symmetry

MDPI

Review

Towards a Holistic ICT Platform for Protecting Intimate Partner Violence Survivors Based on the IoT Paradigm

Ignacio Rodríguez-Rodríguez [1,2,*], José-Víctor Rodríguez [3], Aránzazu Elizondo-Moreno [4], Purificación Heras-González [5] and Michele Gentili [6]

[1] Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, 30100 Murcia, Spain

[2] Instituto Universitario de Estudios de Género, Universitat d'Alacant, 03080 Alicante, Spain

[3] Departamento de Tecnologías de la Información y las Comunicaciones, Universidad Politécnica de Cartagena, 30202 Cartagena, Spain; jvictor.rodriguez@upct.es

[4] Expert in Family Counselling, Freelance Worker, 30008 Murcia, Spain; areli7815@hotmail.com

[5] Departamento de Ciencias Sociales y Humanas, Universidad Miguel Hernández de Elche, 03202 Elche, Alicante, Spain; p.heras@umh.es

[6] Dipartimento di Ingegneria Informatica Automatica e Gestionale 'Antonio Ruberti', Sapienza Università di Roma, 00185 Roma, Italy; gentili@diag.uniroma1.it

[*] Correspondence: ignacio.rodriguez1@um.es

Received: 3 December 2019; Accepted: 20 December 2019; Published: 23 December 2019

Featured Application: A complete review of information and communication technology (ICT) strategies to manage intimate partner violence (IPV) and protect IPV survivors is provided. A holistic ICT solution which would overcome the limitations of previous works is presented, promoting symmetry in society.

Abstract: Intimate partner violence (IPV) remains a scourge that compromises the rights of many women around the world, shaping an asymmetry in civil rights. Fighting gender-based violence, especially when it is committed by an intimate partner, is an important responsibility that needs to be addressed from all angles. It is also remarkable that our society is clearly conditioned by information and communication technology (ICT), which involves many aspects of our daily life. Unfortunately, violence that is performed in the real world is also replicated in this 'virtual' existence, by offenders in ICT contexts. On the other hand, the same technologies also provide a plethora of opportunities to fight IPV, which are enhanced by the innovative paradigm of the so-called Internet of Things (IoT). In this work, we first present a thorough compilation of ICT proposals already published—based on either hardware or software—aimed at protecting IPV survivors, and which can be applied in real life situations but also within social networks. The challenges that still lie ahead are highlighted and, a complete ICT-based platform for IPV management, within an IoT framework, that overcomes the limitations of previous works is proposed, and then promoting a symmetry between individuals in society.

Keywords: intimate partner violence; information and communication technologies; wearable sensors; internet of things; machine learning

1. Introduction

Intimate partner violence (IPV) is currently a serious problem for millions of women around the world. It includes physical, sexual, and psychological harm by a current or former partner or spouse, in any form or means. According to UN (United Nations) statistics, almost 35% women around the world have experienced some kind of physical or sexual violence [1]. The same statistics show that some 75% of women face physical and sexual aggression. This is a call for attention to be paid to this scourge. It is incredible that in 2017, some 87,000 women were killed across the world, of whom 58% (50,000) were killed by their husband or other relatives (https://www.unodc.org/).

In recent years much research has focused on IPV and its connection to many related issues, that is, social awareness [2]. This wide scope includes resources used by the victims (from now on, more appropriately called 'survivors') [3], barriers, and formal assistance in facing different expressions of violence [4]. Nonetheless, some authors like Bruckman have noted that the way violence is developed and its impact on women in an environment characterized by the use of information and communication technology (ICT), such as mobile phones, social media, or generally using internet, has not been properly studied or documented [5], although in recent years it has become an issue of study [6].

In 2019, ICT and especially the internet, have clearly advanced in every aspect of society, and have had an effect in every part of the world. In the early 1990s, Haraway [7] anticipated the social changes and the effect, especially in gender issues, that would accompany ICT. It is important to bear in mind that ICT has changed the way we interact socially in issues as important as job seeking, health promotion, commerce, work, and every kind of human relations [8].

In this sense, human interaction in a virtual environment resembles relationships in the real world, and old forms of harassment, including sexual harassment and harassment on the grounds of sex, have adapted to this new habitat, in the form of new violence [9,10]. As a result, we are now getting used to concepts such as *cyberstalking*, *doxing*, *phishing*, *grooming*, or *sextortion*. These new offences have been widely described in the literature [11,12].

In addition to these expressions of violence, the cyber environment also reproduces the general gender gap that exists in society [13]. Combined with gender pay gap and the other inequalities present in our world, the terms "digital gender gap" or "digital gender divide", involve a social issue referring to the differing amount of information between those who have access to the internet (especially broadband access) and those who do not, as described in terms of gender. This comprises three different gaps [14]: differences in resources and access to them, inequalities in abilities and utilizing ICT effectively, and also a content divide, wherein much web-based information is simply not relevant to the real needs of women. Nearly 70% of the world's websites are in English. This digital gender divide is increased with poverty, illiteracy, lack of computer literacy and language barriers. The digital gender divide leads to dependence in several ways, including economic dependency, isolation, perpetuated stereotypical portrayals and the exploitation of women, enhanced when other intersections are found [15].

Fortunately, ICT also offers new opportunities to prevent and manage these types of violence. Technological advances, software solutions, and new concepts such as the Internet of Things (IoT), and cloud computing strategies, offer a wide range of possibilities for dealing with violence against women [16], both in real life and also in a cyber environment. These resources has been successfully applied to other fields, such as e-health [17]. Strategies for advanced data processing, such as machine learning (ML) and Big Data [18], can also combat gender violence.

This work first provides a complete review of ICT applications used to prevent, manage, and increase awareness of IPV, focused on increasing the safety of survivors, sometimes still cohabiting with offenders, sometimes living apart. A new ICT-based platform for protecting IPV survivors, which considers the IoT paradigm, is presented. Section 2 describes contributions based on hardware, mainly aimed at tele-monitoring; Section 3 explores the possibilities of software solutions using ML approaches and also remote assistance. Section 4 explains some emergency systems. Section 5 discusses the dilemmas of privacy, security communications, ethics and the importance of IPV survivors accepting ICT solutions. Section 6 describes challenges to be faced, and in Section 7 a complete, holistic IoT-based platform to deal with IPV using ICT—which overcomes the limitations of previous works—is proposed. Section 8 draws conclusions, and closes the document.

2. Hardware-Based Solutions: Telemonitoring

Telemonitoring involves the continuous harvesting of data from survivors in order to clearly identify their exact condition and location. Advances in the field of biometrics make it possible to maintain 24-h monitoring of the person suffering harassment, thus recording important information about their status in order to detect or even anticipate (see following sections) a risky situation. Collected biometric information can be addressed using the IoT. The gathering device used as the cornerstone of this process will, of course, be the *smartphone*.

2.1. Wearable Devices Structured in a Body Area Network (BAN) Environment Within an Internet of Things (IoT) Context

Remarkable electronics advances have introduced miniaturization and more powerful innovations in biometrics, the field in which measurable biological characteristics are studied. It is now possible to measure certain variables in a continuous mode, most of them vital signs (such as the heart rate and exercise), which can change due to a risky situation in real life, characterizing the body response to an attack. By now, thanks to devices such as smartbands, smartwatches and other wearables (some designed in principle for fitness and medical purposes), it is possible to obtain a great deal of useful information. Moreover, their connectivity, with options such as Bluetooth, near-field communication (NFC) or ZigBee make it possible to easily share the data. Unfortunately, this is restricted by their size, length of battery life, and the fact that these devices were generally designed for recreational uses.

