries that authors came from
Source	Digital library or search engine where study was found
Contribution	Solution to the problem the authors are addressing in their study
Approach	Specific technologies used to address the problem
Category	Online detection, offline detection, safety, or education
Type	Conference, journal, book chapter, etc.

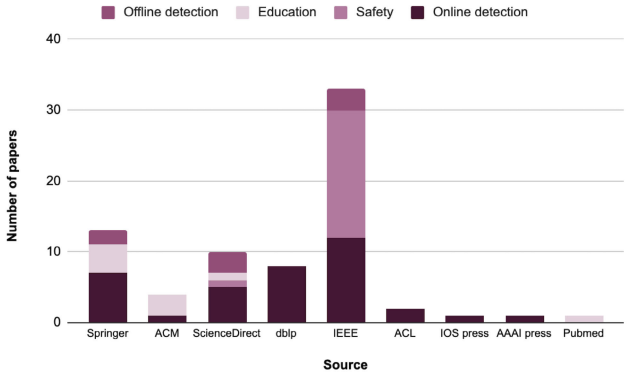

FIGURE 1. Distribution of papers selected by source.

If duplicate publications were found across platforms, only one was used. Afterward, the quality assessment from the previous section was used to evaluate the studies for quality. If discrepancies on eligibility persisted at this stage, authors resolved these by discussion, which occurred in only a few cases. Finally, 73 studies were selected to be in the study. The data from Table 3 was extracted from the papers that were selected for this study.

Fig. 1 shows that the majority of the selected studies came from IEEE (45.2%). This is followed by Springer (17.8%), ScienceDirect (13.7%), dblp (10.9%), ACM (5.5%), ACL (2.7%), and IOS press, AAAI press and PubMed with 1.4% each.

Fig. 2 displays the selected studies distributed by publication year. The majority of studies were published between 2018 and 2020, indicating a growing interest from the CS and engineering research community to tackle the problems of VAW and VAC in recent years.

Fig. 3 distributes the selected studies by the country of origin of the contributors. There is at least one study from each continent. This reflects that VAW and VAC are global crises. It is critical to take measures to stop VAW and VAC. The majority of the studies came from India, with 18 total contributions. Spain follows with 9 papers.

IV. DATA SYNTHESIS

The purpose of this phase is to answer the two research questions by using the information extracted from the selected studies.

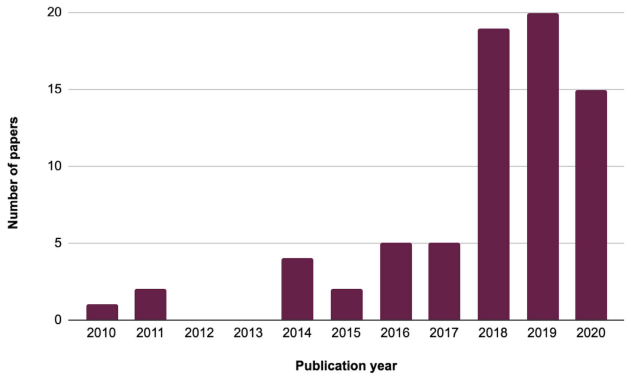

FIGURE 2. Distribution of selected studies by publication year.

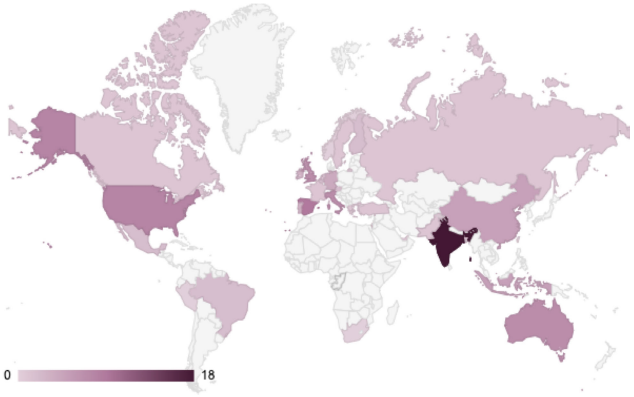

FIGURE 3. Distribution of selected papers by country.

TABLE 4. Summary of primary studies in their corresponding category.

Category	Studies
Online detection	[15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [9], [39], [40], [41], [42], [43], [8], [44], [45], [46], [47], [48], [49]
Offline detection	[50], [51], [52], [53], [54], [7], [55], [56]
Safety	[57], [13], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74]
Education	[75], [12], [11], [76], [77], [78], [79], [10], [80]

A. ANSWER TO THE FIRST RESEARCH QUESTION

In order to identify the main application domains related to VAW or VAC that are addressed using CS and engineering technologies, the primary studies were divided into four different categories depending on the purpose of their solution. This categorization is based on the current and future relevance of the application domain, and not on the number of related proposals. The categories are (I) online detection, (II) offline detection, (III) safety, and (IV) education. The selected studies can be observed within their corresponding category in Table 4. The distribution of the main studies can be visualized in Fig. 4. It can be observed that the majority of the studies focused on online detection (50.7%), followed by safety (26.0%), education (12.3%), and offline detection (11.0%).

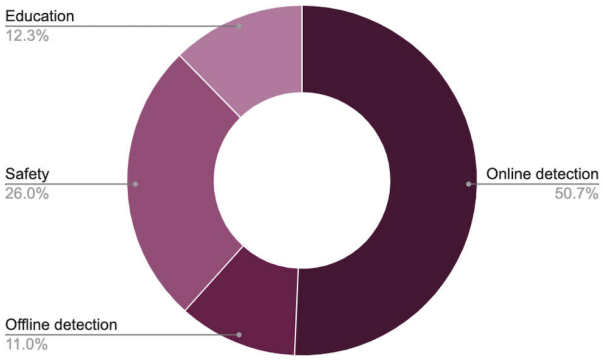

FIGURE 4. Distribution of selected studies by category.

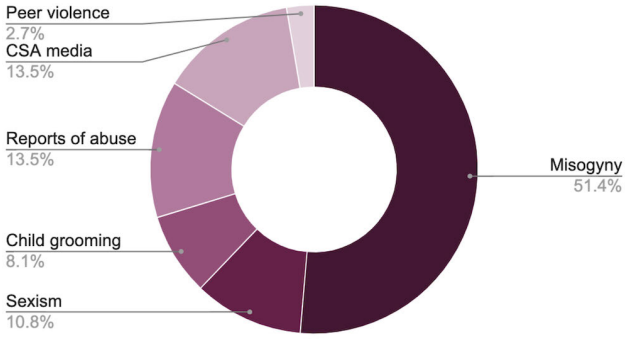

FIGURE 5. Online detection studies split into subcategories.

1) ONLINE DETECTION

Selected papers grouped in this category used artificial intelligence (AI), mainly machine learning (ML) algorithms, to identify Internet content that may be violent or offensive towards women or children. These studies built ML models that received images, videos [8], written text [9], or a combination of them [28] as input, to automatically classify them as abusive or not abusive towards women or children. ML used in this context made it possible to quickly separate large amounts of abusive Internet content from its non-abusive counterpart, a task that can be time-consuming [42] or emotionally-taxing [46] when done manually.

To detect and eliminate VAW and VAC, it is necessary to address both explicit violence and the risk factors that lead to their occurrence. It is vital to address DV, physical or sexual abuse, and other forms of violence that affect women and girls [1], but also the intolerance, discrimination, and gender stereotypes that lead to it [81]. For children, it is necessary to address their presence in environments with inadequate protection, like the Internet, which makes children vulnerable to grooming, bullying, or other forms of abuse [2]. In this context, studies belonging to the online category address explicit forms of VAW and VAC on the Internet and their risk factors. Fig. 5 categorizes these forms of VAW and VAC as the following: misogyny (51.4%), sexism (10.8%), child grooming (8.1%), peer violence (2.7%), reports of abuse (13.5%),

and CSA media (13.5%). Some representative examples of the online detection category are summarized below.

a: MISOGYNY

These studies propose methods for the automatic detection of written Internet content that is misogynistic. Misogyny is hate speech that is targeted towards women [16]. The work in [9] addressed the VAW problem of misogyny on social media by building ML models that identified and classified misogynistic tweets in English, Spanish, and Italian. The authors experimented with a mixture of datasets, features, and classifiers to discriminate misogynistic tweets from non-misogynistic tweets, classify misogynistic content into five different misogynistic behaviors, and identify the target of the misogynistic tweets as either individual women or groups of women. The authors also conducted experiments regarding cross-lingual identification of misogyny and explored the relationship between misogyny and other forms of abuse by conducting a cross-domain classification experiment. For the task of identifying whether a tweet is misogynistic or not, their best performing English-language model in terms of accuracy was a support vector machine (SVM) classifier with a radial basis function (RBF) kernel, along with stylistic, lexical, and handcrafted features. The accuracy of this model was 91.32%. For their Spanish-language binary classification model, the best-performing model had an accuracy of 81.47%. The authors selected the same features as the English-language model but used an SVM classifier with a linear kernel. Lastly, for the binary classification model of misogyny detection in Italian, the best-performing model was a BERT-based algorithm that achieved an accuracy of 84.8%.

b: SEXISM

Studies within the sexism subcategory aim to automatically detect Internet content that is sexist towards women, where sexism refers to the idea that certain people are inferior due to their sex or gender [82]. In the proposal introduced in [28], ML models were built that automatically detect sexist jokes on the Internet. The authors created a dataset of Internet jokes that contained both images and text from social media websites and developed ML models to classify this content as sexist or not sexist, at a unimodal and bimodal level. For the task of identifying sexist images, the authors used handcrafted features and experimented with various classifiers, where SVM achieved the highest precision at 76.2%. For the identification of text-based sexist jokes, the authors achieved 75.2% precision using k-nearest neighbors (K-NN) with a bag of words (BoW). For the bimodal approach, the authors achieved 75.9% precision using an SVM classifier and a combination of visual and textual features.

c: REPORTS OF ABUSE

Primary studies that belong to this subcategory are concerned with the automatic detection of self-reports of VAW or VAC on social media. The work in [33] used deep learning (DL) to automatically identify Facebook posts of people who require immediate assistance due to DV. The authors extracted Facebook posts from DV Facebook pages, testing multiple DL classifiers and word embeddings to create a multi-class identification model that identifies people who require critical help due to DV incidents. The best-performing model was a gated recurrent unit (GRU) classifier with word embeddings, which obtained 91.78% accuracy. Another study that explores self-reported accounts of abuse on social media is introduced in [21]. The authors built a DL model to investigate sexual violence self-reports within the #MeToo hashtag on Twitter. The authors created a multi-class model to identify the perpetrators of sexual violence or the locations where sexual violence occurs. The best-performing model was a convolutional neural networks (CNN) model that obtained 83% accuracy.

d: CHILD GROOMING

Grooming is defined as the act of gradually establishing a relationship, trust, and an emotional connection with children or young people with the end goal of manipulating, exploiting, and abusing them [83]. In this context, selected studies within the subcategory used ML techniques to detect child grooming situations in online chat rooms. The proposal described in [43] detects online child sex offenders in chat logs by using an SVM classifier and experimenting with features that encapsulate the personality, emotions, and vocabulary of online sex offenders, as well as the phenomenon of their unwillingness to change the topic during a grooming conversation [84]. The authors achieved an accuracy of 97% on a dataset that contains both cybersex conversations between consenting adults and conversations between volunteers posing as children and online sex offenders. The study in [45] analyzed child grooming conversations to find the most common indicators of grooming, and used them as features to build a logistic regression (LR) model that automatically identifies cases of child grooming in online conversations, achieving an accuracy of 95%.

e: CSA MEDIA

Studies that fall within this subcategory use ML models to facilitate the detection of child pornography on the Internet. The study in [8] builds ML models that detect CSA media on peer-to-peer (P2P) networks. The authors implemented three models to detect CSA media from its filename, image content, or video content. To identify CSA filenames, the authors implemented a model that uses an SVM classifier with character n-grams and semantic features such as pedophile keywords and words referring to children or family, achieving an accuracy of 73.0% when tested on a corpus of CSA-filenames against CSA-related filenames. The image and video classification models also used SVM as their classifier, but the features for the image classification model were color-correlograms, skin-feature, and visual words and pyramids. The video features were the same as the image features but also included audio words. The latter models earned an average accuracy of 92% and 95%, respectively, when tested on a dataset that contains adult pornography and

numerical representations of real CSA media provided by European law enforcement. In [47], the authors propose a methodology for child pornography and child face detection that combines neural network architectures to determine if an image contains child pornography. Their best-performing model achieves an accuracy of 79.8% when tested on a CSA dataset created in collaboration with the Brazilian Federal Police.

f: PEER VIOLENCE

The studies in this category detect cases of peer violence between students in an online setting. The single paper within this subcategory [49] experimented with various ML models to detect bullying in Greek virtual learning communities of K-12 students. This study aims to facilitate the ability of teachers to intervene in online peer violence, given the difficulty of monitoring students in an online environment. The authors applied various pre-processing techniques to the text, used *n*-grams as features, and fed these features to multiple classifiers to detect aggressive behavior. Their best result in terms of recall was a DL classifier with 95.4%.

