IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

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]Tecnológico Nacional de Méxco/IT Mexicali, Department of Computer Systems, Mexicali, B.C., México, 21376 (e-mail: {m20490496, adiaz, elias.miranda}@itmexicali.edu.mx)
[2]Department of Electrics and Electronics, Tecnológico Nacional de México/IT Tijuana, Tijuana, B.C., México, 2414 (e-mail: leonardo.trujillo@tectijuana.edu.mx)
[3]CINVESTAV-GUADALAJARA, Zapopan, Jal, México, 45017, (e-mail: pmalvarez@cs.cinvestav.mx)

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

ABSTRACT Violence against women and children are public health issues of pandemic proportions. It is estimated that one in every three women worldwide have experienced physical, emotional or sexual violence. Similarly, each year one 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 also now vulnerable to other types of violence such as cyber-bullying and online sexual or emotional harassment. To help alleviate these social problem, the use of computer sciences 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. 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 in four application domains: online detection, offline detection, safety and education. Additionally, 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 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 certain groups of people, such as women and children, are at particular risk of becoming victims. With about one in every three women worldwide having experienced physical or sexual intimate partner violence (IPV) or non-partner sexual violence during their lifetime [1], as well as estimates indicating that one out of two children worldwide suffer from some form of violence each year [2], it is clear that violence against women (VAW) and violence against children (VAC) are major public health concerns in need of any and all forms of intervention.

IPV is one of the most common forms of VAW [3], with 30% of women who have been in a relationship reporting that they have experienced physical or IPV during their lifetime, and 38% of feminicides happening at the hands of an intimate partner or ex-partner [1]. Men are the most common perpetrators of IPV, and some factors that lead to IPV against women include socially accepted norms, such as male dominance, and the belief that men have a right to beat their female partner [3]. VAW is in part fostered by gender inequality and discrimination. These issues need to be addressed as well in order 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]. Also, 49.3% do not report because they think that the violence that they suffered was not an important issue [5], highlighting that women have been taught that it is acceptable to commit violence against them. Lawmakers appear to support this belief as well, given that one in four countries have no laws protecting women from domestic violence (DV) [4]. However, VAW may lead to serious 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 serious. Therefore, it is necessary to teach women and society at large that any and 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. It is estimated that 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 such as bullying, which affects one in three students between the ages of eleven and fifteen each month, and dating violence, experienced by at least 20% adolescents aged between thirteen and eighteen [3]. Given the correlations between VAW and VAC, it is important to address both VAW and VAC at the same time.

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 CSA. Given that the majority of cases of VAW are not reported, and that 60% of cases of sexual VAC have a five-year delay in disclosure [7], technological solutions may be a valuable tool to assist practitioners in identifying victims of abuse. CS can also be used to detect and prevent pedophilia, by monitoring or controlling the seemingly uncontrollable influx of Internet content that is violent or has a potential to spread violence such as media files depicting CSA [8], or social media posts that are discriminatory or hateful towards women and girls [9], a task which may be time-consuming or emotionally-taxing for those in charge of removing said content.

CS is also being used with the purpose of providing education on the subject of VAW and VAC. CS can provide tools to educate healthcare workers on how to better identify victims of abuse [10]. Therefore, victims of abuse who were scared to speak up about their abuse, or reluctant for other reasons 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 that is respectful and empathetic towards women and children, and hopefully less likely to engage in violence.

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.

Based on the potential of CS and related technologies to address VAW and VAC as described in the previous paragraphs, this paper aims to describe the current state-of-the-art of contributions in these fields, as well as 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 a CS and engineering perspective. This paper aims to fill in this gap in the literature, and guide researchers who are interested in addressing VAW and VAC from a CS and engineering point of view. In order to provide a thorough and unbiased review, a systematic literature review protocol was pre-defined using [14] as a guideline.

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

II. PLANNING

The protocol for conducting this systematic literature review is introduced in this section. 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 are being implemented to address the problems of VAW and VAC?
   Between the months of September to December 2020, a systematic Internet search using search engines and academic digital libraries was performed, in order 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 of scientific and technological topics, including those closely related to the objective of this paper.

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

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, GBV, women hatred, women hate speech, child abuse, child sexual abuse, CSA, CPA, 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

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. Search strings were constructed by combining at least one term from Group 1 and at least one term from Group 2, using Boolean ANDs and ORs.

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.

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.

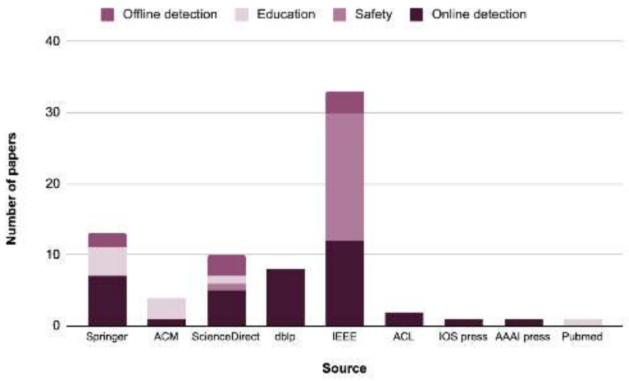

FIGURE 1. Distribution of papers selected by source

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.

If duplicate publications were found across platforms, only one was used. Afterwards, the studies were evaluated for quality using the quality assessment from the previous section. If discrepancies on eligibility persisted at this stage, they were resolved by discussion amongst the authors, 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 selected papers that were used in this study.

As it can be observed in Fig. 1, the majority of the selected studies came from IEEE (45.2%). This is followed by Springer (17.8%), ScienceDirect (13.7%), Dblp (11%), 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. It should be noted that the majority of studies were published between 2018 and 2020. This indicates a growing interest from the CS and engineering research community to tackle the problems of VAW and VAC in recent years.

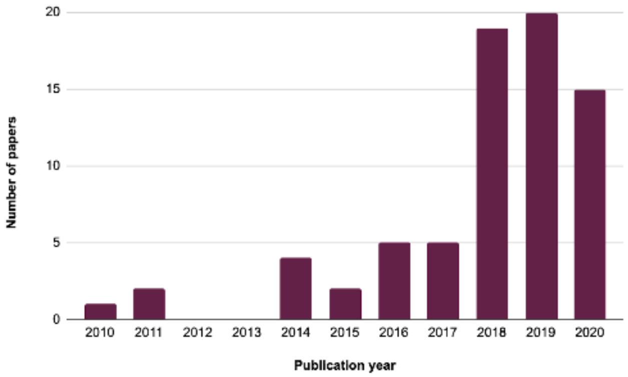

FIGURE 2. Distribution of selected studies by publication year

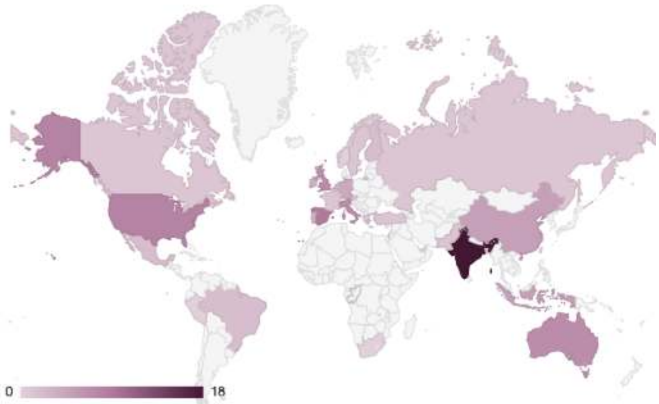

FIGURE 3. Distribution of selected papers by country

In Fig. 3, the selected studies distributed by the country of origin of the contributors are shown. It can be observed that at least one study from each continent has been selected. The majority of the studies came from India, with 18 total contributions. This is followed by Spain with 9 contributions.