Variables such as exercise, movement, heart rate temperature, perspiration, location, velocity and acceleration in motion can be taken into account in order to check abnormal variations caused by physical violence. In this sense, several studies have examined such variables. Ye et al. [19] discovered that it is possible to detect expressions of violence thanks to the movements of the person being monitored, using accelerometers and extracting and filtering patterns. More recently, and using a wider application, Elbasiony et al. [20] explored the possibility of describing ordinary activities and human behavior using only registered movements. This idea was also studied using smartphone accelerometers [21,22].

Location is another important feature that needs to be taken into account. Identifying the exact Global Positioning System (GPS) coordinates of an offence being committed allows fast interventions in critical situations. This is sometimes implemented as a measure activated by the survivor [23], and also complemented with other systems, such as the Global System for Mobile communications (GSM) and NFC [24].

The physical variables of survivors can be measured in several ways, but one of the most interesting alternatives is smartbands [25]. Recent models from different manufactures offer an affordable and reliable way to monitor every day more characteristics, including temperature, perspiration, and blood pressure, and have improved connectivity and battery duration. Heart rate is one of the commonly measured features in most of the models, and Ferdinando et al. [26] found that it could be an indicator of emotional state. Other complex systems involve the use of the electrocardiogram (ECG) to detect an abuse situation [27].

In summary, thanks to commercial wearable devices we can now easily identify the following variables of an IPV survivor:

- Location
- Movement
- Heart rate
- Temperature
- Perspiration

- Blood pressure
- Schedule (habits)
- Other physical features considered in the system, with the aim of personalizing their management, such as age, height and weight

The inclusion of monitored features generates a large amount of information, however, and creates a new problem: the need to handle it in an appropriate ICT framework that is designed to collect and gather data, process it and obtain useful information.

A body area network (BAN) is a wireless network carried by a person, composed of the forenamed wearable computing devices. A BAN involves all of the applications and communications on, in and near the body. As stated, the monitoring of physiological signals can be used in order to detect a reaction to an attack.

The idea of a BAN was introduced more than a decade ago, in the work of Broens et al. [28], focusing on epilepsy sufferers. Via a 24-h monitoring method, the system forecast epileptic attacks and then prevented harm to the patient. The concept of the BAN was completed later, using a proper data-exchange platform, which is necessary to funnel the data [29].

A BAN requires the use of a device able to play the roles of a body gateway and a network hub. Nowadays, this is something that most of us are carrying close to us for 24 h: a smartphone. This device has been called a monitoring wearable thanks to its accelerometers and GPS equipment, but it can help as a gateway and a tool to manage information.

At the moment, smartphones present a level of adaptability that are unachievable by any other device. They allow us to:

- Keep the software responsible for managing a risky situation and supervise the survivor protection.
- Gather information from wearables devices. There are many possibilities for connectivity, including not only 4G/5G, but also Bluetooth, Wi-Fi, NFC (Near Field Communication), Ant+, and so on, offering a plethora of different choices.
- Send data and information to the cloud, to be either stored or computed (cloud computing).
- Forward emergency calls in case the survivor is at risk.
- Update their software when required.

These ideas need a proper environment to be developed and in this sense, an innovate concept is becoming common in our daily lives: the IoT, which could be described as the interconnection, via the internet, of computing devices embedded in everyday objects, enabling them to send and receive data. This structure has been applied to protect IPV survivors by Monisha et al. [30], who added a camera for video recording of specific recognized human postures, using a hidden Markov and Baum-Welch algorithm adopted to classify, train and test the system. By now, these proposals are often found in literature [31,32] and will be the subject of a deeper analysis at a later stage.

2.2. Communications Environment

Once the main architecture is outlined, a proper communication infrastructure is required to send the data to the gateway and then to the cloud, where data about survivor status will be processed and a proper response will be chosen. There are now many connection possibilities, offering a wide range of ways to transmit information.

A simple Wi-Fi transmitter attached to the monitoring devices can open new perspectives in connectivity, however, outside the range of Wi-Fi, which may only be available in a home or other building, the smartphone mobile connections themselves, either a 4G connection or the leading edge 5G, offers many possibilities, as Mavromoustakis et al. noted [33]. Monitoring devices can also send data collected from the survivor directly to the cloud if they have an individual SIM (Subscriber Identification Module) card.

Cooperation and communication between monitoring systems can be achieved using Bluetooth technology, and has the advantage of Bluetooth low energy (BLE) which improves energy saving. BLE allows a connection to be put to sleep, and wake up quickly (3 ms) [34], and can also use NFC, although this requires a small distance between devices.

ZigBee is another alternative for funneling data, as it is a high-level communication protocol able to create BANs with small, low-power digital radios. It has been widely studied and applied in home automation and other small-scale projects. It is cheap and allows a high number of nodes in the network (more than 65,000), offering lower energy consumption.

2.3. Other IoT Devices

The previously exposed smart environment is not restricted to the BAN built on the survivor to monitor her physical and vital signs. The faces of IPV are revealed, in varying stages of violence, usually in their own home, sometimes while living with the offender, sometimes because the offender has managed to enter the survivor's house. Today domotics, understood as ICT applied to the home to create a 'smart home', can also offer opportunities to protect and guard women suffering violence.

Environmental control units (ECUs) have been becoming more popular for a few years, and are also known nowadays as 'smart speakers' or 'virtual assistants'. There are many commercial devices, such as the Echo, which is equipped with an artificial intelligence (AI), called Alexa (Amazon), the HomePod with an AI called Siri (Apple), and Google Home (Google) [35]. The use of female voices in these devices has introduced a discussion about a possible inappropriate usage [36]. These devices are usually connected by Wi-Fi and prepared with far field microphones, enabling voice recognition and hands-free operation for environmental control purposes. This allows other possibilities beyond recreational use, and they have proven useful for people with disabilities [37]. There are also applications in the field of home security, such as the commercial Alexa Guard, which provides an alarm when noises are detected (such as breaking glass), and can also detect a cry for help. The idea of a scream detector has been explored by Huang et al. [38]. Such devices could be applied in the management and prevention of IPV.

Many other ICT applications for safety are reported in the literature. Using IoT environments, security cameras, motion detection systems, opening/closing detectors for windows and doors, and many other applications [39] can be applied in a survivor's home, allowing remote monitoring by the survivor, but also by a trusted third party, and of course, the installation of alarms.

Domotics can also be used to generate violence, however, if control is in the offender's hands. Web-connected devices are also being used against women to control, harass, abuse and even lock them in their own homes [40].

2.4. Offenders Monitoring: Global Positionining System (GPS) Bands/Social Networks Monitoring

When talking about protection from IPV, the focus is often on the survivor's safety. This means monitoring, installing devices in their home and overall increasing their surveillance, however, this strategy can be extended when an offender is with the police, in a court process, or if, under a legal protective order, a judge decides that the accused needs to be under supervision and cannot be near the survivor in a given area. For this purpose, technology offers GPS bands, equipped with security measures to stop them being manipulated or removed. Beyens and Roosen [41] studied the possibility of replacing remand custody with such technology in Belgium, concluding that is a good option with which to control home confinement. Gies et al. [42] showed that the GPS condition was associated with significantly fewer parole and arrest violations, arrests, and convictions.