2) OFFLINE DETECTION

Studies that are part of the offline detection category use ML to detect potential victims of abuse or violence from data not collected from or not available on the Internet. This data can include medical records from public health institutions [50], self-figure drawings of clients provided by therapists [7], or child welfare records [51]. The purpose of these studies is to create assistive tools for teachers, social workers, healthcare workers, and other professionals that work directly with potential victims of abuse. Given the low reporting rate of victims [4], and the lack of training that healthcare professionals receive to detect and deal with cases of abuse [78], professionals may benefit from tools that can help them identify cases of abuse that otherwise go unreported. Therefore these tools may lead professionals to help more women and children access the support and services necessary to prevent further violence from occurring.

Fig. 6 classifies technological solutions that fall under this category can into the following offline detection subcategories: peer violence (50.0%), child abuse (37.5%), and IPV (12.5%). Below is a description of some representative examples of CS and engineering solutions that fall under online detection.

a: PEER VIOLENCE

Studies within this subcategory use ML to detect violence in schools. These studies are the initial stages of Internet of Things (IoT) school violence response systems. The purpose of these systems is to use ML techniques to detect violence and automatically contact school authorities for intervention. These studies only focus on the aspect of identifying violence by using ML. The study in [53] propose two models that identify physical and verbal bullying in schools. The authors recorded students acting out emotions that were

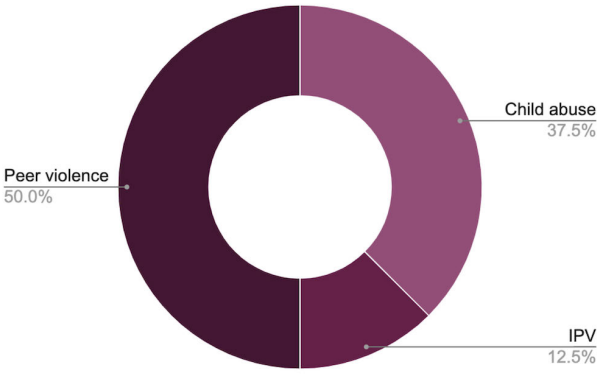

FIGURE 6. Offline detection studies split into subcategories.

indicative of bullying. These included crying and yelling. The authors used Mel Frequency Cepstral Coefficients (MFCC) to extract sound features and classified these recordings as verbal bullying or non-bullying by using a k-NN algorithm. The best-performing model for verbal violence identification obtained 70.4% accuracy. For physical bullying detection, k-NN was also the classifier of choice. The authors acquired acceleration and 3D gyros data from a movement sensor worn by students during simulations of various violent and non-violent activities. The best model for the detection of physical bullying activities obtained a 52.8% accuracy.

In [56], the authors developed WiVi, a school violence detection system based on the commercial Wi-Fi infrastructure. The authors observed that Channel State Information streams from Wi-Fi devices were affected by human actions and used this knowledge to build a ML model that detects changes in these streams that may indicate bullying activities. The model, which uses least square SVM (LSSVM) as its classifier, was tested on various real-life environments such as an office, a dorm room, and a laboratory. It obtained an average recall rate of 93.4%.

b: CHILD ABUSE

Studies within this subcategory propose AI methods to automatically detect potential cases of child abuse, where child abuse refers to the neglect or physical, sexual, or emotional violence of a child at the hands of parents, caregivers, or other figures of authority [85]. The study in [50] extracts a set of features from a dataset composed of semi-medical files of Dutch children, written by nurses and pediatricians, and uses it to build various ML models that predict whether a child is suffering from abuse. The best-performing model in terms of accuracy is an SVM model with a polynomial RBF. It obtained 88.0% accuracy.

In [51], the authors explore whether ML and predictive analytics help improve the accuracy in identifying cases of child welfare risk through the use of the decision tree (DT) algorithm, with boosting and ensemble learning techniques.

Using another approach, in [7], the authors worked on the automatic detection of CSA from self-figure drawings. They

built two CNN models: one to classify self-figure drawings as male or female, and another to differentiate self-figure drawings by clients with a history of sexual abuse from those without a history of sexual abuse according to their self-reports. The gender CNN model performed with an accuracy of 87%, whereas the CSA CNN model achieved an accuracy of 69%. The authors found that experts in the field of therapy still performed better than the model by sixteen percentage points, highlighting the complexity of the task.

c: IPV

Studies within this subcategory aim to automatically detect potential victims of DV, specifically IPV, a form of violence that affects 35% of women [1]. The proposal introduced in [52] addresses physical acts of IPV by utilizing a DL framework with class activation maps that automatically identifies facial injuries caused by IPV. The proposed model was tested against other models, outperforming them with an accuracy of 80%.

3) SAFETY

Studies within the safety category focus on using IoT technologies to create tools that will provide security for women and children in situations where they may be alone or unsafe. Solutions within this category use the Internet and other communication technologies to facilitate parents to monitor their children [58], or the ability of children [62] and women [66] to get help if they are involved in a violent situation. About 120 million girls and women under twenty years old have suffered from non-consensual sexual abuse [2], and 137 women are murdered by a family member every day [81]. Therefore, these studies address the need for a timely response and intervention to cases of violence. These studies aim to help victims to get help as soon as possible. Fig. 7 categorizes safety studies into mobile phone applications (10.5%), wearable or portable devices (84.2%), and non-portable devices (5.3%). Some of the safety studies fit into more than one subcategory. For instance, in [57] it was proposed a safety system for women that consists of a smart band and mobile phone application. Representative examples of each subcategory are summarized below.

a: MOBILE PHONE APPLICATIONS

Studies within this subcategory develop mobile phone applications that provide safety for women and children. The study introduced in [62] proposes a smartphone application for child safety. The application, meant to be installed on a child's smartphone, uses a geofencing technique, GPS, and a gravity sensor to monitor the child's location. If the child exits the geofence established by parents or caregivers, the device issues an alarm to predetermined contacts via SMS or Wi-Fi with the child's location. The smartphone will also begin voice recording for evidence of maltreatment or abuse and will send these recordings via SMS. In an emergency, the child can also shake the smartphone to activate the alarm mechanism described above.

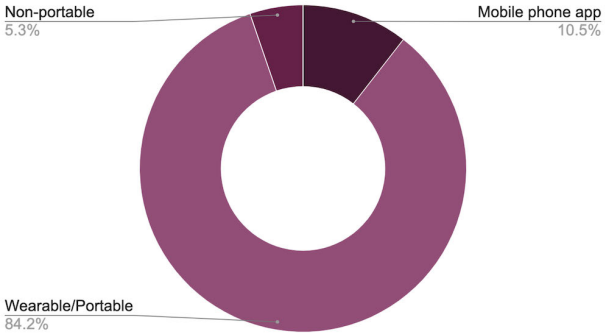

FIGURE 7. Safety studies split into subcategories.

In [74], the authors developed the mobile phone application WeDoCare for women's safety. WeDoCare monitors location through GPS and uses speech recognition and gesture detection technology to detect when the user is in a dangerous situation. The user activates the alarm mechanism for this application by three different methods: clicking a button on the application homepage, performing a chop gesture with the phone, or yelling, ''help.'' If activated, the application will send an SMS to the police with the location of the user.

b: WEARABLE/PORTABLE DEVICES

Studies within this category propose wearable or portable devices that provide safety for women or children. The study in [72] provides an IoT smart band connected to a smartphone application via Bluetooth that facilitates the ability of a woman to get assistance if she finds herself in a dangerous situation. The application is connected to the Internet, provides self-defense education videos, information on laws concerning women, an emergency button, and a map with secure locations that the user can go to if she finds herself in danger. The application allows volunteers to sign up to assist women who have activated the emergency mechanism or to include their homes as secure locations for women in danger to use. Users can activate the emergency mechanism of this system by pressing the emergency switch on the smart band or a button on the application. Once activated, the smartphone will send an emergency SMS containing the GPS location of the user to the nearest police station, volunteers, and her predetermined contacts.

Using a different approach, the authors in [61] considered situations in which a woman is in danger but is unable to press a help button or utter emergency keywords. The authors propose a wearable IoT device that predicts whether or not a woman is in danger by detecting changes in her body temperature and pulse rate. The device has body temperature and pulse sensors, which send data from the device to the cloud through the Internet or a ZigBee mesh network if there is no Internet connection. In the cloud, a LR model evaluates the data and determines if the user is in danger. In such a case, the system will automatically dial emergency contacts.

The work in [65] proposes a device aimed for the safety of women living in rural areas or where Internet and cellular networks are unreliable. The safety solution uses the IoT paradigm. It is in the form of a beacon device with a help button that the user can press if she feels threatened. Each beacon device has a unique identifier. Beacon devices are Bluetooth-connected to a Bluetooth network of solar-powered street poles and central stations installed for this application. When the user presses the help button, a distress message travels through the network of street poles until it reaches a central station. There, the help message is processed through a server so that the user can get help.

Some wearable solutions aimed at women's safety also include self-defense mechanisms. In [64] it was proposed an IoT system consisting of a wearable device with a mobile application that uses fingerprint scanning technology for activation. If activated, the device will send instant messages to emergency contacts and police stations. For self-defense, the system also includes an alarm and a shock generator. The alarm aims to get the attention of nearby people and also to scare away the perpetrator. If the perpetrator gets too close to the victim, the victim can use the shock wave generator to defend herself from the perpetrator. Other wearable solutions that include self-defense mechanisms are found in [66], [67], and [69].

c: NON-PORTABLE DEVICES

This subcategory is concerned with stationary or non-portable devices that help parents monitor their children to keep them safe from abuse. In [58], the authors propose a video surveillance system that parents can use to monitor their children while they are at daycare. The system is connected to the Internet through a Local Area Network (LAN) cable and provides real-time video streaming and motion detection. To verify that only those authorized to view the stream can access it, those authorized may only access it with a username and password.