IV. DATA SYNTHESIS

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

1) 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 current and future relevance of the application domain, and not in 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%).

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]

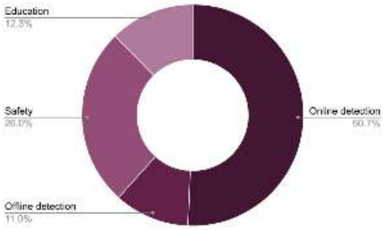

FIGURE 4. Distribution of selected studies by category

2) 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 is often time-consuming [42] or emotionally-taxing [46] when done manually.

In order to detect and eliminate VAW and VAC, it is necessary to address explicit cases of violence, but also 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 important to address their presence in environments with inadequate protection, like the Internet, which make children vulnerable to grooming, bullying, or other forms of abuse [2]. In this context, the studies belonging to this category address both explicit forms of VAW and VAC present on the Internet, as well as their risk factors and categorized as shown in Fig. 5 as: misogyny (51.4%), sexism (10.8%), child grooming (8.1%), peer violence (2.7%), reports of abuse (13.5%), and child sexual abuse (CSA) media (13.5%). Some representative examples of the online detection category are summarized below.

Misogyny: Studies within this subcategory propose methods for the automatic detection of written Internet content

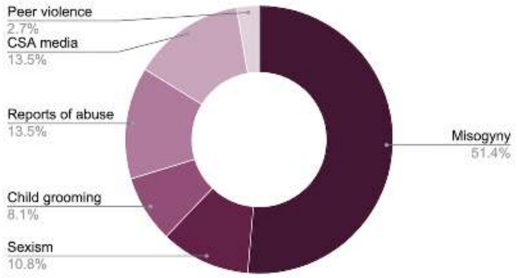

FIGURE 5. Online detection studies split into subcategories

that is misogynistic in nature, where misogyny is defined as hate speech that is targeted towards women [16]. [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. In particular, 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 classify the targets of the misogynistic tweets as either geared towards 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 abusive activity by conducting a cross-domain classification experiment. For the binary classification task, namely 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 in the English-language model but used a SVM classifier with 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%.

Sexism: Studies within the sexism subcategory aim to automatically detect Internet content that is sexist towards women, where sexism is defined as any expression based on the idea that certain people are inferior due to their sex or gender [82]. [28] built ML models to 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, with SVM achieving the highest precision at 76.2%. For the identification of textual sexist jokes, the authors achieved the highest precision of 75.2% using a k-nearest neighbors (K-NN) with bag of words (BoW) approach. For the bimodal approach, the authors combined visual and textual features, achieving a 75.9% precision through the use of a SVM classifier.

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. [33] used deep learning (DL) to automatically identify Facebook posts of people who are in need immediate assistance due to DV. The authors extracted Facebook posts from DV Facebook pages and experimented with various DL classifiers, as well as word embeddings, with the goal of creating a multi-class identification model that identifies people who are in need of 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 [21]. The authors built a DL model to explore 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.

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 in order to detect cases of child grooming in online chat rooms. For instance, in [43], the authors use an SVM classifier and experiment with various combinations of 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], to detect online child sex offenders in chat logs. 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 grooming characteristics, 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%.

CSA media: Studies that fall within this subcategory use ML models to facilitate the detection of child pornography on the Internet. The study [8] builds ML models to automatically detect CSA media on peer-to-peer (P2P) networks. Specifically, the authors built three models to detect CSA media from its filename, image content, or video content respectively. For filename identification, the authors implemented a model that uses an SVM classifier with semantic features, such as pedophile keywords, explicit keywords, and words referring to children or family, as well as character n-grams, 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 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 dataset that was created in collaboration with the Brazilian Federal Police, which includes real child pornography.

Peer violence: The studies in this category detect cases of peer violence between students. The single study within this subcategory, [49] experimented with various ML models, in order to detect bullying in Greek virtual learning communities of K-12 students. The goal of this study is to facilitate the ability of teachers to intervene to online peer violence, given the difficulty of monitoring students in an online environment. The authors applied various preprocessing techniques and used n-grams as features, that were fed to multiple classifiers to detect aggressive behavior. Their best result in terms of recall was a DL classifier, which obtained 95.4% recall.

3) Offline Detection

Studies that are part of the offline detection category mainly use ML to detect potential victims of abuse or violence from data that is not generally collected from or 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 relevant professionals, that will facilitate the detection of possible cases 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 that otherwise go unreported. This ultimately, and most importantly, can lead to getting women and children in need the support and services necessary to prevent further violence from occurring.

Technological solutions that fall under this category can be further classified into the following offline detection subcategories, as shown in Fig. 6: peer violence (50.0%), child abuse (37.5%), and IPV (12.5%). Some representative examples of CS and engineering solutions that fall under the category of online detection are described below.

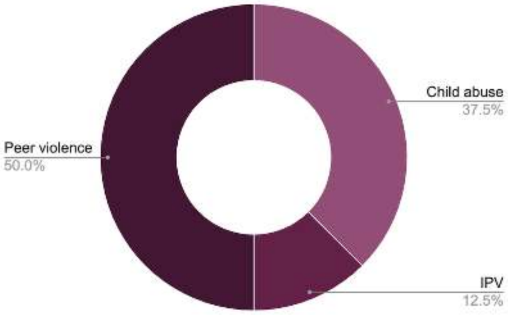

FIGURE 6. Offline detection studies split into subcategories

Peer violence: The majority of studies within this subcategory use ML. These studies are the initial stages of larger Internet of Things (IoT) school violence response systems where, upon detection of violence, the system will use communication technologies to contact school authorities so that these can intervene. Therefore, these studies do not focus on the whole violence response system, but only on the creation of a suitable peer violence detection model based on ML. [53] propose two models to automatically detect physical and verbal bullying in schools. In order to detect verbal bullying, sound data were obtained from sound recordings of students portraying emotions that may indicate bullying. Features from this data were extracted by using Mel Frequency Cepstral Coefficients (MFCC) and classified as bullying or non-bullying using the k-NN algorithm. The best performing model obtained 70.4% accuracy. For physical bullying detection, K-NN was also used as a classifier. In this case, acceleration and 3D gyros data were obtained from a movement sensor that was worn by students during a simulation of various violent and non-violent activities. The best model for 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 gestures, and used this knowledge to build a ML model that detects changes in these streams that are indicative of bullying activities. The model, which uses least square SVM (LSSVM) as its classifier, was tested on various real-life environments including an office, a dorm room, and a laboratory and obtained an average recall rate of 93.4%.

Child abuse: Studies within this subcategory propose AI methods to automatically detect potential cases of child abuse, where child abuse is defined as 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 a SVM model with a polynomial RBF which 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.

IPV: Studies within this subcategory aim to automatically detect potential victims of DV, specifically IPV which affects 35% of women [1]. The study [52] addresses physical acts of IPV by means of building a DL framework with class activation maps that automatically identifies facial injuries caused by IPV. The proposed model performs with an accuracy of 80%, outperforming all baseline models that it was tested against.

4) Safety

Studies within the 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 the ability of 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. It is estimated that 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, in such a way that victims can get the needed help or support as soon as possible. Studies within this category can be further subcategorized, as shown in Fig. 7, into mobile phone applications (10.5%), wearable or portable devices (84.2%), and non-portable devices (5.3%). It must be highlighted that some of the selected studies within this category can be placed in more than one subcategory. For instance, [57] proposed a system aimed to provide safety to women, comprised of a smart band and mobile phone application. Representative examples of each subcategory are summarized below.