Payne and DeMichelle [43] noted some weaknesses in the use of such surveillance, however, such as promoting a false sense of security in some ways, and the lack of a deep understanding of the systems by police and survivors, which can lead to errors.

Social media networks are an environment in which offenders can continue their harassment in cyberspace, Monitoring social networks is not a hardware-based solution, but it is included here as a means of telemonitoring. It is possible due to ML techniques and AI strategies, which can auto-recognize offensive text. This involves the monitoring both the survivor's, and also the offender's, activities in social networks. AI (Artificial Intelligence) algorithms will be introduced in more detail in the next section, as well as the possibilities of implementing software for IPV management and prevention.

3. Software-Based Solutions

This section discusses solutions based in software which can deal with data that has been harvested from both the survivor and the offender. After processing data, some situations could be detected and a proper response could be activated, in order to protect someone from a real/cyber assault.

3.1. Machine Learning (ML) Algorithms

ML is an application of AI that provides ICT-based systems with the ability to automatically learn and improve from experience without being explicitly programmed. These algorithms are able to extract knowledge from data and then, after a learning phase, develop a complex task. Among the possible applications are diagnosis, analysis, forecasting and many others. Raw data become then knowledge.

Smart speakers implement AIs which are equipped with modules for voice recognition based in ML. This is fundamental in protecting survivors, as voice recognition can distinguish orders and keywords given by women suffering from IPV, or by offenders, then obtain the requested information, or warn the emergency channels. Islam et al. [44] partially based their proposal exposed in their work in this idea.

ML can also recognize abnormal physical activity, thanks to classification techniques. Ye et al. [45] created a physical violence detection algorithm for school bullying prevention, which could be easily adapted to IPV survivors. Similarly, Hegde et al. [46] used data collected from wearable sensors to identify the activities of daily life. This could also be useful to detect unexpected situations, such as potential aggression.

Text recognition and applications to identify violence discourse have been developed. O'Halloran et al. [47] explore this idea in their recent work. In the next subsection we will note some uses of this technique in social media.

ML techniques are also powerful in making predictions. Ozkan [48] studied the possibility of future recidivism in offenders, using neural networks with good results. The results of algorithms can be used to decide about parole in interpersonal violence situations [49], and Berk et al. [50] used Random Forest algorithms and concluded that approximately 20% of those released after an arraignment for domestic violence are arrested within two years for a new domestic violence offense, and also offered an important ranking of risk factors for multiple assaults.

3.2. Other Strategies: Apps for Smartphones/Social Media Monitoring/Tele-Assistance

This section concludes with an overview of other important solutions that are non-hardware based. In this sense, it is fair to begin remarking on the enormous impact of the promotion of some apps on society, focused in smartphones and developed with the aim of raising awareness of IPV, and also managing harassment situations [51]. Right now, a search of *Google Play* (https://play.google.com/), (the main platform for users to download apps based on the Android operating system) results in hundreds of apps related to the terms 'domestic violence', 'intimate partner violence' and 'violence against women', in many different languages, for different purposes, and some of them developed by official institutions such as governments, or security forces. One was developed by Mareeswari et al., who in [52] explain their Android app with implemented emergency measures for IPV survivors in danger, such as an auto audio recorder, video recorder, SOS button, and a system to detect hidden cameras.

Threats and verbal abuse are also carried out using social networks. A feeling of anonymity and impunity mean that some people give full rein to violence. The impact of gender-based violence in Twitter was studied by Purohit et al. [53], revealing public awareness of domestic-violence tolerance and suggesting opportunities for intervention. Some offenders use these networks to stay in contact with their victims, or to impose a control strategy so that their abuse can continue (or be initiated) abuse in cyberspace. Del Vigna et al. develop two strategies, based on support vector machines and neural networks to detect hate speech on Facebook [54]. Monitoring activity can be implemented on social networks on behalf of the survivor, but also on behalf of the offender (if considered in a court).

Finally, it is also important to note that ICT allows remote assistance and permanent support for survivors. This aid could be at a psychological level, using videoconferences [55], but also technological. It is necessary to highlight the importance of providing survivors with specialized help in ICT issues, since some offenders use spy-programs, trojans, phising, and many other strategies to continue harassment in cyberlife. It is thus conceivable that survivors could need, and increasingly in this technological society, ICT support from a computer expert. With this idea, two secondary but important aspects should be noted: (1) this aid could be provided using remote assistance, via a remote desktop, and (2) The computer expert needs to be trained in dealing with survivors, so they must receive education in gender-sensitive approaches [56].

4. Emergency Measures

Once we have exposed a consistent structure, either in hardware or in software, then we can develop tools to improve the safety of a survivor in a risky situation. Most of the emergency measures based on technology handled by the survivor involve two methods: identifying the abuse situation and facilitating the requests for help.

For the former, Nanjo et al. propose the acoustic detection of emergency shouts, using a voice recognition algorithm [57]. Viswanath et al. [58] describe a chip that is attached to footwear and is activated when a person taps one leg behind the other four times. In essence, the methods found in the literature are focused on a key event that indicates an abusive situation.

The screaming alarm in a belt with Arduino based on IoT [59] presented by Harikiran et al., or a safety armband which would help the victims not only to send a panic and alert message but also to collect evidence in the form of images [60], should be noted. Mohanaprakash and Sekar [61] similarly propose a smart band able to emit a loud alarm for self-defense purposes, and to send location and messages to emergency contacts. Of course, the ability to call for help through a specific APP located within the smartphone is also an interesting option, as addressed in the previous section.

Other work has improved the emergency response, such as the proposal by Sun et al. [62], where, thanks to a support decision making system, it is possible to send assistance to a municipality or police forces to handle a dangerous situation.

5. Vulnerabilities: Ethics, Hardware Limitations and Survivors' Acceptance

5.1. Ethics: Security and Privacy Dilemmas

Security in ICT environments is one of the most controversial issues in technology applications, and in recent years this concern has become critical in IoT environments, an area still in an evolutionary stage. IoT devices are generally cheap, and have limited computing and storage capacity, and this makes them vulnerable to various attacks. This becomes truly serious in areas such as banks, healthcare, and, without doubt, IPV survivor safety. Some authors, such as Yu et al. [63], insist on the importance of this idea in ICT and especially IoT-based structures, which can easily be exposed to a distributed denial of service (DDoS) attack. Chiang and Zang [64] suggest some future strategies to strengthen IoT communications: keeping security credentials and software up to date, protecting resource-constrained devices, assessing the security status of a large distributed system in a trustworthy manner, and responding to security compromises without causing intolerable disruptions.

Security concerns are also connected to privacy issues. As stated, privacy is an important issue for IPV survivors. Offenders try to keep in touch with survivors, and then continue their control and harassment. When women are under protection, their data (new address, new telephone number etc.) is carefully protected, and they cannot afford a lack of privacy. A huge number of privacy-preserving algorithms have been developed to protect sensitive data, such as k-anonymity, and l-diversity [65]. In a k-anonymized dataset, each record is indistinguishable from at least $k-1$ other records, with regard to certain identifying attributes. L-diversity is a form of group-based anonymization which increases privacy in data sets by reducing the granularity of a data representation. Finally, the increasingly popular technology called 'blockchain' can also be an appropriate way to protect data, and thus, a survivor's privacy [66].