4) EDUCATION

Studies that belong in the education category aim to train healthcare professionals and educate children about VAW and VAC. The proposals rely on the use of digital serious games (SG) that educate on the topics of VAW and VAC. As mentioned previously, IPV is the cause of more than a third of the women intentionally killed in 2017 [81]. Many women in the USA sought health services during the year before being murdered by an intimate partner [3]. Moreover, healthcare students have expressed feeling stressed about not having enough training on detecting victims of child abuse, as well as not knowing how to respond to the cases they do notice [10]. Therefore, it is necessary to provide appropriate training for healthcare professionals to detect cases of abuse and know the best approach towards helping women and children who suffer from violence. SG have been deemed beneficial in teaching STEM subjects such as mathematics [86] and have been used for health care purposes to positive results as well. For instance, cancer patients who played SG that taught them about the side effects of chemotherapy were more likely to adhere to their treatment than other patients [87]. Given these results, SG could help provide the education and training that healthcare workers need. SG can help also help lower the costs of traditional instruction [88].

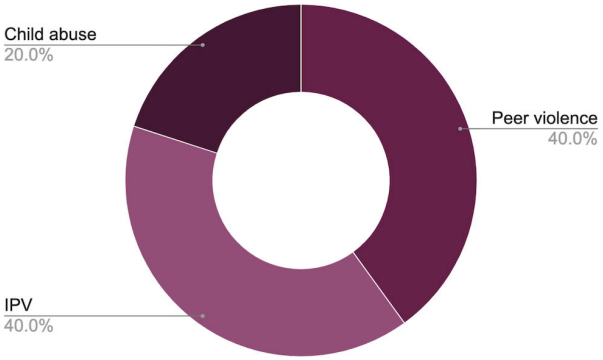

FIGURE 8. Education studies split into subcategories.

Classroom settings may benefit from the use of SG as well. The entertainment aspect of SG could help educate children and adolescents on norms and values that lead them to act in violence towards their peers, a necessary step for preventing VAW [2]. Fig. 8 visualizes that studies within this category provide education about the following VAW and VAC issues: peer violence (40.0%), IPV (40.0%), and child abuse (20.0%). It is worth highlighting that the study in [77] can belong in two categories because it addresses the intersection between IPV and child abuse.

a: PEER VIOLENCE

Studies in the subcategory of peer violence address VAC through SG that teach children about bullying in schools. In [11], the authors evaluated the design of the SG *Stop the Mob!*, a point-and-click SG for tablet and PC that addresses bullying in lower secondary schools. Students, playing as bystanders, were presented with scenarios in which their classmate Bob is bullied. Students were able to assess the situation and made decisions in response that range from helping Bob to bullying Bob. The SG lets students observe how their response to bullying affects Bob for better or for worse. By playing the game in a classroom where a teacher can help students reflect on the scenarios presented in the game, *Stop the Mob!* aims to help teach students that actions that students make regarding bullying have consequences.

In [80], the authors compare two prototypes of SG for PC that raise awareness about bullying amongst teenage students. Similar to *Stop the Mob!*, the prototypes are simulation-style games that aim to teach players about the consequences of bullying. The prototypes differ given that one is a cartoon-style game where students are guided from one scene to the next, whereas the other game is a fantasy game that allows players to move freely around the game world. The authors evaluated the prototypes in a classroom

with students between the ages of 12 and 15. The authors provided the students with post-game questionnaires, finding that 23 out of 26 students prefer the fantasy game because it lets characters walk around freely, making the game more adventurous and entertaining than the game where students are guided from scene to scene.

b: IPV

Studies grouped in this subcategory proposed SG that aimed to facilitate education regarding IPV. The proposal in [12] developed a PC game titled *Green Acres High* to educate adolescents on the topic of dating violence. Through a series of simulation-style lessons mediated in a classroom setting, the SG aims to facilitate teaching teenage students about healthy and abusive relationships. The authors tested the game on real students to both positive and negative feedback. Students said that its simulation-style SG allowed them to learn about the topic from experience. Moreover, the concept of learning from a digital game was appealing. Negative feedback focused on technological inefficiencies such as the game not loading and confusion regarding the instructions.

The work introduced in [78] caters to the needs of healthcare professionals. The authors propose a free online SG that educates healthcare providers about identifying and appropriately responding to patients who may be victims of DV. *Responding to DV in Clinical Settings* is comprised of seventeen modules, each with three sections: information and strategies regarding detection and response to cases of IPV as instructed by a qualified professional, a simulation where players got to apply the techniques learned in the previous section, and a quiz. The authors carried out a study to obtain feedback from healthcare workers who played the game. The game had positive feedback, where players referred to it as interesting, engaging, realistic, and easy to follow.

c: CHILD ABUSE

Studies placed in this subcategory use SG to address child abuse. The study in [10] introduces the *Computer Simulated Interactive Child Abuse Screening Tool (CSI-CAST)*. It is an assessment and training system for healthcare students which includes a simulation-style knowledge assessment component where students assume the roles of physicians evaluating a child patient. Students interact with the non-player characters in the simulation by asking them questions that may lead to the discovery of child physical abuse (CPA). The game records the questions asked by different players as features and uses ML to identify specific areas where the group needs further training regarding detecting and responding to CPA.

In [77], the authors address the intersection between IPV and child abuse in their SG named *None in Three*. It is a simulation-style game that aims to teach Caribbean people aged ten through eighteen about DV and provide training for professionals on this topic. Players play as different characters. For example, they can play as Diana, a victim of IPV, or Jesse, her son. Players can also play as minor characters such as teachers and friends of Jesse. Playing a variety of characters allows players to observe the consequences of IPV on Diana and Jesse. For example, players can witness Diana's conflicting feelings towards her husband. Players also become aware of how Jesse's grades and behavior deteriorate due to the violence at home. Jesse becomes a victim of abuse by being a witness to the violence inflicted upon his mother. Therefore, players can observe how VAW and VAC intersect.

B. ANSWER TO THE SECOND RESEARCH QUESTION

The previous section answered the first research question by providing examples of how CS and engineering technologies address VAW and VAC. This section details the CS and engineering approaches and technologies used by the selected studies. The authors answer the second research question by categorizing the selected studies as AI, IoT, and SG.

AI: About 64% of the studies addressed VAW and VAC by applying AI techniques. Specifically, these studies used ML to address VAW and VAC. All studies belonging to the online and offline detection categories used ML. 11% of the studies in the safety category, and 11% of the studies in the education category also employed ML. The following stages comprise the process of building a ML model for classification: data collection, features engineering, learning algorithm, and performance evaluation.

- Data collection: Fig. 9 shows that, out of all the studies that proposed ML models, 54.7% used data from social media (Twitter, Facebook, Instagram, and Reddit). Social media, in particular Twitter, is considered a valuable source of information regarding the issues of VAW and VAC. Aside from specific social media websites, 7.5% of studies originated from unspecified chat rooms, 1.9% of studies originated from YouTube, and 9.4% of studies originated from other websites. For non-Internet data, 13.2% of data was from experiments involving signals, voice recordings, or simulations, 11.3% of data was in the form of legal documents provided by police, healthcare, or social work, and 1.9% of the data originated from user inputs, as in the case of the work described in [10].
  Fig. 10 highlights that the majority of data collected were in text format (67.3%). This is followed by image or video files (17.3%), signals (11.5%), voice recordings (1.9%), and user input (1.9%).
  Methods for data collection included the Twitter API [21], Facebook Graph API [33], Urban Dictionary API [30], existing datasets [24], manual retrieval of online data [28], and experiments [55].
- Features engineering: As seen in Fig. 11, different data formats were collected for ML purposes. Therefore, different features engineering techniques were necessary for each format.
  - Text features engineering: Based on Fig. 11, it can be observed that there is not one pre-defined approach for text features engineering. However, sentence embeddings and part-of-speech tags were

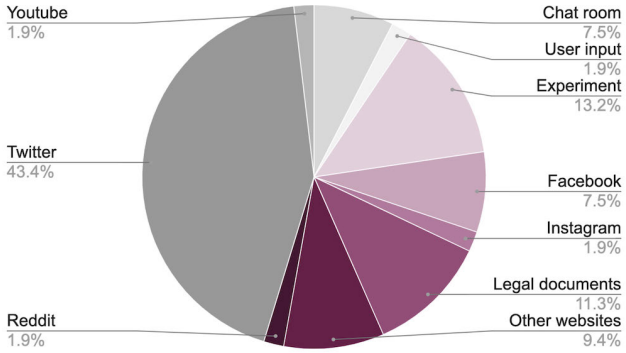

FIGURE 9. Sources of data collected for ML models.

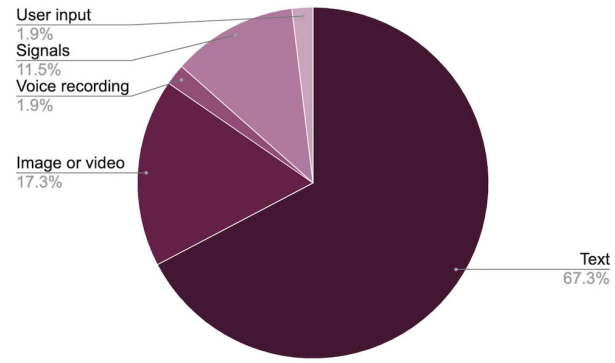

FIGURE 10. Format of data collected for ML models.

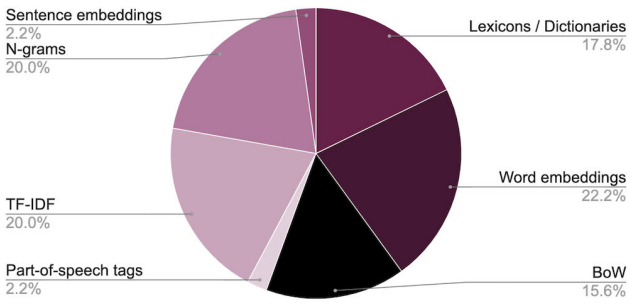

FIGURE 11. Text features engineering techniques (best model per study).

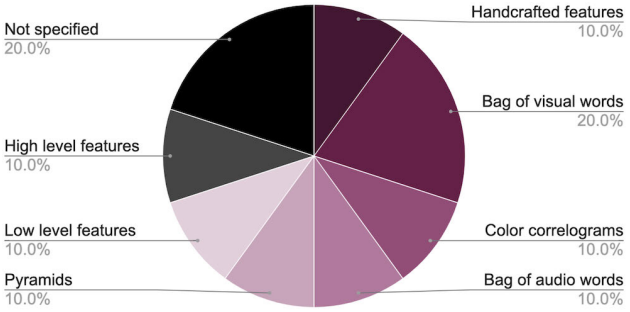

FIGURE 12. Visual features engineering (best model per study).

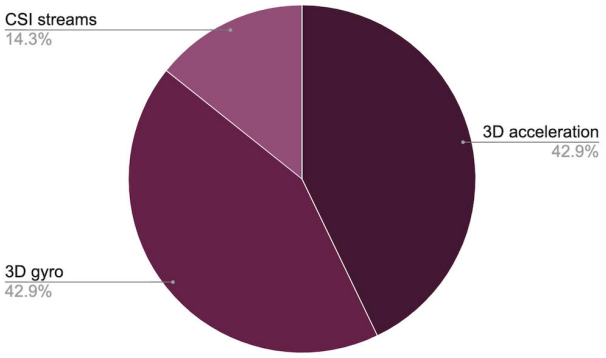

FIGURE 13. Signals features engineering (best model per study).

the least used methods of feature representation for text processing ML tasks at only 2.2% use each.