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 is installed on a smartphone of a children and it uses a geo-fencing technique, GPS, and a gravity sensor to monitor the location of the children. If he or she exits the geo-fence established by parents or caregivers, the device will issue an alarm to pre-determined contacts via SMS or Wi-Fi with his or her location. The smartphone will also begin voice recording for evidence of maltreatment or abuse and will send these recordings via SMS. In an emergency situation, the child can also shake the smartphone in order to activate the alarm mechanism described above.

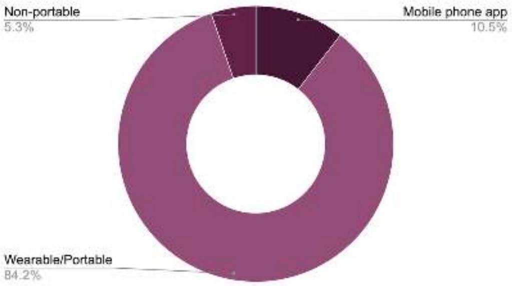

FIGURE 7. Safety studies split into subcategories

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

Wearable/Portable devices: Studies within this category propose wearable or portable devices that provide safety for women or children. The study [72] provides an IoT smart band along with a smartphone application that facilitates the ability of a woman to get assistance if she finds herself in a dangerous situation. The application, which 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 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. The emergency mechanism of this system can be activated 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 his or her predetermined contacts.

Using a different approach, in [61], the authors considered situations in which a woman is in danger but is unable to press a help button or utter emergency words. The authors propose a wearable IoT device that predicts whether or not a woman is in danger, based on 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 through a ZigBee mesh network if there is no Internet connection. In the cloud, a LR model will evaluate the data and determine if the user is in danger. In such case, the system will automatically dial emergency contacts.

[65] proposes a device aimed for safety of woman that caters to her needs when living in rural areas, or where Internet and cellular networks are unreliable. The safety solution, using the IoT paradigm, is in the form of a beacon device with a help button that the user can press if she feels threatened. The beacon device has a unique identifier and is connected using Bluetooth to a network of solar-powered street poles and central stations that have been installed for the purpose of this application. The street poles have pre-defined GPS coordinates and are also connected to the central stations through Bluetooth. If the user presses the help button, a distress message travels from the nearest street poles until it reaches a central station, where the help message is processed through a server so that the user can get help

Some wearable solutions aimed at women safety also include self-defense mechanisms. [64] proposes an IoT system consisting of a wearable device with a mobile application that uses a 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 shockwave generator. The purpose of the alarm is to get the attention of nearby people, but 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 [66], [67], and [69].

Non-portable devices: This subcategory is concerned with stationary or non-portable devices that help parents monitor their children in order to keep them safe from abuse. In [58], the authors propose a video surveillance system so that parents can 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. In order to verify that only those authorized to view the stream can access it, those authorized may only access with a private username and password.

5) Education

Studies that belong in this category aim to train healthcare professionals and educate children about VAW and VAC. Most of the proposals rely on the use of digital serious games (SG). As mentioned previously, more than a third of the women intentionally killed in 2017 were killed by an intimate partner [81], and it has been shown that many women in the USA sought health services during the year prior to being murdered by an intimate partner [3]. Moreover, healthcare students have expressed feelings stressed about not having enough training on how to detect victims of child abuse, as well as not knowing how to respond to the cases they do detect them [10]. There is a necessity to provide appropriate training for healthcare professionals so that they can both detect and know the best approach towards helping women and children who suffer from violence. SG have been deemed as beneficial in teaching STEM subjects such as mathematics [86] and have been used for health care purposes to beneficial 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]. Therefore, SG could help provide the education and training that healthcare workers need at a lower cost than traditional instruction [88]. Similarly, classroom settings may benefit from the use of SG. 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]. As it can be seen in Fig. 8, 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 to highlight that the study [77] can belong in two categories because it addresses the intersection between IPV and child abuse.

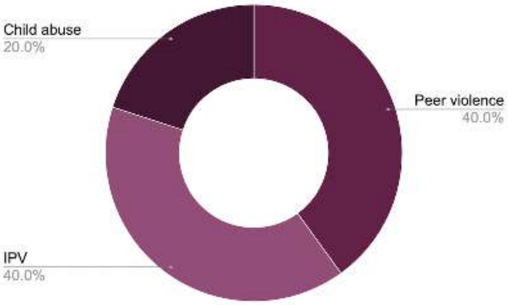

FIGURE 8. Education studies split into subcategories

Peer violence: Studies in the subcategory 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. Stop the Mob! allows students to observe how their response to bullying affect 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 teach students that bullying is a serious topic and actions that students make in regard to it, 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. Both games are evaluated in a classroom with students between the ages of 12 and 15. The authors provided the students with post-game questionnaires and found that 23 out of 26 students prefer the fantasy game because the aspect of letting characters walk around freely made the game more adventurous and entertaining.

IPV: Studies grouped in this subcategory proposed SG that aimed to facilitate education regarding IPV. [12] developed a PC game titled Green Acres High with the goal of educating adolescents on the topic of dating violence. Through a series of simulation-style lessons mediated in a classroom setting, Green Acres High aims to teach teenage students about healthy and abusive relationships. Authors tested the game on real students to both positive and negative feedback. Students said that its simulation style 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 of the game.

In order to cater to the needs of healthcare professionals, [78] proposes 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.

Child abuse: Studies placed in this subcategory use SG to address child abuse. In [10] the Computer Simulated Interactive Child Abuse Screening Tool (CSI-CAST) was introduced, 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 which may be relevant to child physical abuse. The game records the questions asked by different players and uses ML to identify specific areas that the group needs further training on, in regard to detecting and responding to child physical abuse.

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 people of ages ten through eighteen in the Caribbean about DV. In the game, the players roleplay as different characters including Diana, a victim of IPV, and her son, Jesse. Playing as different characters allows players to observe how being a victim of IPV affects Diana but also Jesse. For example, players are able to observe Diana's conflicting feelings towards her husband, the perpetrator, but they also observe how Jesse's grades and behavior at school deteriorate due to the violence he witnesses at home. By witnessing the violence inflicted upon his mother, Jesse becomes a victim of the abuse as well. Therefore, players can observe how VAW and VAC intersect.

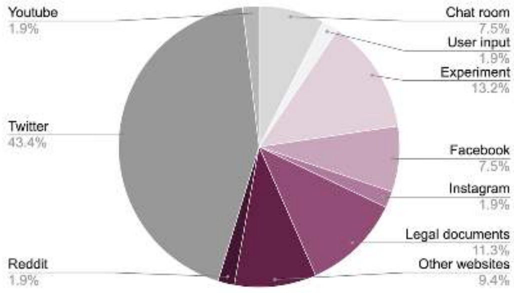

FIGURE 9. Sources of data collected for ML models

6) Answer to the second research question

Despite that several computer science technologies were described previously to answer the first research question, a more detailed description of the CS approaches and technologies used by the selected studies is provided. To answer the second research question, the contributions reviewed used in this document were categorized as: AI, IoT, and SG.

AI: About 66% of the studies applied AI techniques to their solutions. Specifically, these studies used ML algorithms to address VAW and VAC. ML was used in every study belonging to the online and offline detection categories. ML was also used in 11% of the studies in the safety category, and 11% of the studies in the education category. The process of creating a ML model for classification can be split into the following stages: data collection, features engineering, classification, and performance evaluation.