5.2. Hardware Limitations and Information and Communication Technology (ICT) Weaknesses: Interoperability and Battery Autonomy

Harvesting data from IPV survivors is advantageous, as far having large amounts of data allows ML techniques to extract valuable knowledge that is useful for protecting survivors, but we need to bear in mind that compatibility is required between monitoring devices, and also in order to promote the sharing of data. This implies full integration into wireless sensor networks, and taking into account the mobility of the source of data [67].

Introducing different sensors to a survivor's BAN could mean a broad range of different communications requirements in this IoT structure. We need high continuous data transmission, sufficient bandwidth but also low energy consumption, together with the idea of using a smartphone as a gateway. This idea has been previously studied in healthcare, as we can see in Talpur et al. [68], who report on low power BANs, using BLE, as well as NFC or Wi-Fi [29]. Zigbee has been also implemented successfully in low-power wireless body area networks with discrete sensors, such as blood pressure monitors and weighing scales [69], and could also be included in an IPV survivor monitoring system.

A 6LoWPAN (acronym of IPv6 over Low -Power Wireless Personal Area Networks) approach as well as NFC [70] have also been used in elderly healthcare, and could be considered for IPV.

5.3. Survivor Acceptance and ICT Education

Ultimately, telemonitoring requires acceptance from the IPV survivor. These techniques can improve their safety, but also imply recording personal data, wearing smart devices, and allowing text and voice recognition software, and this could be considered interference in a private life. This could lead to a rejection of the technology by the survivor. Claudio et al. [71] identified such feelings from users of emergency systems, some of whom were focused on healthcare. Variables such as age, education level, and lifestyle can moderate the level of acceptance. Motty et al. presented a list of 20 human-centered design principles [72] that need to be considered.

On the other hand, when talking about ICT technologies, a survivor requires a minimum level of skills in this field, including to be aware of the risks involved, to know at a basic level how to handle devices and computers, and how to avoid an excessive sense of security. Finn et al. [73] noted this crucial requirement and suggested a useful and effective program with survivors to improve computer confidence and knowledge of computer safety.

6. Challenges to Be Overcome

As can be summarized in Table 1, we have so far provided a brief overview of the scientific literature regarding ICT solutions for IPV survivor safety, and it is possible to identify some characteristics for improvement, in order to draft a holistic solution for IPV management and survivor support using ICT technologies.

The potential of BAN have not been exploited to their full extent as regards physical IPV survivor monitoring. Tracking vital signs has been reported in literature but, to the best of the authors' knowledge, there is no complete body tracking that can unambiguously detect an abuse situation. Integration with a smartphone, in order to complete a BAN, is only partially studied, as are the possibilities of smartphones being a cornerstone to gather information in the cloud. A proper discussion of communication channels, including Wi-Fi, ZigBee, 6LowPAN, and BLE, also needs to be assessed and analyzed.

Table 1. Topics and related works.

Topic	Related Works
Contextualization	[1–8]
Emergence of ICT related violence	[9–12]
Gender gaps	[13–15]
Smart management platforms	[16–18,74]
Telemonitoring, Body Area Network	[19–32,75,76]
Communications funnels	[33,34]
Potential IoT devices	[35–40]
Offenders monitoring	[41–43]
Machine learning algorithms	[44–50]
Apps, Social media, Tele assistance	[51–56]
Emergency measures	[57–62]
Ethics, privacy	[63–66]
Hardware weakness	[29,67–70]
Survivors' acceptance	[71–73]

Utilities such as GPS location undoubtedly need to be implemented, as well as continuous GPS tracking, or both survivors and offenders (if considered in a court).

Due to the variety of smartphone apps available, it is necessary to create one with all the required functionalities. The controller application installed in a phone has to be reliable, avoiding clashes with other applications running in the device. Circumstances such as the eventual discharge of battery or loss of connectivity must be prevented.

The opportunities presented by ML techniques should also be taken into account. This includes text and voice recognition and also forecasting algorithms to prevent a hypothetical abuse situation.

In summary, a complete IPV management platform can be described, considering the following terms:

- The complete characterization of IPV survivor status: not only related to biological facts, but also to their environment (including their home or workspace), and their virtual life (i.e., social networks).
- Full sensor integration. Technological advances have introduced novel biosensors, which have to be coordinated with smartphone capabilities (accelerometers, gyroscopes, light sensors, microphone, camera, and many others). These devices could work with different ways of transmitting information. A management platform needs to unite all these data sources.
- Large data volume. Considering the previous requirement, the amount of data provided could be huge, so we have to foresee ways to deal with it (Big Data solutions).
- Leverage of ML techniques. AI and particularly ML techniques are being applied to a wide variety of fields where data can be collected. Although some approaches have been made, the applications of these algorithms have not been exploited to their limits.
- Emergency module. With all the previously mentioned tools, an IPV platform needs to take control of the situation when an abusive situation is taking place. So, we need mechanisms to: (1) Detect situations (activated by survivor or automatically), (2) Discourage offenders (using acoustic alarms or other defenses), and (3) Warn emergency services and security forces about the status of the survivor.
- Easy connection between survivor, reliable persons, police and counselors. Information should flow in many directions, contacting all the subjects involved in IPV management.
- Multiple access points. From the survivor's smartphone, and also from an internet browser, to provide access for the authorized people involved.
- Privacy, security, integrity. The previous point requires that the privacy and security of the survivor needs to be insured, since personal data is processed and survivor safety is at stake. This is a critical point that requires special attention.

- User-oriented environment. Taking into account all these ideas, it should not be forgotten that the IPV survivor will be the final user, so a proper interface is essential to create a satisfying quality of experience (usually called QoE), maintaining a good quality of service (QoS). This ICT habitat needs to be intuitive and simple, considering that some survivors could have certain disabilities, or be elderly, and enable a fast response without mistakes in the case of danger. Customizable options could also be considered.

Regarding the above, since, to the best of the authors' knowledge there is not a complete ICT-based platform for IPV management which takes into account the points previously addressed, an holistic proposal will be proposed in the next section.

7. An Holistic ICT Platform Proposal for Intimate Partner Violence (IPV) Management Based on an IoT Approach

In this section we aim to harness all the concepts and challenges identified throughout this work, in order to provide a proposal that is as complete as possible. Some previous approaches in the literature have tried to offer a holistic solution, but unfortunately there are some missing ideas in each of these works. Miriyala et al. [74] offer a smart intelligent security system, but it is not actually an IoT platform. On the contrary, it includes an emergency module and active defense systems, such as tear gas. Unfortunately, the system does not automatically detect the assault situation and the survivor needs to activate the intervention.

A complete BAN is detailed in the work of Ahir et al. [75], including not only a smartband, but also sensors for heart rate and even in the footwear to activate an intervention if an assault is taking place. It is also able to send a survivor's location and activates a sound alarm. The idea of an IoT environment is partially used here. In any case, other interventions are not considered, however, in areas such as the home, work, social media, and so on.

Some of the proposals already reported [30,31] include smartbands and biosensors arranged in a BAN over the survivor's body, gathering information to the cloud and building a real IoT environment with real-time monitoring. Some, however, do not include the ML potential [30], and others do so only partially [31], trying to anticipate risky situations. Seth et al. [76] offer a fairly complete solution, adding the potential of the electroencephalogram (EEG) to survivor monitoring, using a hidden Markov model which enhances the proposal. The information flow between modules and devices is structured in layers. Unfortunately, other potential areas (social media, home, tele assistance with ITC issues, etc.) are not considered.