– Image or video (visual) features engineering: Due to the widespread of images and videos on the Internet, detecting violent and discriminatory behavior on these media has become very relevant. In this context, high-level features refer to things like faces and bodily forms, whereas low-level features refer to skin texture, shapes, or ratios [44], as shown in Fig. 12.
– Signal features engineering: For violent or dangerous activity recognition models within the area of VAW and VAC, such as those that identified bullying in schools [55], authors extracted features from sensors, such as accelerator signals (42.9%), gyro signals (42.9%), and CSI signals (14.3%). Fig. 13 highlights that there are not many CSI-based violent activity recognition studies addressing VAW and VAC. This area may benefit from further exploration.
– Audio features engineering: There was one study that involved audio features. In [53], the authors used MFCC to extract features from voice recordings. The goal was to detect physical and verbal bullying in schools through speech emotion recognition using the k-NN algorithm. They obtained an accuracy of 78%.
– Features engineering of user inputs: In the game described in [10], players role-play as doctors by simulating a medical appointment where they interact with a child patient and their parent with the final purpose of assessing whether the child has been a victim of physical violence. Each interaction between the doctor and patient is considered a feature. The authors utilized a recursive feature elimination method with a penalized logistic regression estimator to extract the features that most affect players' decision to classify the child is a victim or not.

- Learning algorithm for classification: Table 5 lists the best classifying approach per ML study. SVM was the most widely used ML classifier overall in the area of VAW and VAC. Performance varies among studies even

TABLE 5. ML models involving a classifier (best-performing model per study).

Format	Category	Subcategory	Classifier	Authors	Accu.	Prec.	Recall	F1
Text	Online	Reports of abuse	SVM	[15]	97.0	97.0	97.0	97.0
			CNN	[21]	83.0	N/A	N/A	N/A
			DT	[25]	95.0	94.0	94.0	94.0
			GRU	[33]	91.7	91.6	91.6	91.6
			Majority voting classifier	[37]	N/A	80.4	83.4	80.8
		Misogyny	SVM	[16]	79.7	N/A	N/A	N/A
				[18]	81.4	N/A	N/A	N/A
				[23]	80.5	N/A	N/A	N/A
				[24]	91.3	N/A	N/A	N/A
				[29]	79.4	N/A	N/A	N/A
				[35]	77.0	N/A	N/A	N/A
				[9]	91.3	87.1	91.1	89.1
			LR + Naive Bayes + SVM	[26]	N/A	N/A	N/A	79.0
			RNN + SVM	[17]	79.1	N/A	N/A	N/A
			Majority voting classifier	[19]	87.0	N/A	N/A	N/A
				[39]	75.4	74.7	73.9	74.2
			Bidirectional long short-term memory (Bi-LSTM)	[20]	78.9	N/A	N/A	N/A
			Classifiers fused by combining probabilities	[22]	62.7	N/A	N/A	N/A
			CNN	[27]	76.2	77.4	74.0	75.6
			Bi-GRU	[30]	93.1	N/A	N/A	N/A
			LSTM	[34]	84.6	80.6	75.7	78.1
			DL	[31]	72.0	N/A	N/A	N/A
			BERT	[9]	84.8	83.9	87.1	85.4
			NN + BERT	[40]	74.9	N/A	N/A	73.6
		Sexism	SVM	[28]	N/A	72.8	72.8	74.4
				[29]	89.3	N/A	N/A	N/A
			CNN + LR	[32]	N/A	98.4	96.5	97.4
			fastText	[38]	N/A	92.2	88.6	N/A
		Child grooming	SVM	[43]	97.0	N/A	N/A	N/A
			LR	[45]	95.0	N/A	N/A	N/A
			Fuzzy Twin SVM	[48]	60.9	N/A	N/A	N/A
		CSA material	SVM	[8]	N/A	89.9	66.1	76.1
		Peer violence	DT	[49]	94.2	99.2	94.1	96.6
	Offline	Child abuse	SVM	[50]	84.3	N/A	82.5	N/A
			Ensemble	[51]	93.0	N/A	N/A	N/A
Visual	Online	Sexism	K-NN	[28]	N/A	75.2	74.9	75.0
		CSA media	SVM	[42]	62.0-94.0	N/A	N/A	N/A
				[8]	94.6	N/A	N/A	N/A
				[44]	74.1	N/A	N/A	N/A
			DL	[46]	60.0-80.0	N/A	N/A	N/A
				[47]	79.8	68.6	64.6	66.5
			Linear classifier	[41]	69.4	N/A	N/A	N/A
	Offline	IPV	DL-based framework	[52]	80.0	N/A	N/A	N/A
		Child abuse	CNN	[7]	69.0	N/A	N/A	N/A
Signals	Offline	Peer violence	K-NN	[55]	80.0	N/A	N/A	N/A
				[53]	70.4	N/A	N/A	N/A
			LSSVM	[56]	N/A	N/A	93.4	N/A
			DT-RBF NN	[54]	93.7	92.6	84.4	88.3
	Safety		Boosted J48	[13]	100	N/A	N/A	N/A
			LR	[61]	73.3	N/A	N/A	N/A
Audio	Offline	Peer violence	K-NN	[53]	78.0	N/A	N/A	N/A

when the same classifier is used. The choice of dataset and features engineering technique per model affects the overall performance of the model.

- Performance metric: Accuracy, precision, recall, and F1-score were common performance metrics in the selected studies. Table 5 highlights that accuracy was the most widely used performance metric. Accuracy, precision, recall, and F1-score are defined below.
  - **Accuracy** = (TP + TN)/(TP+FP+TN+FN), where TP = true positives, TN = true negatives, FP = false positives, FN = false negatives.
  - **Precision** = TP/(TP + FP)
  - **Recall** = TP/(TP + FN)
  - **F1-score** = 2 × ((p × r)/(p + r)), where p is precision, and r stands for recall.

Table 5 lists the selected studies that used ML to address VAW and VAC.

IoT: 24% of the selected studies, namely every study within the safety category, addressed the issue of VAW and VAC through violence response systems based on IoT. This study organizes technologies employed by IoT solutions into the following categories: environment and user monitoring, self-defense, evidence-collection, communication technologies, location-monitoring, activation techniques, controllers, cloud services, and visualization techniques.

- Environment and user monitoring: IoT proposals aim to monitor the environment, the vital signs, or behavioral patterns of users. For this purpose, 63% of the solutions from the safety category used sensors. 25% of the offline detection studies incorporated sensors as well. Given

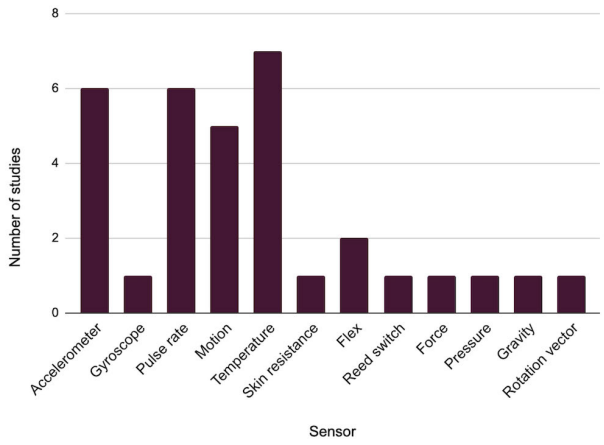

FIGURE 14. Distribution of sensors used in IoT applications.

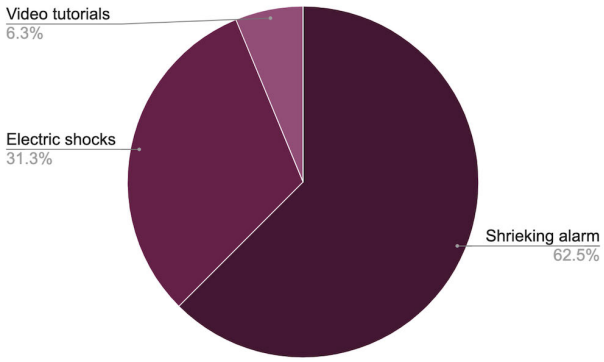

FIGURE 15. Distribution of self-defense tools in IoT applications.

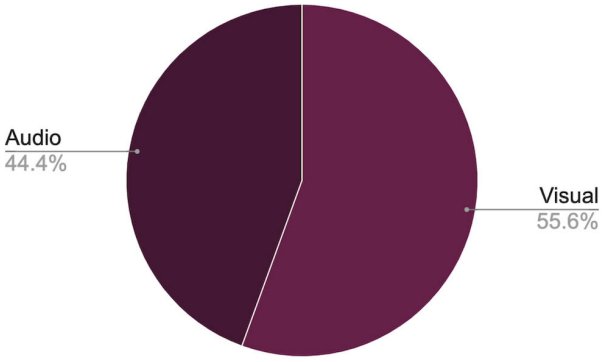

FIGURE 16. Evidence collection mechanism distribution in IoT applications.

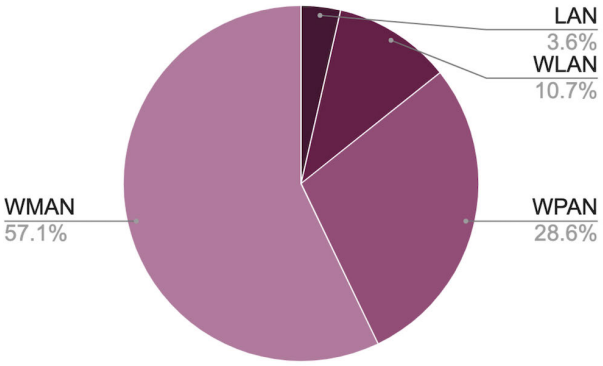

FIGURE 17. Distribution of communication technologies in IoT applications.

that studies in the offline detection category do not focus on creating an entire violence response system, but only on developing a ML learning model, the use of sensors in these cases is not considered for this category. Fig. 14 shows that the most widely used sensor was the temperature sensor, followed by accelerometer and pulse rate sensors, highlighting that sudden changes in body temperature, pulse rate, and velocity were considered good indicators of victimization.

- Self-defense: Nearly 63% of IoT solutions incorporated self-defense technologies into their IoT systems. These technologies consist of shrieking alarms, electric shock generators, and video tutorials. Shrieking alarms emit a loud noise when activated, which may scare the attacker away, and video tutorials taught the viewer how to protect herself against an attacker. The most widely used self-defense tool was the shrieking alarm, as evidenced by Fig. 15.
- Evidence-collection: 37% of the safety studies incorporated technologies for evidence collection. Fig. 16 shows that visual evidence techniques, such as photography and video, are incorporated into safety solutions as commonly audio recording techniques. Therefore researchers view visual and audio are both valuable forms of evidence.
- Communication technologies: Every safety study proposed the use of at least one communication technology. Fig. 17 shows that the most widely used communication technologies were Wireless Metropolitan Area Networks (56.7%), namely cellular technologies (GPRS/GSM/3G/4G). Wireless Personal Area Networks such as ZigBee and Bluetooth (26.7%), Wireless Local Area Networks like Wi-Fi (13.3%), and Local Area Networks like Ethernet (3.3%) follow. Wireless communication technologies were vastly preferred over wired ones.
- Location-monitoring: Many proposals in the safety category consider location monitoring. Specifically, Fig. 18 shows that 89% of studies in the safety category use location-monitoring technology such as GPS for location-sharing and highlights a possible belief that monitoring vulnerable populations can aid in preventing their victimization.
- System activation techniques: Fig. 19 shows that 57.9% of safety solutions relied on a switch, the utterance of an emergency keyword or the shaking of the device [74] to activate the emergency mechanism. On the other hand, 42.1% of safety solutions had an automatic

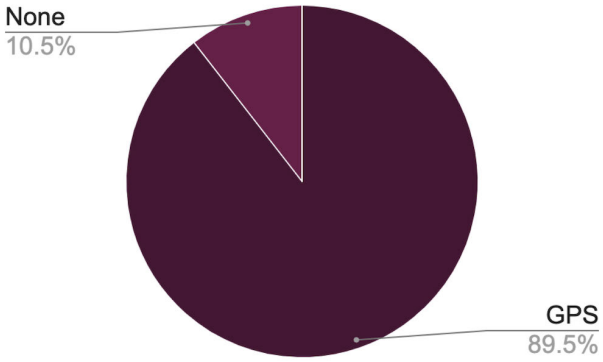

FIGURE 18. Location monitoring technologies employed by IoT applications.