- Data collection: In Fig. 9, it can be observed that, out of all the studies that proposed ML models, 54.7% used data originating from social media (Twitter, Facebook, Instagram, and Reddit). This indicates that social media, in particular Twitter, is considered a valuable source of information in regard to 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 were collected from experiments involving signals or voice recordings, 11.3% of data were 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 [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], or experiments [55].
- Features engineering: As seen in Fig. 11, different data

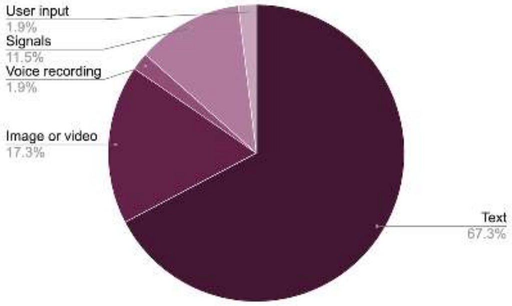

FIGURE 10. Format of data collected for ML models

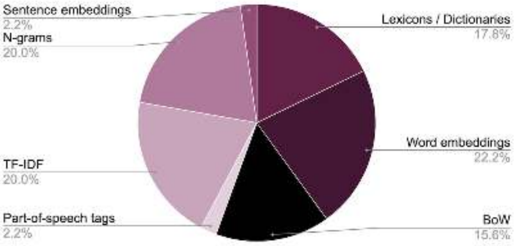

FIGURE 11. Text features engineering techniques (best model per study).

formats were collected to be used by the ML models. 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 the least used methods of feature representation for text processing ML tasks at only 2.3% use each.
- Image or video (visual) features engineering: Due to the widespread of images and videos on the Internet and social media, 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%). In Fig. 13, it can be observed that there are not many CSI-based violent activity recognition studies addressing VAW and VAC, therefore this is an area that can be explored further.

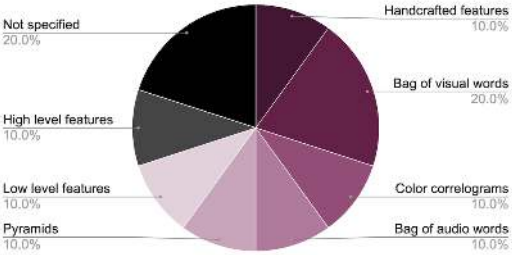

FIGURE 12. Visual features engineering (best model per study).

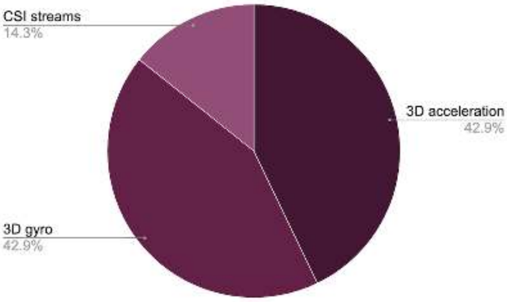

FIGURE 13. Signals features engineering (best model per study)

- 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 [10]'s game, 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. Recursive feature elimination method with a penalized logistic regression estimator is utilized to extract the features that most affect players' decision to classify the child is a victim or not.

- ML algorithms as classifiers: Table 5 lists the best classifying approach per ML classification study. SVM was the most widely used ML classifier overall in the area of VAW and VAC. It can be observed that studies perform differently even though they use the same classifier. It can be concluded that the choice of dataset and features engineering per model affects the overall performance of the model.
  - Performance metric: Accuracy, precision, recall and F1-score were widely used performance metrics. As it can be observed in Table 5, accuracy was the most widely used performance metric. The definitions of accuracy, precision, recall, and F1-score are located below.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103459, IEEE Access

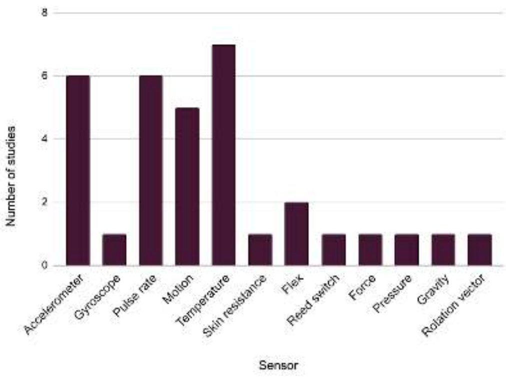

FIGURE 14. Distribution of sensors used in IoT applications

- ∗ **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 x ((p x r) / (p + r)), where p is precision, and r stands for recall.

The ML models and their performance in regard to VAW and VAC, are shown in Table 5.

IoT: 26% of the selected studies, namely every study within the safety category, addressed the issue of VAW and VAC by means of violence response systems based on IoT. Technologies employed by IoT solutions were organized in 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 are mainly aimed 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. In fact, sensors were also incorporated into 25% of the offline detection studies as well. However, given that studies in the offline detection category do not focus on the creation of an entire violence response system, but only on the development of a ML learning model, the use of sensors in these cases is not considered in 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.

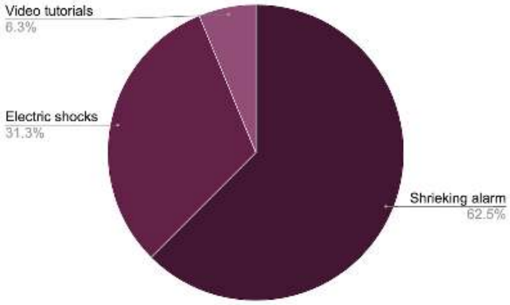

FIGURE 15. Distribution of self-defense tools in IoT applications

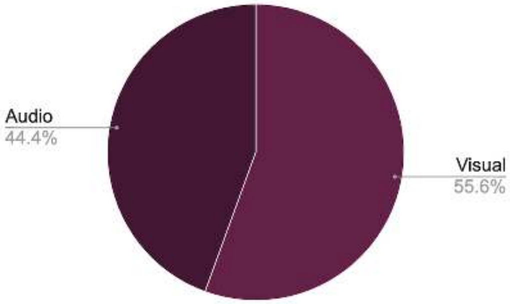

FIGURE 16. Evidence collection mechanism distribution in IoT applications

- 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 almost as common as audio recording techniques. This highlights that 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). This is followed by 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%). It must be noted that wireless communication technologies were vastly preferred over wired ones.
- Location-monitoring: Knowing the location of the user is a key element in some proposals. As it can be seen in Fig. 18, location-monitoring technology was widely used for the purpose of emergency situations, with 89% of studies in the safety category proposing the use of GPS for location-sharing.
- 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 for

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

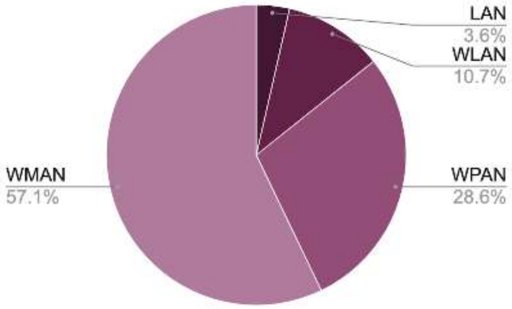

FIGURE 17. Distribution of communication technologies in IoT applications

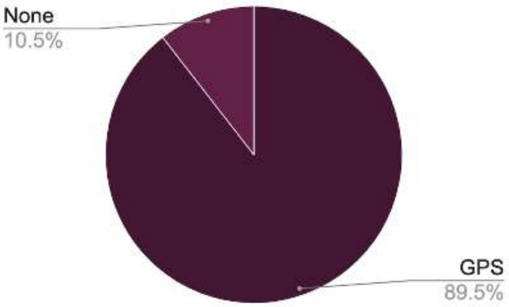

FIGURE 18. Location monitoring technologies employed by IoT applications

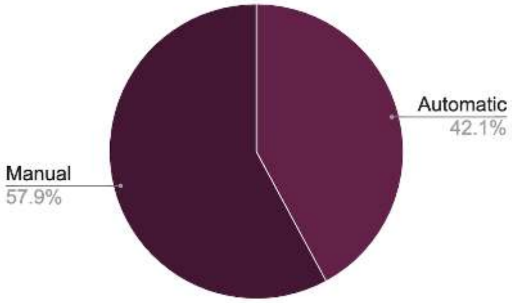

FIGURE 19. System activation technique for IoT applications

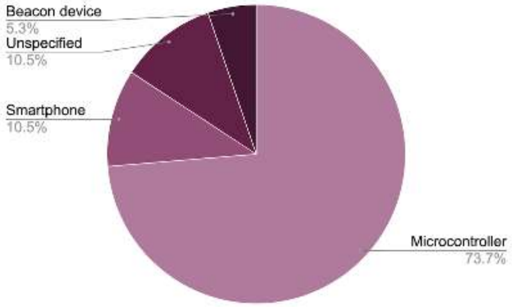

FIGURE 20. Distribution of devices for IoT applications

activation purposes [74]. On the other hand, 42.1% of safety solutions had an automatic 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, such as 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.