The so-called 'layers deployment' is a common approach in IoT environments and can be found in several areas, such as e-health platforms [16]. We propose an ICT-based platform for the management of IPV situations, as shown in Figure 1, and detailed as follows:

- *Substrate*. This is the layer where data is generated, that is, the real source of information, and this is where the inception of the data occurs. Here we distinguish three areas: (1) Cyberspace: social networks and daily use of internet; (2) Environment monitoring (work/home); and, (3) Biological substrate: the physical survivor's status.
- *Sensorization layer*. Data is acquired via applications, sensors and biosensors, all connected to an IoT framework. It can be configured and controlled remotely through the internet, creating a technological structure. (1) Cyberspace: here we use software that intercepts writing, video and audio, either received by the survivor or self-generated, for monitoring; (2) Environment monitoring (work/home): using the domotic resources detailed; and, (3) Biological substrate: using biosensors which monitor physical changes. It should be remembered that if a court deems it appropriate, these resources could be extended to the offender.
- *Communication layer.* The aim here is data permeation in preparation for the next stage. Using wireless communications such as Wi-Fi, 4G/5G, ZigBee (or 6LowPAN) and Bluetooth connections,

information is sent to a more capable smart device (smartphone) which collects the data and acts as a gateway. Following the IoT idea, this layer sends communications to the cloud.

- *Middleware layer*. As we are working with different biosensors, domotic sensors, and also capturing software, a middleware mediator is required to transform and unite all the data sources.
- *Computing and management layer*. In this layer, the data collected is managed in order to carry out a data analysis, which could be text/voice/image/video recognition in order to identify harassment, but also to forecast and then anticipate risky situations and assaults. This task should be carried out in the cloud by powerful servers, as the ML algorithms used can be very demanding in terms of computer resources. Ubiquitous computing can therefore be used to enhance the process and achieve a faster solution.
- *Display layer (interface)*. Access to the system will be via a friendly browser, in order to check information, adjust user preferences but also to launch the alarm if under an attack. It is thus possible to use not only a smartphone to display the interface, but also a desktop computer. This way, not only the survivor, but also the police and emergency services can gain access in case of alarm, and also a trusted person who can check that the survivor is out of risk.
- *Output*. We can consider several outputs of the management system, depending on the situation. The platform simply check the survivor's status, study possible risk situations to enhance the ML forecasting algorithm, and of course, manage a risky situation with the cooperation of security forces, medical services, and remote tele-assistance in ICT areas.

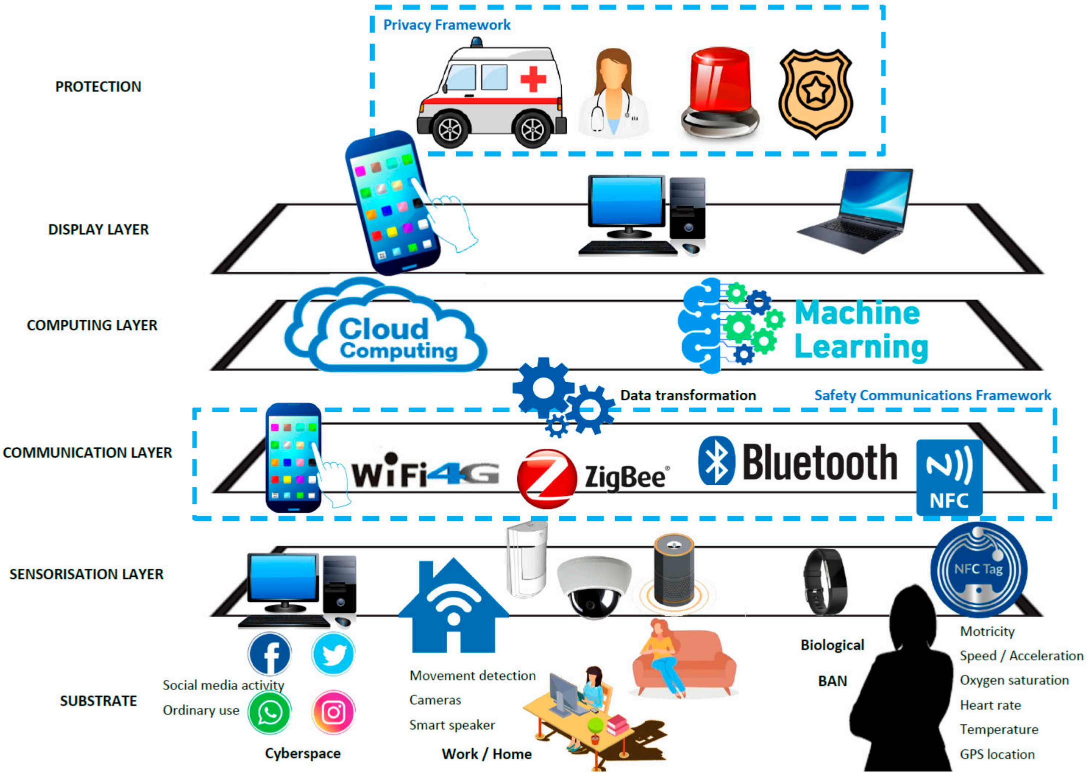

Figure 1. Proposed Internet of Things (IoT) layered structure.

The proposed platform above makes it possible to obtain:

- Continuous knowledge of the status of the survivor and, if necessary, of the offender. In this way, and using GPS location, it is possible to avoid their accidental meeting. It can provide help in terms of emergency situations but also in routine tasks.

- Emergency management. A comprehensive management system must be ready to deal with a risky situation. GPS would show the exact point where an assault has taken place; biosignals would suggest the survivor's status, etc., and the coordinated action of resources.
- Easy exchange of information. Between the survivor and police, healthcare professionals, trusted person, and all people involved in managing IPV.

The flow of data in the proposed ICT platform can be seen in Figure 2. There is a local gateway (smartphone) that is connected to the internet via 4G or through domestic Wi-Fi. The data is stored in a data warehouse on the internet, and where ML algorithms extract knowledge. The smartphone has to be reliable in establishing and managing connections with all the devices. Finally, by using several methods of communication (BLE is a good candidate, but 6LoWPAN, NFC, and so on can also be used), an exchange of data becomes possible.