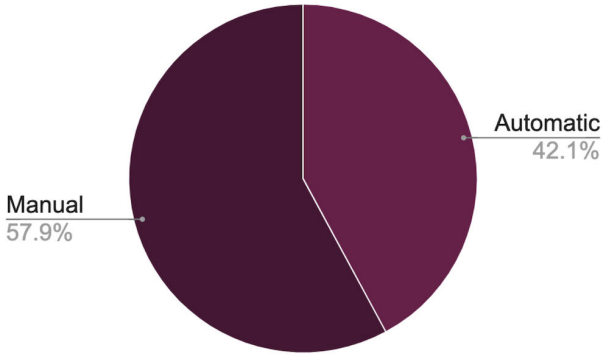

FIGURE 19. System activation technique for IoT applications.

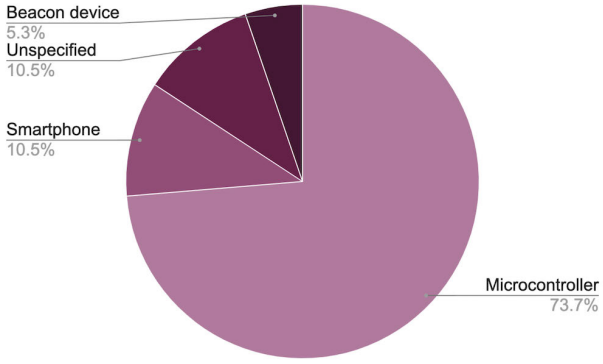

FIGURE 20. Distribution of devices for IoT applications.

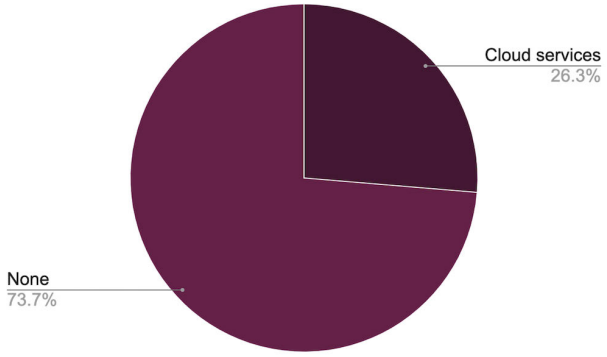

FIGURE 21. Cloud services usage in IoT applications.

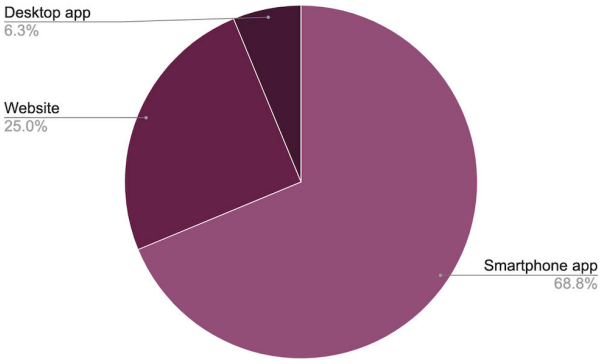

FIGURE 22. Visualization techniques used by IoT applications.

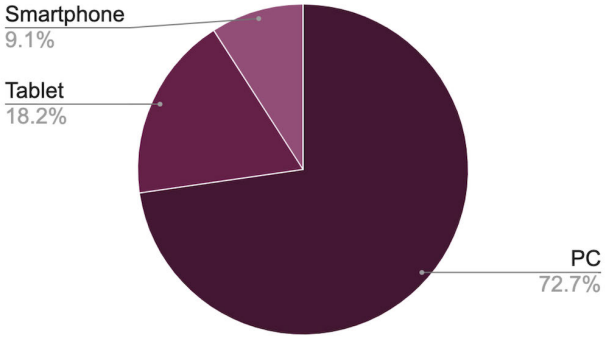

FIGURE 23. Gaming platforms utilized in SG.

activation mechanism based on AI [13] or a mathematical model [68].

- Devices: Fig. 20 shows that 73.7% of safety or IoT solutions used microcontroller (MCU) development units to build prototypes and evaluate their proposals. These include Arduino [60] or Raspberry Pi [58] connected to a cellphone through Bluetooth or working on its own. Additionally, 10.5% of solutions relied on the cellphone as the main unit of control. 5.3% of devices used a beacon device and 10.5% an unspecified wearable gadget.
- Cloud services: Fig. 21 highlights that only 26.3% of IoT applications use the cloud for storage or remote computing.
- Visualization techniques: 68% of IoT applications involved a visualization technique. Fig. 22 shows that the most widely used visualization methods are smartphone applications (68.8%), followed by websites (25.0%), and desktop applications (6.3%).

Serious games: Every study in the education category, 11.3% of all studies, proposed the use of SG. Technologies used by SG solutions that address VAW and VAC can be further organized in the following criteria: platform, graphics, Internet, and AI.

- Platform: Fig. 23 shows that PC was the platform of choice in 72.7% of SG applications. Tablets follow with 18.2% and smartphones with 9.1%. Given the low percentage of SG applications involving smartphones, there is a huge potential to expand SG applications in this area.

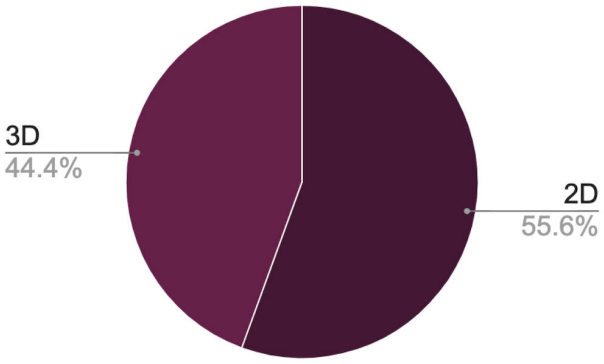

FIGURE 24. Graphics used in SG.

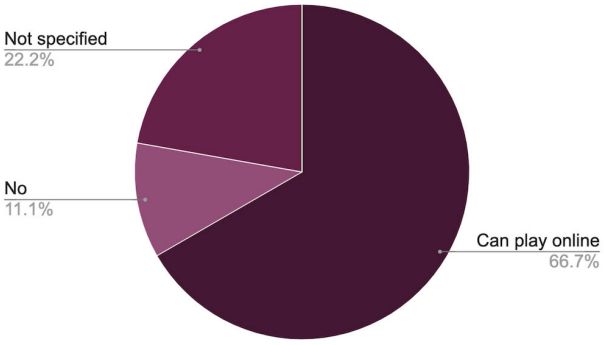

FIGURE 25. Proportion of SG that could be played online.

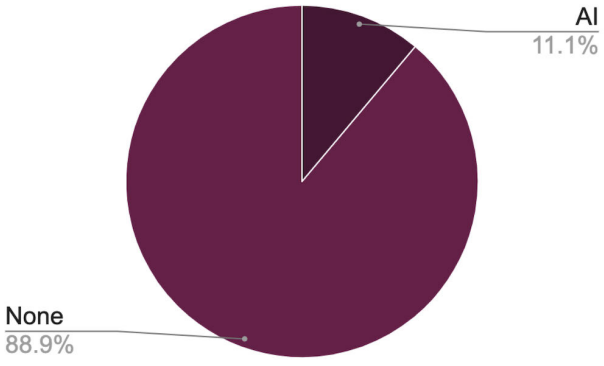

FIGURE 26. Proportion of SG that used AI technology.

- Graphics: Fig. 24 shows that two-dimensional (2-D) SG were used slightly more than their more sophisticated three-dimensional (3-D) counterpart. 2-D graphics were used in 55.6% of SG, whereas 3-D graphics were used in 44.4%.
- Internet: Fig. 25 shows that 66.7% of SG in this study could be played online. Only one SG (11.1%) required users to install the game on their computer. 22.2% of studies involving SG did not specify whether their SG could be played online or not.
- AI: Fig. 26 shows that only 11.1% of studies involving SG, one study, used AI techniques in their design. It would be interesting to incorporate AI into more SG applications that address VAW and VAC and explore how players may benefit from AI in SG.

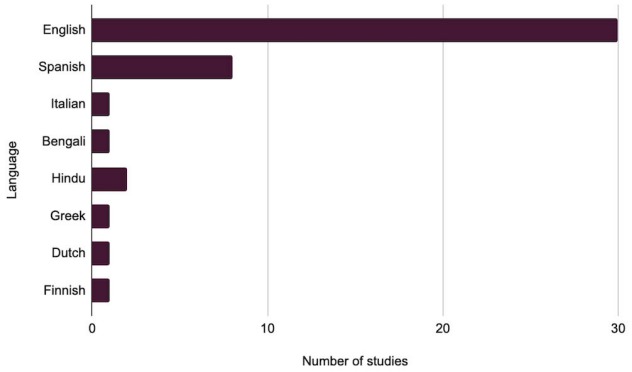

FIGURE 27. Language distribution in ML models that performed text analysis.

V. ANALYSIS

An analysis of the difficulties and limitations perceived in the primary studies has led to insights and open issues described below.

A. EXPLORE MORE SOCIAL MEDIA

Studies dealing with the detection of abusive phenomena on the Internet would benefit from exploring other social media platforms. Twitter was the most widely used social media platform for data extraction in ML models. Studies could expand their research onto the YouTube comment section or Instagram, given that these are frequently visited social media platforms [89]. There were no studies that explored child grooming or pedophilia detection on social media, so it offers potential as an area of research given that 94% of adolescent people living in developed nations use a social media platform [90].

B. MORE LANGUAGE DIVERSITY FOR ML TASKS

Studies dealing with the detection of abusive phenomena from textual data used data primarily in the English language. VAW and VAC are prominent issues worldwide. There should be more studies addressing the detection of abusive phenomena in other languages. In particular, no studies that detected CSA media or child grooming in online chat rooms were in a language other than English. Fig. 27 shows the full distribution of languages in ML models that performed text analysis.

C. MORE AUTOMATION OF SAFETY DEVICES

The majority of safety devices required the user to activate the emergency mechanism manually. Users may not be able to do this in an emergency due to not having enough time, being in the middle of an assault, or being paralyzed with fear. Therefore, there should be a greater focus to automate the activation of emergency mechanisms in safety devices.

D. MORE THOUGHTFUL DESIGN FOR WEARABLE TECHNOLOGIES

Some wearable safety devices were very large or required users to hold them at all times. This is not discreet and it

is impractical for daily use. Therefore, there is a necessity to make wearable devices that are ubiquitous or non-invasive and will not inconvenience the user.

E. SECURITY AND PRIVACY

Some anti-abuse solutions facilitate abuse. Every safety device used either location-monitoring technology or visual monitoring technology. Devices intended for keeping children from abuse allowed those with access to the system the ability to monitor the children at all times. This type of technology can facilitate abuse since perpetrators can use this type of system to monitor their victims at all times. Designers of devices for women and child safety should make sure that their proposed solutions are indeed safe and cannot be used for malicious purposes.

Moreover, location-monitoring and visual monitoring in every safety device may imply that users must give up their right to privacy to stay safe.