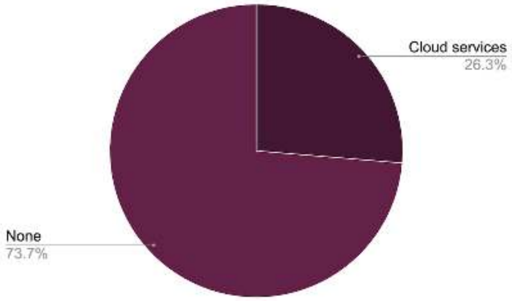

FIGURE 21. Cloud services usage in IoT applications

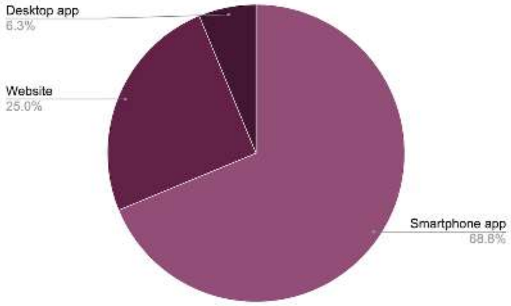

FIGURE 22. Visualization techniques used by IoT applications

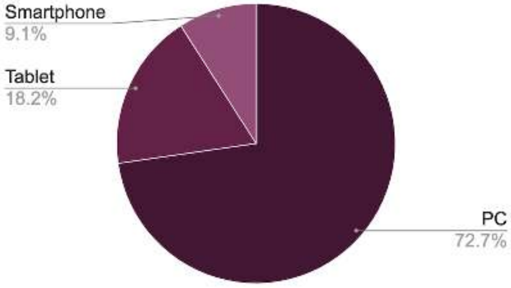

FIGURE 23. Gaming platforms utilized in SG

- 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, and 12% 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: As it can be observed in Fig. 23, the PC was the platform of choice in 72.7% of SG applications. This is followed by tablets (18.2%) and smartphones (9.1%). Given the low percentage of SG applications involving smartphones, there is a huge potential to expand SG applications in this area.
- 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: It can be observed in Fig. 26 that only 11.1% of studies involving SG, a total of one study used AI. It would be interesting to incorporate AI into more SG

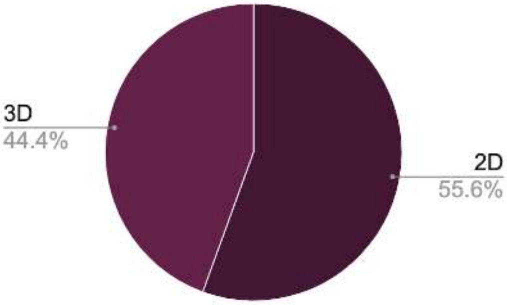

FIGURE 24. Graphics used in SG

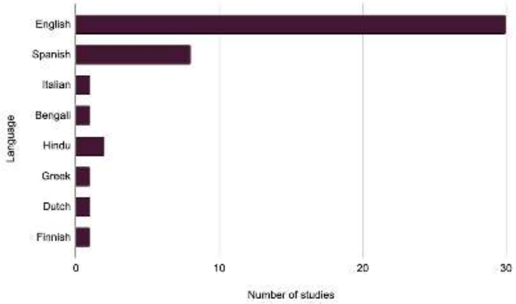

FIGURE 27. Language distribution in ML models that performed text analysis

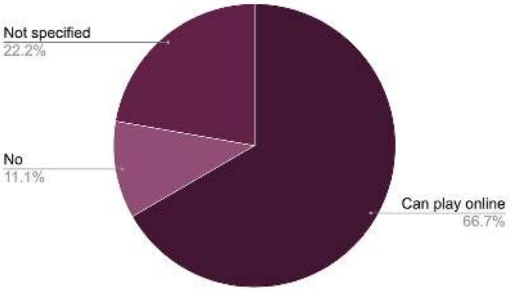

FIGURE 25. Proportion of SG that could be played online

applications that address VAW and VAC and explore how players may benefit from the use of AI in SG.

V. ANALYSIS

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

Explore more social media: Studies dealing with the detection of abusive phenomena on the Internet would benefit from exploring other social media platforms. It was observed that 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 used [89]. There were no studies that explored child grooming or pedophilia detection on social media, so it would be an interesting area of research given that 94% of adolescent people living in developed nations use a social media platform [90].

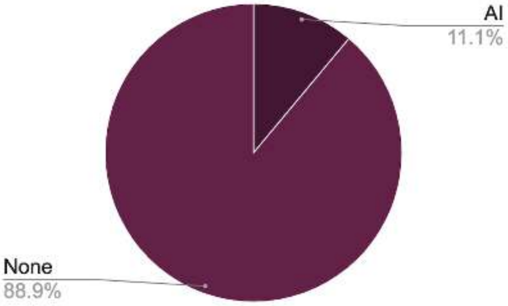

FIGURE 26. Proportion of SG that used AI technology

More language diversity for ML tasks: Studies dealing with detection of abusive phenomena from textual data used data primarily in the English language. Given that 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 chatrooms were in a language other than English. Therefore, it is important to explore these areas. The full distribution of languages in ML models that performed text analysis can be seen in Fig. 27.

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 situation due to not having enough time, being in the middle of an assault, or being paralyzed with fear. Therefore, there should be greater focus placed upon the incorporation of IoT and AI technologies that may automatize the activation of safety devices.

More thoughtful design for wearable technologies: Some wearable safety devices were very large or required to be held at all times. This is not discreet nor is it practical for daily use. Therefore, there is a necessity to make wearable devices that are ubiquitous or non-invasive and will not inconvenience the user.

Security: Some anti-abuse solutions can be used to facilitate abuse. Every safety device used either location-monitoring technology or visual monitoring technology. In particular, devices that were made 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 be used to facilitate abuse, since perpetrators can use this type of system to monitor their victims at all times. Therefore, 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.

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 directly depends on whether anyone decides to act upon the victim's call for help as well as how long it takes for that person to get to the scene of the crime. 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 actually takes for victims to get help. It is important to incorporate this type of information in safety device studies in order to set realistic expectations of how much these devices can actually do to help potential victims and to diminish any false sense of security that may arise from using these devices.

Education for boys: Acts of IPV and sexual violence are more likely to be committed by men upon women [1]. There were no educational SG addressing issues of VAW that were aimed directly at boys or men. In order to prevent VAW, it is important to change beliefs and norms that condone or lead to its acceptance [1]. Therefore, it would be beneficial to have educational SG that focus on ideologies and beliefs they make men perpetrators of VAW.