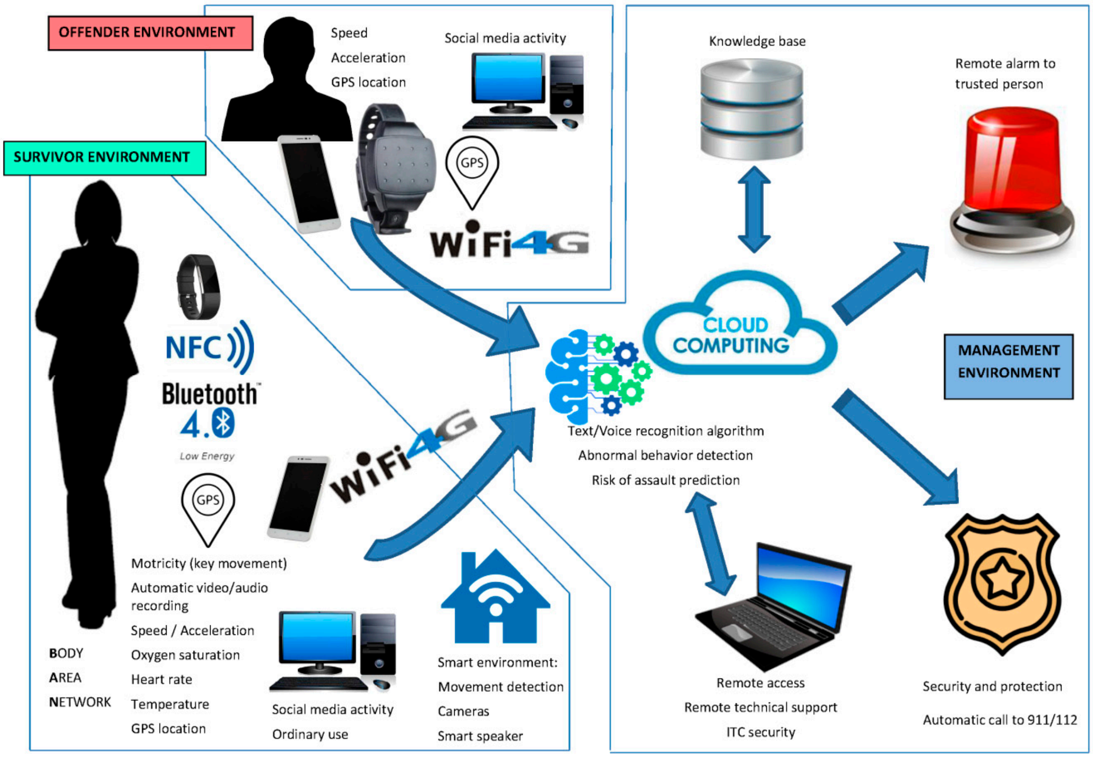

Figure 2. Diagram of the data flows.

8. Conclusions

When it comes to living in a high-technology society such as ours, the limits between real life and cyberspace are fuzzy. Human behaviors are reproduced in virtual life, and sexual harassment often begins in the real world and continues in social media, or vice versa. These issues are particularly common in IPV situations. An offender intends to control and manage all aspects of a survivor's life, and that includes virtual environments, and also using technology to harass the survivor in real life.

We have shown that ICT has multiple resources to care for survivors every minute, everywhere. In this sense, a holistic ICT-based platform for IPV management and prevention—based on the IoT paradigm—has been presented. The idea of continuous observation has been strongly developed in areas such as health, work places, homes, and also sports and other recreational uses. These applications can be transferred to another areas, such as security, and especially an IPV survivor's security and support.

Novel paradigms are emerging in almost every part of our life, causing massive revolutions in every single space: this is true for IoT and ML techniques. In fact, these two archetypes complement each other. The former results in multiple access, huge amounts of data, and is linked to the idea of small, affordable, simple devices. The latter brings the concepts of knowledge, intelligence, and inference of skills. Both, in combination with the cloud concept, result in ubiquity and permanent computing. These revolutionary ideas should be adopted in IPV management.

It is clear that there are many approaches using IoT to monitor a survivor's vital signs, but there are few that apply IoT to IPV protection in the work place, or at home. In this sense, the possibilities that allow domotics, long used in the field of energy saving, and also for home security, have not yet been concretely applied to IPV survivor safety. Voice recognition in smart speakers could also detect risky situations, and cameras and motion detectors can assure survivors that their home has not been assaulted.

Some software applications, many of which rely on ML algorithms, have a residual presence in IPV management. Text recognition has been used to detect hate speech in social media, but it can also be used in survivor's devices to warn about possible harassment.

On the other hand, the offender is a part of the equation that also requires the adoption of measures, and some of those presented in this paper could be adapted to control his behavior (of course, as this is a restriction on privacy and other rights, this has to be settled by a judge). GPS trackers are well known and used in many countries, but other tools such as software monitoring systems to follow social media and smartphone activities are not regularly included and could be added to a complete ICT platform for IPV prevention and management.

In conclusion, in the authors' opinion, the target must be to achieve a holistic solution. The proper integration of all these approaches could lead to a multi-strategy proposal that could improve IPV survivor safety and contribute to the end of the scourge of this kind of violence.

Future work needs to follow this comprehensive view and make real progress in an integrated way in order to manage IPV.

Author Contributions: Conceptualization, I.R.-R. and J.-V.R.; methodology, A.E.-M.; formal analysis, J.-V.R.; investigation, I.R.-R.; resources, P.H.-G. and M.G.; writing—original draft preparation, I.R.-R., P.H.-G. and M.G.; writing—review and editing, J.-V.R. and A.E.-M.; supervision, A.E.-M.; project administration, J.-V.R. and I.R.-R.; funding acquisition, I.R.-R., J.-V.R. and A.E.-M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: Authors would like to thank the Instituto Universitario de Estudios de Género of Universidad de Alicante (Spain) for its support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Devries, K.M.; Mak, J.Y.; Garcia-Moreno, C.; Petzold, M.; Child, J.C.; Falder, G.; Pallitto, C. The global prevalence of intimate partner violence against women. *Science* **2013**, *340*, 1527–1528. [CrossRef] [PubMed]
2. Heras, P.; Padilla, M.J. Contra la violencia, la formación en igualdad. *Isonomía. Elimin. Obs. Para Alcanzar La Igual.* **2014**, *3*, 79–95.
3. Hyman, I.; Forte, T.; Mont, J.D.; Romans, S.; Cohen, M.M. Help-seeking rates for intimate partner violence (IPV) among Canadian immigrant women. *Health Care Women Int.* **2006**, *27*, 682–694. [CrossRef] [PubMed]
4. West, C.M.; Kantor, G.K.; Jasinski, J.L. Sociodemographic predictors and cultural barriers to help-seeking behavior by Latina and Anglo American battered women. *Race Crime Justice A Reader* **2005**, *1*, 161–173. [CrossRef]
5. Dimond, J.P.; Fiesler, C.; Bruckman, A.S. Domestic violence and information communication technologies. *Interact. Comput.* **2011**, *23*, 413–421. [CrossRef]
6. Tully, J.; Larkin, F.; Fahy, T. New technologies in the management of risk and violence in forensic settings. *CNS spectrums* **2015**, *20*, 287–294. [CrossRef]
7. Haraway, D. A manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s. *Fem. /Postmod.* **1990**, 190–233.
8. Box, S.; West, J.K. Economic and social benefits of internet openness. *OECD Digit. Econ. Ser.* **2016**, *257*, 101–110. [CrossRef]