F. SAFETY DEVICES WOULD BENEFIT FROM SIMULATIONS

In most cases, safety devices send a notification to the police or predetermined contacts when the user is in danger. Some devices may emit a loud alarm to alert nearby civilians that the user needs help. Therefore, the effectiveness of these devices depends on whether anyone decides to act upon the victim's call for help. Effectiveness also depends on how long it takes for that person to get to the crime scene. Given these considerations, safety devices may benefit from simulations that will allow the creators of these devices to get an idea of how long it takes for victims to get help. Researchers must incorporate this information into safety device studies to set realistic expectations of how much these devices can do to help potential victims and diminish any false sense of security that may arise from using these devices.

G. EDUCATION FOR BOYS

Acts of IPV and sexual violence are more likely to be committed by men upon women [1]. There was no educational SG addressing issues of VAW that was aimed directly at boys or men. Beliefs and norms that condone or lead to the acceptance of VAW must be challenged to prevent VAW [1]. There are SG that teach children about peer violence; it might be beneficial to have an educational SG that challenges men about ideologies and beliefs that make them perpetrators of VAW.

H. TECHNOLOGY AS AN AUXILIARY TOOL

Every SG that addressed VAW and VAC required for there to be a teacher or a medical professional that helped players reflect upon the content of the games. Similarly, offline detection studies are mostly intended to create tools to facilitate professionals' detection of VAW or VAC. They do not mean to replace professionals who do these jobs. Although technology can have a positive impact in preventing violence, it should be considered an auxiliary tool rather than a solution to VAW and VAC.

I. AI FAIRNESS

VAW and VAC are sensitive topics. Unfortunately, AI algorithms have biases that may affect their performance. They could unfairly criminalize someone or ignore violent behavior due to bias. AI fairness is a recent research area that should be incorporated into AI proposals that address VAW and VAC.

VI. CONCLUSION

This paper presented a systematic literature review of CS and related technologies that address VAW and VAC. A total of 73 primary studies were selected from six different sources to answer two research questions. Selected studies came from every continent, reflecting the pandemic spread of VAW and VAC. The study revealed that most research focuses on detecting abusive acts against women and children in online settings (50.7%). Safety solutions follow with 26.0%, education with 12.3%, and offline detection with 11.0%.

Selected studies address the urgent need to prevent and respond to VAW and VAC by proposing applications based on AI, IoT, and SG. ML, a subset of AI techniques, detects VAW and VAC in online and offline settings. Studies also propose IoT-based violence response systems that makes use of AI, sensors, electric shock generators, alarms, cameras and microphones, communication technologies, GPS, controllers, cloud services, and visualization platforms such as smartphone applications and websites to facilitate women and children's ability to get the assistance they need during a violent event. Lastly, studies created digital simulation-style SG to educate children and healthcare professionals about VAW and VAC.

Even though most studies approached VAW and VAC as separate issues, the methodologies used to attack these two problems are very similar, further emphasizing the intersection that exists between VAW and VAC [2]. In the future, it would be interesting to see more CS and engineering studies that address the correlations between VAW and VAC, given that addressing both issues at once may be beneficial to preventing violence against both groups.

This paper provided a systematic review that shares a glimpse into what the CS and engineering research community is doing to contribute to the fight against VAW and VAC. Although VAW and VAC are widespread and complicated social issues, technology has the potential to contribute meaningfully to prevent violence and make the world a safer place for women and children.

REFERENCES

[1] V. P. Alliance. (2021). *Definition and Typology of Violence*. [Online]. Available: https://www.who.int/violenceprevention/approach/definition/en/

[2] W. H. Organization. (2020). *Global Status Report on Preventing Violence Against Children*. Geneva, Switzerland: World Health Organization. [Online]. Available: https://www.who.int/teams/social-determinants-of-health/violence-preven tion/global-status-report-on-violence-against-children-2020

[3] WHO and P. A. H. O. (PAHO). (2012) *Feminicide. Understanding and Addressing Violence Against Women*. [Online]. Available: https://www.who.int/reproductivehealth/publications/violence/rhr12_38/en/

[4] UN and P. Mlambo-Ngcuka. (2021). *Violence Against Women and Girls: The Shadow Pandemic*. [Online]. Available: https://www.unwomen.org/en/news/stories/2020/4/statement-ed-phumzile-violence-against-women-during-pandemic

[5] I. N. Y. de Estadística Geografía (INEGI), *Encuesta Nacional sobre la Dinámica de las Relaciones en los Hogares (ENDIREH). Mexico*. Aguascalientes, México: Instituto Nacional de Estadística y Geografía, 2016. [Online]. Available: https://www.inegi.org.mx/rnm/index.php/catalog/286

[6] W. H. Organization. (2016). *Understanding and Addressing Violence Against Women*. [Online]. Available: https://www.who.int/reproductivehealth/topics/violence/vaw_series/en/

[7] L. Kissos, L. Goldner, M. Butman, N. Eliyahu, and R. Lev-Wiesel, "Can artificial intelligence achieve human-level performance? A pilot study of childhood sexual abuse detection in self-figure drawings," *Child Abuse Neglect*, vol. 109, Nov. 2020, Art. no. 104755, doi: 10.1016/j.chiabu.2020.104755.

[8] C. Peersman, C. Schulze, A. Rashid, M. Brennan, and C. Fischer, "iCOP: Automatically identifying new child abuse media in P2P networks," in *Proc. IEEE Secur. Privacy Workshops*, San Jose, CA, USA, May 2014, pp. 124–131, doi: 10.1109/SPW.2014.27.

[9] E. W. Pamungkas, V. Basile, and V. Patti, "Misogyny detection in Twitter: A multilingual and cross-domain study," *Inf. Process. Manage.*, vol. 57, no. 6, Nov. 2020, Art. no. 102360, doi: 10.1016/j.ipm.2020.102360.

[10] R. Zhao, C. R. Shelton, M. D. Hetzel-Riggin, J. LaRiccia, G. Louchart, A. Meanor, and H. J. Risser, "Knowledge assessment: Game for assessment of symptoms of child physical abuse," in *Proc. 14th Int. Conf. Found. Digital Games*, New York, NY, USA, Aug. 2019, pp. 1–7, doi: 10.1145/3337722.3337747.

[11] C. Walsh and A. Schmoelz, "Stop the Mob! Pre-service teachers designing a serious game to challenge bullying," in *Games and Learning Alliance* (Lecture Notes in Computer Science), I. A. D. Gloria and R. Veltkamp, Eds. Cham, Switzerland: Springer, Jun. 2016, pp. 431–440, doi: 10.1007/978-3-319-40216-1_48.

[12] E. Bowen, K. Walker, M. Mawer, E. Holdsworth, E. Sorbring, B. Helsing, and S. Jans, "'It's like you're actually playing as yourself': Development and preliminary evaluation of 'green acres high', a serious game-based primary intervention to combat adolescent dating violence," *Psychosocial Intervent.*, vol. 23, no. 1, pp. 43–55, Apr. 2014, doi: 10.5093/in2014a5.

[13] A. Jatti, M. Kannan, R. M. Alisha, P. Vijayalakshmi, and S. Sinha, "Design and development of an IOT based wearable device for the safety and security of women and girl children," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, Bangalore, India, May 2016, pp. 1108–1112, doi: 10.1109/rteict.2016.7808003.

[14] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele Univ., Keele, U.K., Tech. Rep. EBSE-2007-01, Jul. 2007. [Online]. Available: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

[15] S. Subramani, H. Q. Vu, and H. Wang, "Intent classification using feature sets for domestic violence discourse on social media," in *Proc. 4th Asia–Pacific World Congr. Comput. Sci. Eng. (APWC on CSE)*, Mana Island, Fiji, Dec. 2017, pp. 129–136, doi: 10.1109/APWConCSE.2017.00030.

[16] M. Anzovino, E. Fersini, and P. Rosso, "Automatic identification and classification of misogynistic language on Twitter," in *Natural Language Processing and Information Systems* (Lecture Notes in Computer Science), vol. 10859. Paris, France: Springer, May 2018, pp. 57–64, doi: 10.1007/978-3-319-91947-8_6.

[17] R. Ahluwalia, E. Shcherbinina, E. Callow, A. Nascimento, and M. De Cock, "Detecting misogynous tweets," in *Proc. 3rd Workshop Eval. Human Lang. Technol. Iberian Lang. (IberEval) Co-Located 34th Conf. Spanish Soc. Natural Lang. Process. (SEPLN)*, S. Sevilla, Ed. Aachen, Germany: CEUR-WS.org, RWTH Aachen Informatik V (Information Systems), 2018, pp. 242–248. [Online]. Available: http://ceur-ws.org/Vol-2150/AMI_paper3.pdf

[18] J. S. Canós, "Misogyny identification through SVM at IberEval 2018," in *Proc. 3rd Workshop Eval. Hum. Lang. Technol. Iberian Lang. (IberEval) Co-Located 34th Conf. Spanish Soc. Natural Lang. Process. (SEPLN)*, Sep. 2018, pp. 229–233. [Online]. Available: http://ceur-ws.org/Vol-2150/AMI_paper1.pdf

[19] S. Frenda, B. Ghanem, and M. Montes-y Gómez, "Exploration of misogyny in Spanish and English tweets," in *Proc. 3rd Workshop Eval. Hum. Lang. Technol. for Iberian Lang. (IberEval) Co-Located 34th Conf. Spanish Soc. Natural Lang. Process. (SEPLN)*, vol. 2150, Sep. 2018, pp. 260–267. [Online]. Available: http://ceur-ws.org/Vol-2150/AMI_paper6.pdf

[20] I. Goenaga, A. Atutxa, K. Gojenola, A. Casillas, A. D. Ilarraza, and N. Ezeiza, "Automatic misogyny identification using neural networks," in *Proc. 3rd Workshop Eval. Hum. Lang. Technol. Iberian Lang. (IberEval) Co-Located 34th Conf. Spanish Soc. Natural Lang. Process.*, Sep. 2018, pp. 249–254. [Online]. Available: http://ceur-ws.org/Vol-2150/AMI_paper4.pdf

[21] A. Khatua, E. Cambria, and A. Khatua, "Sounds of silence breakers: Exploring sexual violence on Twitter," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Barcelona, Spain, Aug. 2018, pp. 397–400, doi: 10.1109/asonam.2018.8508576.

[22] H. Liu, F. Chiroma, and M. Cocea, "Identification and classification of misogynous tweets using multi-classifier fusion," in *Proc. 3rd Workshop Eval. Hum. Lang. Technol. Iberian Lang. (IberEval) Co-Located 34th Conf. Spanish Soc. for Natural Lang. Process. (SEPLN)*, Sep. 2018, pp. 268–273. [Online]. Available: http://ceur-ws.org/Vol-2150/

[23] V. Nina-Alcocer, "Ami at IberEval 2018 automatic misogyny identification in Spanish and English tweets," in *Proc. 3rd Workshop Eval. Hum. Lang. Technol. Iberian Lang. (IberEval) Co-Located 34th Conf. Spanish Soc. Natural Lang. Process. (SEPLN)*, 2018, pp. 274–279.

[24] E. W. Pamungkas, A. T. Cignarella, V. Basile, and V. Patti, "Exploiting lexical knowledge for detecting misogyny in English and Spanish tweets," in *Proc. 3rd Workshop Eval. Hum. Lang. Technol. Iberian Lang. (IberEval) Co-Located 34th Conf. Spanish Soc. Natural Lang. Process. (SEPLN)*, J. G. Rosso, R. Martínez, S. Montalvo, and J. C. de Albornoz, Eds., Madrid, Spain. Aachen, Germany: CEUR-WS.org, RWTH Aachen Informatik V (Information Systems), Sep. 2018, pp. 234–241. [Online]. Available: http://ceur-ws.org/Vol-2150/AMI_paper2.pdf

[25] S. Subramani, H. Wang, M. R. Islam, A. Ulhaq, and M. O'Connor, "Child abuse and domestic abuse: Content and feature analysis from social media disclosures," in *Databases Theory and Applications* (Lecture Notes in Computer Science), G. C. Wang, J. Chen, and J. Qi, Eds. Cham, Switzerland: Springer, May 2018, doi: 10.1007/978-3-319-92013-9_14.