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, in offline detection studies, offline detection tools were mostly meant to facilitate professionals' detection of VAW or VAC, as opposed to replacing professionals who do these jobs. Therefore, it is important to remember that although technology can have a positive impact in preventing violence, it should be seen as more of an auxiliary tool than a solution to VAW and VAC.

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 volent behavior due to bias. AI fairness is a recent research area that should be incorporated in AI proposals that address VAW and VAC.

VI. CONCLUSION

This paper presented a systematic literature review of CS and related technologies to the fight against 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 in the world, and India contributed the most studies out of every country. The study revealed that most of the research by CS and related fields focuses on the detection of abusive activity against women and children in online settings (50.7%). This is followed by safety solutions (26.0%), education (12.3%), and offline detection (11.0%). Selected studies use CS and related technologies to address the urgent need to both prevent and respond to VAW and VAC by proposing applications based on AI, IoT, and SG. ML, an AI subset of techniques, among others. Studies also propose IoT-based violence response system that make 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 with the purpose of facilitating women and children's ability to get the assistance they need during a violent event. Lastly, digital simulation-style SG were created to facilitate education about VAW and VAC to age groups ranging from elementary school children to professionals in the healthcare sector. 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 selection of primary studies that share a glimpse into what the research community within the field of CS and engineering is doing in order to contribute to the fight against VAW and VAC. These solutions highlight that 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] T. V. n. Alliance. (2021) Definition and typology of violence. retrieved from https://www.who.int/violenceprevention/approach/definition/en/. [Online]. Available: Retrievedfromhttps://www.who.int/violenceprevention/approach/definition/en/

[2] W. H. Organization, *Global status report on preventing violence against children*. Geneva: World Health Organization, 2020.

[3] WHO and P. A. H. O. (PAHO). (2012) Feminicide. understanding and addressing violence against women.

[4] UN and P. Mlambo-Ngcuka. (2021) Violence against women and girls: the shadow pandemic.

[5] I. N. de Estadística y Geografía (INEGI), *Encuesta Nacional sobre la Dinámica de las Relaciones en los Hogares (ENDIREH). Mexico*. Instituto Nacional de Estadística y Geografía, 2016.

[6] W. H. Organization. (2016) Understanding and addressing violence against women.

[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 and Neglect*, vol. 109, p. 2020, November 2020.

[8] C. Peersman, C. Schulze, A. Rashid, M. Brennan, and C. Fischer, "icop: Automatically identifying new child abuse media in p2p networks," in *Proceedings of the IEEE Security and Privacy Workshops*, San Jose, CA, May 2014, pp. 124–131.

[9] E. W. Pamungkas, V. Basile, and V. Patti, "Misogyny detection in twitter: a multilingual and cross-domain study," *Information Processing and Management*, vol. 57, p. 6, Nov 2020.

[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 *Proceedings of the 14th International Conference on the Foundations of Digital Games*, New York, USA, Aug 2019, pp. 1–7.

[11] C. Walsh and A. Schmoelz, "Stop the mob! pre-service teachers designing a serious game to challenge bullying," in *Games and Learning Alliance. GALA 2015. Lecture Notes in Computer Science*, I. A. D. Gloria and R. Veltkamp, Eds. Rome, Italy: Springer, Cham, June 2016, pp. 431–440.

[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," *Pshychosocial Intervention*, vol. 23, no. 1, pp. 43–55, April 2014.

[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 *Proceedings of the IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT)*. Bangalore, India, May 2016, pp. 1108–1112.

[14] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering. keele university and durham university joint report," UK, Tech. Rep. EBSE-2007-01, July 2007.

[15] S. Subramani, H. Q. Vu, and H. Wang, "Intent classification using feature sets for domestic violence discourse on social media," in *Proceedings of the 4th Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)*, Mana Island, Fiji, Dec 2017, pp. 129–136.

[16] M. Anzovino, E. Fersini, and P. Rosso, "Automatic identification and classification of misogynistic language on twitter," *In Natural Language Processing and Information Systems. NLDB 2018. Lecture Notes in Computer Science, Paris, France*, vol. 10859, pp. 57–64, May 2018.

[17] R. Ahluwalia, E. Shcherbinina, E. Callow, A. Nascimento, and M. De Cock, "Detecting misogynous tweets," in *Proceedings of the Third Workshop on Evaluation of Human Language Technologies for Iberian Languages (IberEval 2018) co-located with 34th Conference of the Spanish Society for Natural Language Processing (SEPLN 2018)*, S. Sevilla, Ed., 2018, pp. 242–248.

[18] J. S. Canós, "Misogyny identification through svm at ibereval 2018," in *Proceedings of the Third Workshop on Evaluation of Human Language Technologies for Iberian Languages (IberEval 2018) co-located with 34th Conference of the Spanish Society for Natural Language Processing (SEPLN 2018)*, Sevilla, Spain, Sept 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 *Proceedings of the Third Workshop on Evaluation of Human Language Technologies for Iberian Languages (IberEval 2018) co-located with 34th Conference of the Spanish Society for Natural Language Processing (SEPLN 2018)*, vol. 2150, Sevilla, Spain, Sept 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 *Proceedings of the Third Workshop on Evaluation of Human Language Technologies for Iberian Languages (IberEval 2018) co-located with 34th Conference of the Spanish Society for Natural Language Processing (SEPLN . Sevilla*, Sevilla, Spain, Sept 2018, pp. 249–254.

[21] A. Khatua, E. Cambria, and A. Khatua, "Sounds of silence breakers: Exploring sexual violence on twitter," in *Proceedings of the EEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Barcelona, Spain, Aug 2018, pp. 397–400.

[22] H. Liu, F. Chiroma, and M. Cocea, "Identification and classification of misogynous tweets using multi-classifier fusion," in *Proceedings of the Third Workshop on Evaluation of Human Language Technologies for Iberian Languages (IberEval 2018) co-located with 34th Conference of the Spanish Society for Natural Language Processing (SEPLN 2018)*, Sevilla, Spain, Sept 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 *Proceedings of the Third Workshop on Evaluation of Human Language Technologies for Iberian Languages (IberEval 2018) co-located with 34th Conference of the Spanish Society for Natural Language Processing (SEPLN 2018)*, Sevilla, Spain, 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 *Proceedings of the Third Workshop on Evaluation of Human Language Technologies for Iberian Languages (IberEval 2018) co-located with 34th Conference of the Spanish Society for Natural Language Processing (SEPLN 2018)*, J. G. Rosso, R. Martínez, S. Montalvo, and J. C. de Albornoz, Eds., Sevilla, Spain, Sept 2018, pp. 234–241.

[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. ADC 2018. Lecture Notes in Computer Science*, G. C. Wang, J. Chen, and J. Qi, Eds. Springer Charm, May 2018.

[26] E. Shushkevich and J. Cardiff, "Misogyny detection and classification in english tweets: The experience of the ITT team," in *Proceedings of the Sixth Evaluation Campaign of Natural Language Processing and Speech Tools for Italian. Final Workshop (EVALITA 2018) co-located with the Fifth Italian Conference on Computational Linguistics (CLiC-it 2018), Turin, Italy, December 12-13, 2018*, ser. CEUR Workshop Proceedings, T. Caselli, N. Novielli, V. Patti, and P. Rosso, Eds., vol. 2263. CEUR-WS.org, 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 *(eds) Data Mining. AusDM 2018. Communications in Computer and Information Science. 996. Springer*. Singapore: (eds) Data Mining. AusDM 2018. Communications in Computer and Information Science. 996. Springer, Feb 2019.

