electronics

MDPI

Review

Quality of Life, Quality of Experience, and Security Perception in Web of Things: An Overview of Research Opportunities

Sabina Barakovi ć [1,2,*], Jasmina Barakovi ć Husi ć [3], Dardan Maraj [4], Arianit Maraj [5], Ondrej Krejcar [6], Petra Maresova [6] and Francisco Jose Melero [7,8]

1 Faculty of Transport and Communications, University of Sarajevo, Zmaja od Bosne 8, 71000 Sarajevo, Bosnia and Herzegovina
2 American University in Bosnia and Herzegovina, Zmaja od Bosne 8, 71000 Sarajevo, Bosnia and Herzegovina
3 Faculty of Electrical Engineering, University of Sarajevo, Zmaja od Bosne bb, 71000 Sarajevo, Bosnia and Herzegovina; jbarakovic@etf.unsa.ba
4 Faculty of Electrical Engineering and Computing, University of Zagreb, Unska 3, 10000 Zagreb, Croatia; dardan.maraj@fer.hr
5 Faculty of Computer Sciences, AAB University, Rr. Elez Berisha, Nr.56 10000 Prishtinë, Kosovo; arianit.maraj@universitetiaab.com
6 Faculty of Informatics and Management, University of Hradec Kralove, Rokitanskeho 62, 500 03 Hradec Kralove, Czech Republic; ondrej.krejcar@uhk.cz (O.K.); petra.maresova@uhk.cz (P.M.)
7 Technical Research Centre of Furniture and Wood of the Region of Murcia, C/Perales S/N, 30510 Yecla, Spain; fj.melero@cetem.es
8 Telecommunication Networks Engineering Group, Technical University of Cartagena, 30202 Cartagena, Spain
* Correspondence: barakovic.sabina@gmail.com

Received: 15 April 2020; Accepted: 21 April 2020; Published: 24 April 2020

Abstract: The Web of Things (WoT) is a technology concept that allows the integration of the Internet of Things (IoT) with the World Wide Web (WWW). It will vastly affect our lives in the near future given that it offers new services and applications via the well-known web window. In todays' world where one can hardly imagine everyday life without access to various online services and applications via a plethora of devices, one can notice that technology has a huge impact on our day-to-day quality of living. That is why a user's Quality of Experience (QoE) towards used technology in general plays a crucial role in their Quality of Life (QoL). Furthermore, security perception in terms of technology is the feature that vastly affects QoE and, consequently, QoL, as the number of security and privacy threats, risks, and vulnerabilities in cyber space, i.e., the technology environment that we increasingly use, is constantly rising. In order to reach the ultimate goals—the adoption of WoT technology and improvement of our QoL—we must know how this important aspect of security is so far addressed and analyzed. Therefore, this paper gives a comprehensive and structured analysis of the existing literature in this field through a proposed framework and provides an overview of research opportunities that should be addressed and elaborated in future investigations.

Keywords: quality of experience; quality of life; security perception; web of things

1. Introduction

With the development of new technologies, billions of devices are getting connected to the Internet. It is expected that by 2021 the number of devices on the Internet will exceed 70 billion [1]. As the number of devices connected to the network increases every day, the next step is to use World Wide Web (WWW) and its protocols as a platform for smart things (e.g., sensors, actuators, embedded

devices, etc.) These smart things can be discussed through the concept of the Internet of Things (IoT), which defines a set of smart objects connected to network, where each device is identified uniquely embedded in the infrastructure. The related notion to the IoT is the Web of Things (WoT).

The WoT is considered as a platform which enables the connection of smart objects in both network and application layers [2,3], so it can be used for creation of IoT applications [4–10]. Things in the WoT are not limited to devices that are interconnected, but can also include things that are not connected, such as people and places, ideas, different organizations, etc. There are many use cases where the WoT is being used. One of these is the smart cities [11].

WoT differs from IoT in some aspects. The main difference is that WoT describes approaches and programming patterns that allow real-world objects to be part of the WWW, while IoT creates a network of objects, things, people, and so on. The WoT use cases have the right to lay down the basic requirements for connectivity and functionality of interconnected devices. However, security is a central issue in such environments. Allowing the information to be available on the web can pose numerous security threats. The exposure and sharing of the information is always contradictory to security and privacy. Therefore, despite the differences between the IoT and WoT, the WoT inherits all of the specific properties of the IoT, as well as many security and privacy issues. In addition, it has the same relation with the WWW.