[26] E. Shushkevich and J. Cardiff, "Misogyny detection and classification in English tweets: The experience of the ITT team," in *Proc. 6th Eval. Campaign Natural Lang. Process. Speech Tools Italian. Final Workshop (EVALITA) Co-Located 5th Italian Conf. Comput. Linguistics (CLiC-It)* CEUR Workshop Proceedings, T. Caselli, N. Novielli, V. Patti, and P. Rosso, Eds. vol. 2263. Turin, Italy: CEUR, Dec. 2018. [Online]. Available: http://ceur-ws.org/Vol-2263/paper030.pdf

[27] M. A. Bashar, R. Nayak, N. Suzor, and B. Weir, "Misogynistic tweet detection: Modelling CNN with small datasets," in *Data Mining* (Communications in Computer and Information Science), vol. 996. Singapore: Springer, Feb. 2019, pp. 3–16, doi: 10.1007/978-981-13-6661-1_1.

[28] E. Fersini, F. Gasparini, and S. Corchs, "Detecting sexist MEME on the web: A study on textual and visual cues," in *Proc. 8th Int. Conf. Affect. Comput. Intell. Interact. Workshops Demos (ACIIW)*, Cambridge, U.K., Sep. 2019, pp. 226–231, doi: 10.1109/aciiw.2019.8925199.

[29] S. Frenda, B. Ghanem, M. Montes-y-Gómez, and P. Rosso, "Online hate speech against women: Automatic identification of misogyny and sexism on Twitter," *J. Intell. Fuzzy Syst.*, vol. 36, no. 5, pp. 4743–4752, May 2019, doi: 10.3233/jifs-179023.

[30] T. Lynn, P. T. Endo, P. Rosati, I. Silva, and L. Santos, "A comparison of machine learning approaches for detecting misogynistic speech in urban dictionary," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (Cyber SA)*, Oxford, U.K., Jun. 2019, pp. 1–8, doi: 10.1109/CyberSA.2019.8899669.

[31] D. Nozza, C. Volpetti, and E. Fersini, "Unintended bias in misogyny detection," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell.*, Thessaloniki, Greece, Oct. 2019, pp. 149–155, doi: 10.1145/3350546.3352512.

[32] M. Sajjad, F. Zulifqar, M. U. G. Khan, and M. Azeem, "Hate speech detection using fusion approach," in *Proc. Int. Conf. Appl. Eng. Math. (ICAEM)*, Taxila, Pakistan, Aug. 2019, pp. 251–255, doi: 10.1109/icaem.2019.8853762.

[33] S. Subramani, S. Michalska, H. Wang, J. Du, Y. Zhang, and H. Shakeel, "Deep learning for multi-class identification from domestic violence online posts," *IEEE Access*, vol. 7, pp. 46210–46224, Apr. 2019, doi: 10.1109/access.2019.2908827.

[34] M. A. Bashar, R. Nayak, and N. Suzor, "Regularising LSTM classifier by transfer learning for detecting misogynistic tweets with small training set," *Knowl. Inf. Syst.*, vol. 62, no. 10, pp. 4029–4054, Oct. 2020, doi: 10.1007/s10115-020-01481-0.

[35] M. Cánovas-García, J. A. García-Díaz, and R. Valencia-García, "Automatic misogyny detection with linguistic and morphological features in Spanish," in *Proc. Int. Conf. Technol. Innov.* (Communications in Computer and Information Science), vol. 1309. New York, NY, USA: Springer, 2019, pp. 30–42, doi: 10.1007/978-3-030-62015-8_3.

[36] J. M. Coria, S. Ghannay, S. Rosset, and H. Bredin, "A metric learning approach to misogyny categorization," in *Proc. 5th Workshop Represent. Learn. NLP*, 2020, pp. 89–94, doi: 10.18653/v1/2020.repl4nlp-1.12.

[37] N. Hassan, A. Poudel, J. Hale, C. Hubacek, K. T. Huq, S. K. Santu, and I. Ahmed, "Towards automated sexual violence report tracking," in *Proc. Int. AAAI Conf. Web Social Media*, vol. 14, 2020, pp. 250–259. [Online]. Available: https://ojs.aaai.org/index.php/ICWSM/article/view/7296

[38] V. K. Jha, P. Hrudya, P. N. Vinu, V. Vijayan, and P. Prabaharan, "DHOT-repository and classification of offensive tweets in the Hindi language," *Procedia Comput. Sci.*, vol. 171, pp. 2324–2333, Jan. 2020, doi: 10.1016/j.procs.2020.04.252.

[39] F.-M. Plaza-Del-Arco, M. D. Molina-González, L. A. Urena-López, and M. T. Martín-Valdivia, "Detecting misogyny and xenophobia in Spanish tweets using language technologies," *ACM Trans. Internet Technol.*, vol. 20, no. 2, pp. 1533–5399, May 2020, doi: 10.1145/3369869.

[40] N. S. Samghabadi, P. Patwa, S. Pykl, P. Mukherjee, A. Das, and T. Solorio, "Aggression and misogyny detection using BERT: A multi-task approach," in *Proc. 2nd Workshop Trolling, Aggression Cyberbullying*, Marseille, France, 2020, pp. 126–131.

[41] A. Ibrahim and M. V. Martin, "Detecting and preventing the electronic transmission of illicit images and its network performance," in *Digital Forensics and Cyber Crime* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). vol. 31, Berlin, Germany: Springer, 2010, pp. 139–150, doi: 10.1007/978-3-642-11534-9_14.

[42] A. Ulges and A. Stahl, "Automatic detection of child pornography using color visual words," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2011, pp. 1–6, doi: 10.1109/icme.2011.6011977.

[43] D. Bogdanova, P. Rosso, and T. Solorio, "Exploring high-level features for detecting cyberpedophilia," *Comput. Speech Lang.*, vol. 28, no. 1, pp. 108–120, 2014, doi: 10.1016/j.csl.2013.04.007.

[44] N. Sae-Bae, X. Sun, H. T. Sencar, and N. D. Memon, "Towards automatic detection of child pornography," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Paris, France, Oct. 2014, pp. 5332–5336, doi: 10.1109/ICIP.2014.7026079.

[45] H. Pranoto, F. E. Gunawan, and B. Soewito, "Logistic models for classifying online grooming conversation," *Proc. Comput. Sci.*, vol. 59, pp. 357–365, 2015, doi: 10.1016/j.procs.2015.07.536.

[46] J. Dalins, Y. Tyshetskiy, C. Wilson, and M. J. Carman, "Laying foundations for effective machine learning in law enforcement. Majura–A labelling schema for child exploitation materials," *Digit. Investigation*, vol. 26, pp. 40–54, Sep. 2018, doi: 10.1016/j.diin.2018.05.004.

[47] J. Macedo, F. Costa, and J. A. dos Santos, "A benchmark methodology for child pornography detection," in *Proc. 31st SIBGRAPI Conf. Graph., Patterns Images (SIBGRAPI)*, Oct. 2018, pp. 455–462, 10.1109/SIBGRAPI.2018.00065

[48] P. Anderson, Z. Zuo, L. Yang, and Y. Qu, "An intelligent online grooming detection system using AI technologies," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, New Orleans, LA, USA, Jun. 2019, pp. 1–6, doi: 10.1109/fuzz-ieee.2019.8858973.

[49] S. Nikiforos, S. Tzanavaris, and K.-L. Kermanidis, "Virtual learning communities (VLCs) rethinking: Collaboration between learning communities," *Educ. Inf. Technol.*, vol. 25, no. 5, pp. 3659–3675, Sep. 2020, doi: 10.1007/s10639-020-10132-4.

[50] C. Amrit, T. Paauw, R. Aly, and M. Lavric, "Identifying child abuse through text mining and machine learning," *Expert Syst. Appl.*, vol. 88, pp. 402–418, Dec. 2017, doi: 10.1016/j.eswa.2017.06.035.

[51] I. M. Schwartz, P. York, E. Nowakowski-Sims, and A. Ramos-Hernandez, "Predictive and prescriptive analytics, machine learning and child welfare risk assessment: The broward county experience," *Children Youth Services Rev.*, vol. 81, pp. 309–320, Oct. 2017, doi: 10.1016/j.childyouth.2017.08.020.

[52] P. Majumdar, S. Chhabra, R. Singh, and M. Vatsa, "On detecting domestic abuse via faces," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2018, pp. 859–871, doi: 10.1109/cvprw.2018.00292.

[53] S. Gao and L. Ye, "A physical and verbal bullying detecting algorithm based on K-NN for school bullying prevention," *Artificial Intelligence for Communications and Networks* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 287. Harbin, China: Springer, Jul. 2019, pp. 150–157, doi: 10.1007/978-3-030-22971-9_13.

[54] L. Ye, J. Shi, H. Ferdinando, T. Seppänen, and E. Alasaarela, "School violence detection based on multi-sensor fusion and improved relief-F algorithms," in *Proc. Int. Conf. Artif. Intell. Commun. Netw.* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 287. New York, NY, USA: Springer, 2019, doi: 10.1007/978-3-030-22971-9_22.

[55] L. Ye, H. Ferdinando, T. Seppanen, T. Huuki, and E. Alasaarela, "An instance-based physical violence detection algorithm for school bullying prevention," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, pp. 1384–1388, doi: 10.1109/iwcmc.2015.7289284.

[56] L. Zhang, X. Ruan, and J. Wang, "WiVi: A ubiquitous violence detection system with commercial WiFi devices," *IEEE Access*, vol. 8, pp. 6662–6672, Dec. 2020, doi: 10.1109/access.2019.2962813.

[57] G. C. Harikiran, K. Menasinkai, and S. Shirol, "Smart security solution for women based on Internet of Things(IOT)," in *Proc. Int. Conf. Elect., Electron., Optim. Techn. (ICEEOT)*, Chennai, India, Mar. 2016, pp. 3551–3554, doi: 10.1109/ICEEOT.2016.7755365.

[58] O. Permatasari, S. U. Masruroh, and Arini, "A prototype of child monitoring system using motion and authentication with raspberry pi," in *Proc. 4th Int. Conf. Cyber IT Service Manage.*, Bandung, Indonesia, Apr. 2016, pp. 1–6, doi: 10.1109/citsm.2016.7577516.

[59] A. Helen, M. F. Fathila, R. Rijwana, and V. K. G. Kalaiselvi, "A smart watch for women security based on IoT concept 'watch me,'" in *Proc. 2nd Int. Conf. Comput. Commun. Technol. (ICCCT)*, Feb. 2017, pp. 190–194, doi: 10.1109/ICCCT2.2017.7972266.

[60] M. Kavitha and V. Sivachidambaranathan, "Women self protecting system using Internet of Things," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Madurai, India, Dec. 2018, pp. 1–4, doi: 10.1109/iccic.2018.8782412.

[61] T. Khandelwal, M. Khandelwal, and P. S. Pandey, "Women safety device designed using IoT and machine learning," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, China, Oct. 2018, pp. 1204–1210, doi: 10.1109/smartworld.2018.00210.