[28] E. Fersini, F. Gasparini, and S. Corchs, "Detecting sexist meme on the web: A study on textual and visual cues," in *Proceedings of the 8th International Conference on Affective Computing and Intelligent Interaction Workshops and Demos (ACIIW)*. Cambridge, United Kingdom, Sept 2019, pp. 226–231.

[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," *Journal of Intelligent and Fuzzy Systems*, vol. 36, no. 5, pp. 4743–4752, May 2019.

[30] T. Lynn, P. T. Endo, P. Rosati, I. Silva, and L. Santos, "Comparison of machine learning approaches for detecting misogynistic speech in urban dictionaryinternational conference on cyber situational awareness," in *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Oxford, UK, June 2019, pp. 1–8.

[31] D. Nozza, C. Volpetti, and E. Fersini, "Unintended bias in misogyny detection," in *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, Thessaloniki, Greece, Oct 2019, pp. 149–155.

[32] M. Sajjad, F. Zulifqar, M. U. Khan, and M. Azeem, "Hate speech detection using fusion approach," in *Proceedings of the International Conference on Applied and Engineering Mathematics (ICAEM)*, Taxila, Pakistan, Oct 2019, pp. 251–255.

[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, no. 4, pp. 46 210–46 224, April 2019.

[34] M. A. Bashar, R. Nayak, and N. Suzor, "Regularising lstm classifier by transfer learning for detecting misogynistic tweets with small training set," *Knowledge and Information Systems*, vol. 62, pp. 4029–4054, Oct 2020.

[35] M. Canovas-Garcia, J. A. Garcia-Diaz, and R. Valencia-Garcia, "Automatic misogyny detection with linguistic and morphological features in spanish," *Communications in Computer and Information Science*, vol. 139, 2019.

[36] J. M. Coria, S. Ghannay, S. Rosset, and H. Bredin, "A metric learning approach to misogyny categorization," in *Proceedings of the 5th Workshop on Representation Learning for NLP*. Online: Association for Computational Linguistics, 2020, pp. 89–94.

[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 *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 14, 2020, pp. 250–259. [Online]. Available: https://ojs.aaai.org/index.php/ICWSM/article/view/7296

[38] V. K. Jha, H. P, V. P. N, V. Vijayan, and P. P, "Dhot-repository and classification of offensive tweets in the hindi language hindi language," *Procedia Computer Science*, vol. 171, pp. 2324–2333, 2020.

[39] F.-M. Plaza-Del-Arco, M. D. Molina-González, L. A. Ure na-López, and M. T. Martín-Valdivia, "Detecting misogyny and xenophobia in spanish tweets using language technologies," *ACM Transactions on Internet Technology*, vol. 20, no. 2, pp. 1533–5399, May 2020.

[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 *Proceedings of the Second Workshop on Trolling, Aggression and Cyberbullying*. Marseille, France: European Language Resources Association (ELRA), 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 *Social Informatics and Telecommunications Engineering. Digital Forensics and Cyber Crime. ICDF2C 2009. Lecture Notes of the Institute for Computer Sciences*. Berlin, Heidelberg: Springer, 2010, vol. 31, pp. 139–150.

[42] A. Ulges and A. Stahl, "Automatic detection of child pornography using color visual words," in *2011 IEEE International Conference on Multimedia and Expo*, 2011, pp. 1–6.

[43] D. Bogdanova, P. Rosso, and T. Solorio, "Exploring high-level features for detecting cyberpedophilia," *Computer Speech and Language*, vol. 28, no. 1, pp. 108–120, 2014.

[44] N. Sae-Bae, X. Sun, H. T. Sencar, and N. D. Memon, "Towards automatic detection of child pornography," in *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, Paris, France, Oct 2014, pp. 5332–5336.

[45] H. Pranoto, F. E. Gunawan, and B. Soewito, "Logistic models for classifying online grooming conversation," *Procedia Computer Science*, vol. 59, pp. 357–365, 2015.

[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," *Digital Investigation*, vol. 26, pp. 40–54, Sept 2018.

[47] J. Macedo, F. Costa, and J. A. dos Santos, "A benchmark methodology for child pornography detection," in *31st Conference on Graphics, Patterns and Images (SIBGRAPI)*, 2018, pp. 455–462.

[48] P. Anderson, Z. Zuo, L. Yang, and Y. Qu, "An intelligent online grooming detection system using ai technologies," in *Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, New Orleans, LA, USA, Oct 2019, pp. 1–6.

[49] S. Nikiforos, S. Tzanavaris, and K.-L. Kermanidis, "Virtual learning communities (vlcs) rethinking: Collaboration between learning communities," *Education and Information Technologies*, vol. 25, no. 5, pp. 3659–3675, 2020. [Online]. Available: https://doi.org/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 Systems with Applications*, vol. 88, no. 1, pp. 402–418, Dec 2017.

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

[52] P. Majumdar, S. Chhabra, R. Singh, and M. Vatsa, "On detecting domestic abuse via faces," in *Proceedings og the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, vol. 39, no. 8, Jun 2018, pp. 859–871.

[53] S. Gao and L. Ye, "A physical and verbal bullying detecting algorithm based on k-nn for school bullying prevention," *AICON 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 287, . Harbin, China*, pp. 150–157, July 2019.

[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 *Proceedings of the International Conference on Artificial Intelligence for Communications and Networks*, S. Informatics and C. Telecommunications Engineering. 287. Springer, Eds. Lecture Notes of the Institute for Computer Sciences, 2019.

[55] L. Ye, H. Ferdinando, T. Seppänen, T. Huuki, and E. Alasaarela, "An instance-based physical violence detection algorithm for school bullying prevention," *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1384–1388, 2015.

[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.

[57] G. C. Harikiran, K. Menasinkai, and S. Shirol, "Smart security solution for women based on internet of things," in *Proceedings of the International Conference on Electrical Electronics and Optimization Techniques (ICEEOT)*, Chennai, India, March 2016, pp. 3551–3554.

[58] O. Permatasari, S. U. Masruroh, and Arini, "A prototype of child monitoring system using motion and authentication with raspberry pi," in *Proceedings of the 4th International Conference on Cyber and IT Service Management*, Bandung, Indonesia, April 2016, pp. 1–6.

[59] A. Helen, M. F. Fathila, R. Rijwana, and K. V. K. G., "A smart watch for women security based on iot concept 'watch me'," in *2nd International Conference on Computing and Communications Technologies (ICCCT)*, July, 2017, pp. 190–194.

[60] M. Kavitha and V. Sivachidambaranathan, "Women self protecting system using internet of things," in *Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, Dec 2018, pp. 1–4.

[61] T. Muskan, M. K. Khandelwal, and P. S. Pandey, "Women safety device designed using iot and machine learning," in *Proceedings of the IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, China, Oct 2018, pp. 1204–1210.

[62] S. P. Raflesia, Firdaus, and D. Lestarini, "An integrated child safety using geo-fencing information on mobile devices," in *Proceedings of the International Conference on Electrical Engineering and Computer Science (ICECOS)*, Pangkal, Pinang, Oct 2018, pp. 379–384.

[63] N. R. Sogi, P. Chatterjee, U. Nethra, and V. Suma, "Smarisa: A raspberry pi based smart ring for women safety using iot," in *Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA)*. Coimbatore, India, July 2018, pp. 451–454.

[64] W. Akram, M. Jain, and C. S. Hemalatha, "Design of a smart safety device for women using iot," *Procedia Computer Science*, vol. 165, pp. 656–662, 2019.

[65] R. Paknikar, S. Shah, and P. Gharpure, "Wireless iot based solution for women safety in rural areas," in *Proceedings of the International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, July 2019, pp. 232–237.

[66] A. Z. M. Tahmidul Kabir, A. M. Mizan, and T. Tasneem, "Smart shoe for women safety," in *Proceedings of the IEEE 10th International Conference on Awareness Science and Technology (iCAST)*, vol. 2018, Oct 2019, pp. 1–4.