9. Henry, N.; Powell, A. Technology-facilitated sexual violence: A literature review of empirical research. *Trauma Violence Abus.* **2018**, *19*, 195–208. [CrossRef]
10. Woodlock, D. The abuse of technology in domestic violence and stalking. *Violence Against Women* **2017**, *23*, 584–602. [CrossRef]
11. Machimbarrena, J.; Calvete, E.; Fernández-González, L.; Álvarez-Bardón, A.; Álvarez-Fernández, L.; González-Cabrera, J. Internet risks: An overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming and problematic internet use. *Int. J. Environ. Res. Public Health* **2018**, *15*, 2471. [CrossRef] [PubMed]
12. Snyder, P.; Doerfler, P.; Kanich, C.; McCoy, D. Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In Proceedings of the 2017 Internet Measurement Conference, London, UK, 1–3 November 2017; pp. 432–444.
13. Carvin, A. Mind the Gap: The Digital Divide as the Civil Rights Issue of the New Millennium. *Multimed. Sch.* **2000**, *7*, 56–58.
14. Joiner, R.; Stewart, C.; Beaney, C. Gender digital divide. In *The Wiley Handbook of Psychology, Technology, and Society*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2015; pp. 74–88.
15. Gray, T.J.; Gainous, J.; Wagner, K.M. Gender and the digital divide in Latin America. *Soc. Sci. Q.* **2017**, *98*, 326–340. [CrossRef]
16. Kavitha, M.; Sivachidambaranathan, V. Women Self Protecting System Using Internet of Things. In Proceedings of the 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 13–15 December 2018; pp. 1–4.
17. Rodríguez-Rodríguez, I.; Zamora-Izquierdo, M.Á.; Rodríguez, J.V. Towards an ICT-based platform for type 1 diabetes mellitus management. *Appl. Sci.* **2018**, *8*, 511. [CrossRef]
18. Bryant, R.; Katz, R.H.; Lazowska, E.D. *Big-data Computing: Creating Revolutionary Breakthroughs in Commerce, Science and Society*; New York Times: New York, NY, USA, 2008.
19. Ye, L.; Wang, L.; Wang, P.; Ferdinando, H.; Seppänen, T.; Alasaarela, E. Physical Violence Detection with Movement Sensors. In Proceedings of the International Conference on Machine Learning and Intelligent Communications, Hangzhou, China, 6–8 July 2018; pp. 190–197.
20. Elbasiony, R.; Gomaa, W. A Survey on Human Activity Recognition Based on Temporal Signals of Portable Inertial Sensors. In *International Conference on Advanced Machine Learning Technologies and Applications*; Springer: Cham, Switzerland, 2019; pp. 734–745.
21. Nakano, K.; Chakraborty, B. Effect of dynamic feature for human activity recognition using smartphone sensors. In Proceedings of the 2017 IEEE 8th International Conference on Awareness Science and Technology, (iCAST), Taiwan, 8 November 2017; pp. 539–543.
22. Alruban, A.; Alobaidi, H.; Clarke, N.; Li, F. Physical activity recognition by utilising smartphone sensor signals. In Proceedings of the 8th International Conference on Pattern Recognition Applications and Methods, Prague, Czech Republic, 19–21 February 2019; pp. 342–351.
23. Populi, C.A.; Huela, M.E.; Ilagan, J.P.; Noble, C. On a Touch-Activated Wearable Device with Automated Location Sending Capability. *Proc. Eng. Technol. Innov.* **2018**, *9*, 38.
24. Hussain, S.M.; Nizamuddin, S.A.; Asuncion, R.; Ramaiah, C.; Singh, A.V. Prototype of an intelligent system based on RFID and GPS technologies for women safety. In Proceedings of the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 387–390.
25. Islam, M.N.; Promi, N.T.; Shaila, J.M.; Toma, M.A.; Pushpo, M.A.; Alam, F.B.; Khaledur, S.N.; Alam, T.T.; Anannya, M.F. SafeBand: A Wearable Device for the Safety of Women in Bangladesh. In Proceedings of the 16th International Conference on Advances in Mobile Computing and Multimedia, Yogyakarta, Indonesia, 19–21 November 2018; pp. 76–83.
26. Ferdinando, H.; Ye, L.; Seppänen, T.; Alasaarela, E. Emotion recognition by heart rate variability. *Aust. J. Basic Appl. Sci.* **2014**, *8*, 50–55.
27. Ferdinando, H.; Ye, L.; Han, T.; Zhang, Z.; Sun, G.; Huuki, T.; Alasaarela, E. Violence detection from ECG signals: A preliminary study. *J. Pattern Recognit. Res.* **2017**, *12*, 7–18. [CrossRef]
28. Broens, T.; Van Halteren, A.; Van Sinderen, M.; Wac, K. Towards an application framework for context-aware m-health applications. *Int. J. Internet Protoc. Technol.* **2007**, *2*, 109–116. [CrossRef]

29. Yuce, M.R. Implementation of wireless body area networks for healthcare systems. *Sens. Actuators A Phys.* **2010**, *162*, 116–129. [CrossRef]
30. Monisha, M.; Mohan, P.S. A novel IOT based approach to establish an ultra-low power self security system. In Proceedings of the 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 18 March 2017; pp. 1–6.
31. Shaik, K.; Bogaraju, S.; Vadepu, S. Implementation of Novel Application for Woman and Child Protection Using IOT Enabled Techniques. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 227–242.
32. Jatti, A.; Kannan, M.; Alisha, R.M.; Vijayalakshmi, P.; Sinha, S. Design and development of an IOT based wearable device for the safety and security of women and girl children. In Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bengaluru, India, 20–21 May 2016; pp. 1108–1112.
33. Mavromoustakis, C.X.; Mastorakis, G.; Batalla, J.M. (Eds.) *Internet of Things (IoT) in 5G Mobile Technologies*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 8.
34. Gomez, C.; Oller, J.; Paradells, J. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors* **2012**, *12*, 11734–11753. [CrossRef]
35. Hoy, M.B. Alexa, Siri, Cortana, and more: An introduction to voice assistants. *Med Ref. Serv. Q.* **2018**, *37*, 81–88. [CrossRef] [PubMed]
36. Bergen, H. 'I'd blush if I could': Digital assistants, disembodied cyborgs and the problem of gender. *Word Text J. Lit. Stud. Linguist.* **2016**, *6*, 95–113.
37. Vora, J.; Tanwar, S.; Tyagi, S.; Kumar, N.; Rodrigues, J.J. Home-based exercise system for patients using IoT enabled smart speaker. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017; pp. 1–6.
38. Huang, W.; Chiew, T.K.; Li, H.; Kok, T.S.; Biswas, J. Scream detection for home applications. In Proceedings of the 2010 5th IEEE Conference on Industrial Electronics and Applications, Taichung, Taiwan, 15 June 2010; pp. 2115–2120.
39. Peng, Z.; Kato, T.; Takahashi, H.; Kinoshita, T. Intelligent home security system using agent-based IoT Devices. In Proceedings of the 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan, 27–37 October 2015; pp. 313–314.
40. Domestic-abuse-violence-harassment-smart-home-monitoring. Available online: https://www.refinery29.com/en-ca/2019/01/220847/ (accessed on 15 August 2019).
41. Beyens, K.; Roosen, M. Suspects being watched in real time: Introducing GPS tracking in Belgium. *J. Technol. Human Serv.* **2016**, *34*, 102–116. [CrossRef]
42. Gies, S.; Gainey, R.; Healy, E. Monitoring high-risk sex offenders with GPS. *Crim. Justice Stud.* **2016**, *29*, 1–20. [CrossRef]
43. Payne, B.K.; DeMichele, M. Sex offender policies: Considering unanticipated consequences of GPS sex offender monitoring. *Aggress. Viol. Behav.* **2011**, *16*, 177–187. [CrossRef]
44. Islam, A.; Akter, A.; Hossain, B.A. *HomeGuard:* A Smart System to Deal with the Emergency Response of Domestic Violence Victims. *arXiv* **2018**, arXiv:1803.09401.
45. Ye, L.; Ferdinando, H.; Seppanen, T.; Huuki, T.; Alasaarela, E. An instance-based physical violence detection algorithm for school bullying prevention. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 24–28 August 2015. [CrossRef]
46. Hegde, N.; Bries, M.; Swibas, T.; Melanson, E.; Sazonov, E. Automatic recognition of activities of daily living utilizing insole-based and wrist-worn wearable sensors. *IEEE J. Biomed. Health Inform.* **2017**, *22*, 979–988. [CrossRef]
47. O'Halloran, K.L.; Tan, S.; Wignell, P.; Bateman, J.A.; Pham, D.S.; Grossman, M.; Moere, A.V. Interpreting text and image relations in violent extremist discourse: A mixed methods approach for big data analytics. *Terror. Polit. Violence* **2019**, *31*, 454–474. [CrossRef]
48. Ozkan, T. Predicting Recidivism Through Machine Learning. Ph.D. Thesis, University of Texas and Dallas, Richardson, TX, USA, 2017.
49. Ward-Lasher, A.; Sheridan, D.J.; Glass, N.E.; Messing, J.T. Prediction of Interpersonal Violence: An Introduction. *Assess. Danger. Domest. Violence Offenders Child Abus.* **2017**, *1*, 1–32.
50. Berk, R.A.; Sorenson, S.B.; Barnes, G. Forecasting domestic violence: A machine learning approach to help inform arraignment decisions. *J. Emp. Leg. Stud.* **2016**, *13*, 94–115. [CrossRef]