[62] S. P. Raflesia, Firdaus, and D. Lestarini, "An integrated child safety using geo-fencing information on mobile devices," in *Proc. Int. Conf. Electr. Eng. Comput. Sci. (ICECOS)*, Pangkal, Pinang, Oct. 2018, pp. 379–384, doi: 10.1109/icecos.2018.8605200.

[63] N. R. Sogi, P. Chatterjee, U. Nethra, and V. Suma, "SMARISA: A raspberry pi based smart ring for women safety using IoT," in *Proc. Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Coimbatore, India, Jul. 2018, pp. 451–454, doi: 10.1109/icirca.2018.8597424.

[64] W. Akram, M. Jain, and C. S. Hemalatha, "Design of a smart safety device for women using IoT," *Procedia Comput. Sci.*, vol. 165, pp. 656–662, 2019, doi: 10.1016/j.procs.2020.01.060.

[65] R. Paknikar, S. Shah, and P. Gharpure, "Wireless IoT based solution for women safety in rural areas," in *Proc. Int. Conf. Commun. Electron. Syst. (ICCES)*, Coimbatore, India, Jul. 2019, pp. 232–237, doi: 10.1109/icces45898.2019.9002392.

[66] V. Sharma, Y. Tomar, and D. Vydeki, "Smart shoe for women safety," in *Proc. IEEE 10th Int. Conf. Awareness Sci. Technol. (iCAST)*, Oct. 2019, pp. 1–4, doi: 10.1109/icawst.2019.8923204.

[67] T. Sen, S. Singh, and V. N. Kumar, "ProTecht–implementation of an IoT based 3–way women safety device," in *Proc. 3rd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Coimbatore, India, Jun. 2019, pp. 1377–1384, doi: 10.1109/ICECA.2019.8821913.

[68] M. R. Tejonidhi, K. S. Chaithra, M. K. Dayana, and H. Nagamma, "IoT based smart security gadget for women's safety," in *Proc. 1st Int. Conf. Adv. Inf. Technol. (ICAIT)*, Chikmagalur, India, Jul. 2019, pp. 348–352, doi: 10.1109/ICAIT47043.2019.8987242.

[69] K. Thamaraiselvi, S. Rinesh, L. Ramaparvathy, and K. V, "Internet of Things (IOT) based smart band to ensure the security for women," in *Proc. Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Tirunelveli, India, Nov. 2019, pp. 1093–1096, doi: 10.1109/icssit46314.2019.8987928.

[70] M. S. Uddin, "Development of wearable emergency response system for women," in *Proc. IEEE 6th Int. Conf. Eng. Technol. Appl. Sci. (ICETAS)*, Kuala Lumpur, Malaysia, Dec. 2019, pp. 1–6, doi: 10.1109/icetas48360.2019.9117562.

[71] V. Hyndavi, N. S. Nikhita, and S. Rakesh, "Smart wearable device for women safety using IoT," in *Proc. 5th Int. Conf. Commun. Electron. Syst. (ICCES)*, Coimbatore, India, Jun. 2020, pp. 459–463, doi: 10.1109/icces48766.2020.9138047.

[72] A. Z. M. Tahmidul Kabir, A. M. Mizan, and T. Tasneem, "Safety solution for women using smart band and CWS app," in *Proc. 17th Int. Conf. Electr. Eng./Electron., Comput., Telecommun. Inf. Technol. (ECTI-CON)*, Phuket, Thailand, Jun. 2020, pp. 566–569, doi: 10.1109/ecti-con49241.2020.9158134.
[73] B. S. S. Tejesh, Y. Mohan, C. A. Kumar, T. P. Paul, R. S. Rishitha, and B. P. Durga, "A smart women protection system using Internet of Things and open source technology," in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (ic-ETITE)*, Vellore, India, Feb. 2020, pp. 1–4, doi: 10.1109/ic-etite47903.2020.455.
[74] J. S. Silva, R. Saldanha, V. Pereira, D. Raposo, F. Boavida, A. Rodrigues, and M. Abreu, "WeDoCare: A system for vulnerable social groups," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Las Vegas, Nevada, Dec. 2019, pp. 5332–5336, doi: 10.1109/csci49370.2019.00201.
[75] N. Vannini, S. Enz, M. Sapouna, D. Wolke, S. Watson, S. Woods, K. Dautenhahn, L. Hall, A. Paiva, E. Andre, R. Aylett, and W. Schneider, "'FearNot!': A computer-based anti-bullying-programme designed to foster peer intervention," *Eur. J. Psychol. Educ.*, vol. 26, pp. 21–44, Feb. 2011, doi: 10.1007/s10212-010-0035-4.
[76] C. Raminhos, A. P. Cláudio, M. B. Carmo, A. Gaspar, S. Carvalhosa, and M. D. J. Candeias, "A serious game-based solution to prevent bullying," *Int. J. Pervas. Comput. Commun.*, vol. 12, no. 2, pp. 194–215, Jun. 2016, doi: 10.1108/ijpcc-04-2016-0022.
[77] D. Smith, M. Ma, A. Jones, and E. Unver, "*None in three*: The design and development of a low-cost violence prevention game for the Caribbean region," in *Proc. Joint Int. Conf. Serious Games*. Cham, Switzerland: Springer, Nov. 2017, pp. 259–270, doi: 10.1007/978-3-319-70111-0_24.
[78] R. Mason and L. Turner, "Serious gaming: A tool to educate health care providers about domestic violence," *Health Care for Women Int.*, vol. 39, no. 8, pp. 859–871, May 2018, doi: 10.1080/07399332.2018.1464572.
[79] J. Pearson, S. Wu, H. Royston, H. Smailes, N. Robinson, A. Cowell, and A. Jones, "Designing a serious game to raise awareness of intimate partner violence among adolescents in the UK: The use of 'good games' principles for effective behavioural change," in *Interactivity, Game Creation, Design, Learning, and Innovation* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 328, A. Brooks and E. Brooks, Eds. Cham, Switzerland: Springer, 2020, doi: 10.1007/978-3-030-53294-9_33.
[80] S. Kriglstein, F. Hengstberger, F. Fribert, K. Stiehl, B. Schrank, A. Pfeiffer, T. Wernbacher, and G. Wallner, "Be a buddy not a bully–two educational games to help prevent bullying in schools," in *Proc. Extended Abstr. Annu. Symp. Comput.-Hum. Interact. Play*, New York, NY, USA, Nov. 2020, pp. 287–291, doi: 10.1145/3383668.3419914.
[81] UN Woman, A United Nations Entity. (2021). *Focusing on Prevention: Ending Violence Against Women*. Accessed: Feb. 2021. [Online]. Available: https://www.unwomen.org/en/what-we-do/ending-violence-against-women/prevention
[82] C. of Europe. *Sexism: See it. Name it. Stop it*. Accessed: Mar. 18, 2021. [Online]. Available: https://www.coe.int/en/web/human-rights-channel/stop-sexism
[83] NSPCC. *What Parents Need to Know About Sexual Grooming*. Accessed: Mar. 2021. [Online]. Available: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/#what-is
[84] V. Egan, J. Hoskinson, and D. Shewan, "Perverted justice: A content analysis of the language used by offenders detected attempting to solicit children for sex," *Antisocial Behav.: Causes, Correlations Treatments*, vol. 20, no. 3, pp. 273–297, 2011.
[85] U.S. Department of Health and Human Services. *What is Child Abuse or Neglect? What is the Definition of Child Abuse and Neglect?* Accessed: Mar. 2021. https://www.hhs.gov/answers/programs-for-families-and-children/what-is-child-abuse/index.html
[86] F. Ke, "Computer-game-based tutoring of mathematics," *Comput. Educ.*, vol. 60, no. 1, pp. 448–457, Jan. 2013, doi: 10.1016/j.compedu.2012.08.012.
[87] B. Bonnechere and S. Van Sint Jan, "Rehabilitation," in *DHM and Posturography*, S. Cataglini and G. Paul, Eds. New York, NY, USA: Academic, 2019, Ch. 39, pp. 541–547.
[88] G. Alinier, C. Tuffnell, and B. Dogan, "Simulation on a low budget," in *Clinical Simulation*, G. Chiniara, Ed., 2nd ed. New York, NY, USA: Academic, 2019, Ch. 45, pp. 667–689.
[89] Alexa. *The Top 500 Sites on the Web*. Accessed: Mar. 30, 2021. [Online]. Available: https://www.alexa.com/topsites. https://www.alexa.com/topsites
[90] S. Steinsbekk, L. Wichstrøm, F. Stenseng, J. Nesi, B. W. Hygen, and V. Skalická, "The impact of social media use on appearance self-esteem from childhood to adolescence–A 3-wave community study," *Comput. Hum. Behav.*, vol. 114, Jan. 2021, Art. no. 106528, doi: 10.1016/j.chb.2020.106528.

DALIA ANDREA RODRÍGUEZ received the B.Sc. degree in mathematics, with a focus on computing, from the University of California at Los Angeles (UCLA), Los Angeles, in 2019. She is currently pursuing the M.Sc. degree in computer science with the Tecnológico Nacional de México, Instituto Tecnológico de Mexicali (TecNM/ITM) campus. Her research interests include artificial intelligence (AI), the Internet of Things (IoT), and e-health. Specifically, she analyzes how AI and the IoT can be used to address social issues, such as gender inequality and child abuse.

ARNOLDO DÍAZ-RAMÍREZ (Member, IEEE) received the bachelor's degree in computer sciences from CETYS Universidad, Mexicali, Mexico, in 1988, and the Ph.D. degree in computer sciences from the Universitat Politecnica de Valencia, Spain, in 2006, with a focus on scheduling of real-time systems. Since 1992, he has been with the Tecnológico Nacional de México, Instituto Tecnologico de Mexicali (TecNM/ITM) campus, where he works as a Research Professor. He is currently the coordinator of the Industrial Informatics Research Group, TecNM/ITM. His research interests include real-time systems, cyber-physical systems, ubiquitous computing, ambient assisted living, e-health, artificial intelligence, and wireless sensor networks.

JESÚS ELÍAS MIRANDA-VEGA was born in 1984. He received the B.S. degree in electrical and electronic engineering from ITLM, in 2007, the master's degree in electronic engineering from TecNM/IT, Mexicali, in 2014, and the Ph.D. degree in science and applied physics from the Autonomous University of Baja California, in December 2019, and receiving honorable mention. He has written three book chapters and 11 journals and proceedings conference papers. His research interests include machine vision, data signal processing, the theory and optoelectronics devices, and their applications.

LEONARDO TRUJILLO received the Ph.D. degree in computer science from the CICESE Research Center, Ensenada, Mexico. He is currently a Professor at the Tecnológico Nacional de México/IT Tijuana, Tijuana, Mexico. His work focuses on genetic programming and machine learning. He has been the PI of several national and international research grants and receiving several distinctions from the Mexican Science Council (CONACYT). His work has been published in over 60 journal articles, 60 conference papers, and 18 book chapters, and he has edited four books. He is on the Editorial May/June 2020 Board of the journals: *GPEM* (Springer) and *MCA* (MDPI), regularly serves as a reviewer for highly respected journals in AI, EC, and ML. He is the Series Co-Chair of the NEO Workshop, and has organized and been the track chair or served as a PC Member of various prestigious conferences, including GECCO, EuroGP, PPSN, CEC, GPTP, CVPR, and ECCV.

PEDRO MEJÍA-ALVAREZ received the B.S. degree in computer systems from ITESM, Santiago de Querétaro, Mexico, in 1985, and the Ph.D. degree in informatics from the Polytechnic University of Madrid, Spain, in 1995. He has been a Professor with the Computer Science Department, Cinvestav-IPN, since 1997. His research interests include mobile computing, real-time systems scheduling, adaptive fault tolerance, and software engineering.