[67] T. Sen, S. Singh, and V. N. Kumar, "Protecht – implementation of an iot based 3 –way women safety device," in *Proceedings of the Third International Conference on Electronics Communication and Aerospace Technology [ICECA 2019]*, Coimbatore, India, Sept 2019, pp. 1377–1384.

[68] T. M. R, S. Aishwarya, C. K., D. M. K, and N. H, "Iot based smart security gadget for women's safety," in *Proceedings of the 1st International Conference on Advances in Information Technology (ICAIT)*, Chikmagalur, India, July 2019, pp. 348–352.

[69] K. Thamaraiselvi, S. Rinesh, L. Ramaparvathy, V. Karthick, and Tirunelveli, "Internet of things (iot) based smart band to ensure the security for women," in *Proceedings of the International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, Feb 2019, pp. 1093–1096.

[70] M. S. Uddin, "Development of wearable emergency response system for women," in *Proceedings of the IEEE 6th International Conference on Engineering Technologies and Applied Sciences (ICETAS),*, Kuala Lumpur, Malaysia, June 2019, pp. 1–6.

[71] V. Hyndavi, N. S. Nikhita, and S. Rakesh, "Smart wearable device for women safety using iot," in *Proceedings of the 5th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, July 2020, pp. 459–463.

[72] A. Kabir, A. Mizan, and T. Tasneem, "Safety solution for women using smart band and cws app," in *Proceedings of the 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, Phuket, Thailand, June 2020, pp. 566–569.

[73] B. 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 *Proceedings of the International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Vellore, India, Feb 2020, pp. 1–4.

[74] S. Silva, S. J., P. R., R. V., B. D., R. A. F., and Abreu, "Wedocare: A system for vulnerable social groups," in *Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, Nevada, April 2019, pp. 5332–5336.

[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," *European Journal of Psychology of Education*, vol. 26, pp. 21–44, Feb 2011.

[76] C. Raminhos, A. P. Cláudio, M. B. Carmo, A. Gaspar, S. Carvalhosa, and M. d. Candeias, "A serious game-based solution to prevent bullying," *International Journal of Pervasive Computing and Communications*, vol. 12, no. 2, pp. 194–215, 2016.

[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 *Proceedings of the Joint International Conference on Serious Games*. Springer Cham, Nov 2017, pp. 259–270.

[78] R. Mason and L. Turner, "Serious gaming: A tool to educate health care providers about domestic violence," *Health Care for Women International*, vol. 39, no. 8, pp. 859–871, May 2018.

[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 *Game Creation, Design, Learning, and Innovation. ArtsIT 2019, DLI 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. 328. Springer, Cham*, Brooks and E. Brooks, Eds., 2020.

[80] S. Kriglstein, F. Hengstberger, F. Fribert, K. Stiehl, B. Schrank, A. Pfeiffer, and G. Wallner, "Be a buddy not a bully - two educational games to help prevent bullying in schools," in *Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play*. New York, NY, USA: Association for Computing Machinery, Nov 2020, pp. 287–291.

[81] (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. retrieved march 18, 2021, from https://www.coe.int/en/web/human-rights-channel/stop-sexism. [Online]. Available: RetrievedMarch18,2021,fromhttps://www.coe.int/en/web/human-rights-channel/stop-sexism

[83] NSPCC. What parents need to know about sexual grooming. retrieved march 19, 2021, from https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/#what-is. [Online]. Available: RetrievedMarch19,2021,fromhttps://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/#what-is

[84] V. Egan, J. Hoskinson, and D. Shewan, "In perverted justice: a content analysis of the language used by offenders detected attempting to solicit children for sex," *Antisocial Behavior: Causes, Correlations and Treatments*, vol. 20, no. 3, pp. 273–297, 2011.

[85] U. S. D. of Health and H. Services. What is child abuse or neglect? what is the definition of child abuse and neglect?. retrieved march 24, 2021 from https://www.hhs.gov/answers/programs-for-families-and-children/what-is-child-abuse/index.html. [Online]. Available: RetrievedMarch24,2021fromhttps://www.hhs.gov/answers/programs-for-families-and-children/what-is-child-abuse/index.html

[86] F. Ke, "Computer-game-based tutoring of mathematics," *Computers and Education*, vol. 60, no. 1, pp. 448–457, Jan 2013.

[87] B. Bonnechere and S. Van Sint Jan, "Chapter 39 - rehabilitation," in *DHM and Posturography*, Scataglini and G. Paul, Eds. Academic Press, 2019, pp. 541–547.

[88] G. Alinier, C. Tuffnell, and B. Dogan, "Chapter 45 - simulation on a low budget," in *Clinical Simulation (Second Edition)*, G. Chiniara, Ed. Academic Press, 2019, pp. 667–689.

[89] Alexa. The top 500 sites on the web (2021, march 30). https://www.alexa.com/topsites. [Online]. Available: 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," *Computers in Human Behavior*, vol. 114, p. 106528, Jan 2021.

DALIA ANDREA RODRÍGUEZ earned her B.Sc. in mathematics with a specialization in computing from University of California, Los Angeles (UCLA) in 2019. Rodríguez is currently pursuing an M.Sc. degree in computer science at Tecnológico Nacional de México at their Instituto Tecnológico de Mexicali (ITM) campus. Her research interests include artificial intelligence (AI), Internet of Things (IoT) and eHealth. Specifically, she analyzes how AI and IoT can be used to address social issues such as gender inequality and child abuse.

ARNOLDO DÍAZ-RAMÍREZ earned his bachelor's degree in Computer Sciences from Cetys Universidad, Mexicali, México in 1988. In 2006 he obtained his PhD degree in Computer Sciences from Universitat Politecnica de Valencia, Spain, where his research focused on scheduling of real-time systems. Since 1992 he is with Tecnologico Nacional de Mexico at the Instituto Tecnologico de Mexicali (ITM) campus, where he works as a research professor. Currently, he is the coordinator of the Industrial Informatics research group at 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 E. MIRANDA-VEGA was born in 1984 and received BS degree in Electrical and Electronic Engineering from ITLM, in 2007, and a Master's degree in Electronic Engineering from the TecNM/IT Mexicali, in 2014 and receive PhD degree in Science, Applied Physics from the Autonomous University of Baja California in December 2019 and receiving honorable mention. He has written 3 book chapters and 11 journals and proceedings conference papers. His current research interest includes machine vision, data signal processing, the theory and optoelectronics devices, and their applications.

LEONARDO TRUKILLO is Professor at Tecnológico Nacional de México/IT de Tijuana, Tijuana, Mexico. He has a Doctorate in computer science from CICESE research center in Ensenada, Mexico. His work focuses on genetic programming and machine learning. He has been the PI of several national and international research grants, receiving several distinctions from the Mexican Science Council (CONACYT). His work has been published in over 60 journal papers, 60 conference papers, 18 book chapters, and he has edited 4 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, is series co- chair of the NEO Workshop, and has organized, been track chair or served as 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, QUERETARO, MEXICO, IN 1985, AND THE PH.D. DEGREE IN INFORMATICS FROM THE POLYTECHNIC UNIVERSITY OF MADRID, SPAIN, IN 1995. HE HAS BEEN PROFESSOR FOR THE COMPUTER SCIENCE DEPARTMENT AT CINVESTAV-IPN, SINCE 1997. HIS MAIN RESEARCH INTERESTS ARE MOBILE COMPUTING, REAL-TIME SYSTEMS SCHEDULING, ADAPTIVE FAULT TOLERANCE, AND SOFTWARE ENGINEERING.