51. García Revilla, M.R. El impacto de las APPS en la violencia de género. *Asparkía: Investigació Feminista* **2016**, *28*, 159–160.
52. Mareeswari, V.; Patil, S.S. Smart Device for Ensuring Women Safety Using Android App. In *Advanced Computational and Communication Paradigms*; Springer: Singapore, 2018; pp. 186–197.
53. Purohit, H.; Banerjee, T.; Hampton, A.; Shalin, V.L.; Bhandutia, N.; Sheth, A.P. Gender-based violence in 140 characters or fewer: A BigData case study of Twitter. *arXiv* **2015**, arXiv:1503.02086. [CrossRef]
54. Del Vigna, F.; Cimino, A.; Dell'Orletta, F.; Petrocchi, M.; Tesconi, M. Hate me, hate me not: Hate speech detection on facebook. In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy, 17–20 January 2017.
55. Hassija, C.; Gray, M.J. The effectiveness and feasibility of videoconferencing technology to provide evidence-based treatment to rural domestic violence and sexual assault populations. *Telemed.e-Health* **2011**, *17*, 309–315. [CrossRef] [PubMed]
56. Kortendiek, B. Supporting the Bologna process by gender mainstreaming: A model for the integration of gender studies in higher education curricula. Studies on Higher Education. In *From Gender Studies to Gender IN Studies and beyond*; UNESCO-CEPES: Bucharest, Romania, 2011.
57. Nanjo, H.; Nishiura, T.; Kawano, H. Acoustic-based security system: Towards robust understanding of emergency shout. In Proceedings of the 2009 Fifth International Conference on Information Assurance and Security IEEE, Xian, China, 18–20 August 2009; Volume 1, pp. 725–728.
58. Viswanath, N.; Pakyala, N.V.; Muneeswari, G. Smart foot device for women safety. In Proceedings of the 2016 IEEE Region 10 Symposium (TENSYMP) IEEE, Bali, Indonesia, 9–11 May 2016; pp. 130–134.
59. Harikiran, G.C.; Menasinkai, K.; Shirol, S. Smart security solution for women based on Internet of Things(IOT). In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques, Chennai, India, 3–5 March 2016; pp. 3551–3554.
60. Toney, G.; Jabeen, F.; Puneeth, S. Design and implementation of safety armband for women and children using ARM7. In Proceedings of the 2015 International Conference on Power and Advanced Control Engineering (ICPACE) IEEE, Piscataway, NJ, USA, 12–24 August 2015; pp. 300–303.
61. Mohanaprakash, K.; Sekar, T.G. A Smart Alarm System for Women's Security. *Int. J. Eng. Manag. Res. (IJEMR)* **2018**, *8*, 89–92.
62. Li, N.; Sun, M.; Bi, Z.; Su, Z.; Wang, C. A new methodology to support group decision-making for IoT-based emergency response systems. *Inf. Syst. Front.* **2014**, *16*, 953–977. [CrossRef]
63. Yu, S.; Wang, G.; Liu, X.; Niu, J. Security and privacy in the age of the smart internet of things: An overview from a networking perspective. *IEEE Commun. Mag.* **2018**, *56*, 14–18. [CrossRef]
64. Chiang, M.; Zhang, T. Fog and IoT: An overview of research opportunities. *IEEE Internet Things J.* **2016**, *3*, 854–864. [CrossRef]
65. Machanavajjhala, A.; Gehrke, J.; Kifer, D.; Venkitasubramaniam, M. l-diversity: Privacy beyond k-anonymity. In Proceedings of the 22nd International Conference on Data Engineering (ICDE'06), Atlanta, GA, USA, 14 April 2006; p. 24.
66. Kshetri, N. Can blockchain strengthen the internet of things? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
67. Lim, H.B.; Teo, Y.M.; Mukherjee, P.; Lam, V.T.; Wong, W.F.; See, S. Sensor grid: Integration of wireless sensor networks and the grid. In Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05), Sydney, Australia, 15–17 November 2005; pp. 91–99.
68. Talpur, M.S.H.; Bhuiyan, M.Z.A.; Wang, G. Energy-efficient healthcare monitoring with smartphones and IoT technologies. *Int. J. High Perform. Comput. Netw.* **2015**, *8*, 186–194. [CrossRef]
69. Omre, A.H.; Keeping, S. Bluetooth low energy: Wireless connectivity for medical monitoring. *J. Diabetes Sci. Technol.* **2010**, *4*, 457–463. [CrossRef] [PubMed]
70. Jara, A.J.; Lopez, P.; Fernandez, D.; Zamora, M.A.; Ubeda, B.; Skarmeta, A.F. Communication protocol for enabling continuous monitoring of elderly people through near field communications. *Interact. Comput.* **2013**, *26*, 145–168. [CrossRef]
71. Claudio, D.; Velázquez, M.A.; Bravo-Llerena, W.; Okudan, G.E.; Freivalds, A. Perceived usefulness and ease of use of wearable sensor-based systems in emergency departments. *IIE Trans. Occup. Ergon. Hum. Factors* **2015**, *3*, 177–187. [CrossRef]

72. Motti, V.G.; Caine, K. Human factors considerations in the design of wearable devices. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Chicago, IL, USA, 27–31 September 2014; Volume 58, pp. 1820–1824.
73. Finn, J.; Atkinson, T. Promoting the safe and strategic use of technology for victims of intimate partner violence: Evaluation of the technology safety project. *J. Fam. Violence* **2009**, *24*, 53–59. [CrossRef]
74. Miriyala, G.P.; Sunil, P.V.V.N.D.P.; Yadlapalli, R.S.; Pasam, V.R.L.; Kondapalli, A.T.; Miriyala, A. Smart intelligent security system for women. *Int. J. Electron. Commun. Eng. Technol. (IJECET)* **2016**, *7*, 41–46.
75. Ahir, S.; Kapadia, S.; Chauhan, J.; Sanghavi, N. The Personal Stun-A Smart Device for Women's Safety. In Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 5 January 2018; pp. 1–3.
76. Seth, D.; Chowdhury, A.; Ghosh, S. A Hidden Markov Model and Internet of Things Hybrid Based Smart Women Safety Device. In Proceedings of the 2018 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE), Shillong, India, 1–2 June 2018; pp. 1–9.