These are very serious problems in the architecture of the IoT and WoT which require the following of the concept of "security and privacy by design". This concept is used in several projects (e.g., RERUM, SMARTIE, SocioTal, etc.) [12] to develop a framework which will allow IoT applications to consider security and privacy mechanisms early in their design phase. In addition, there is European IoT Security and Privacy Projects initiative (IoT-ESP) addressing advanced end-to-end security and privacy in heterogeneous IoT environments [13]. The final goal is to allow the IoT to become the enabler of various Smart City applications, following the user-centric approach. Without guarantees that Smart City IoT addresses many security and privacy issues, users are unwilling to adopt this new technology that will be the part of their everyday life [14]. This means that security and privacy are important for broader adoption of the IoT applications requiring security certification due to the presence of a wide range of vulnerabilities and the dynamic environment where IoT is used [15].

Therefore, if users can be sure that WoT will not damage them, violate their privacy or negatively influence their lives, i.e., if they have good perception of WoT security, only then can the full potential of it be used to improve their everyday life. A user's quality of experience (QoE), expectations, perceptions, and needs with respect to technology is what matters today and determines, on one hand, the adoption of the technology, and, on the other hand, contributes to their quality of life (QoL).

In sense of said, this paper aims to timely address and discuss the relationships and interplay between QoL, QoE, security perception, and influence factors affecting security perception. The ultimate goal is to contribute to the improvement of QoL of individuals who will increasingly use the WoT in a security challenged future by listing the issues that need to be addressed in future investigations. We will reach that goal by reviewing the existing literature that tackles the impacts of: (i) QoE on QoL, (ii) security perception on QoE, and (iii) influence factors on security perception, all in the context of WoT, but also IoT and WWW given that WoT inherits their characteristics. One of the main motives behind this approach is to provide a structured overview of findings which can further be utilized by the whole spectrum of interested parties.

The paper is organized as follows: after the introductory section, in Section 2 we provide a theoretical background of QoL, QoE, and security perception, as well as their dependencies in the WoT. Section 3 describes the used research methodology. Section 4 explains the impact matrices between QoL, QoE, and security perception in a given context based on the existing papers. In addition, this section gives the overview of the existing literature addressing system, human, and context influence factors affecting security perception. Key findings together with the limitations of this survey study are provided in Section 5, while Section 6 concludes the paper.

2. Theoretical Background

2.1. Definitions of QoL, QoE, and Security Perception

QoL [16] has many different definitions that depend on the disciplines in which they are considered. For example, one given by the World Health Organization (WHO) is as follows: "Quality of life is a perception of one's position in life in the context of the culture and value systems in which they live an in relation to their goals, expectations, standards, and concerns." Indisputably, QoL is multidimensional in nature and represents the enjoyment of life or the state of mind which results from complex effects of combination of individual's perception of many components present in one's everyday life. The World Health Organization Quality of Life (WHOQOL) [17] Group has proposed four QoL domains, i.e., physical health, psychological, social relations, and environment, together with subjective and objective facets such as social support, transport, mobility, etc. incorporated within those domains [18]. Additionally, Eurostat offers nine QoL dimensions (8+1): material living conditions, health, education, productive and valued activities, governance and basic rights, leisure and social interactions, natural and living environment, economic and physical safety, and overall experience of life [19].

All these dimensions or domains, regardless of terms, strongly rely on technology today, while that bond will be even tighter in the upcoming smart period. The WoT, on one side, will help counter the problem of IoT fragmentation by using web standards, but it will also give the web eyes, ears and all kinds of sensory appendices located anywhere on earth. It is about upcoming seamless connection of the physical and virtual world [20]. In todays' world where one hardly can imagine everyday life without access to various online services and applications via a plethora of devices together with the fact that we spend approximately seven hours online [21], one can conclude that technology has a huge impact on our day-to-day quality of living. That is why now QoE towards used technology in general plays a crucial role in one's QoL.

QoE has several definitions in the literature, yet not an exact one, especially in the context of QoL. The latest given by [22], defines QoE as "the degree of delight or annoyance of the user of an application or service. It results from the fulfilment of his or her expectations with respect to the utility and/or enjoyment of the application or service in the light of the user's personality and current state." The core idea behind QoE is that it represents a multidimensional construct which is a result of multiple perceptual QoE dimensions interaction. **Perceptual QoE dimensions** refer to: "a perceivable, recognizable, and nameable characteristics of the individual's experience of a service which contributes to its quality" [22]. Those dimensions such as perceived usability, aesthetics, latency, security, etc., are affected by individual impact or interplay of **QoE influence factors**, defined as "any characteristic of a user, system, service, application, or context whose actual state or setting may have influence on the QoE for the user" [22], stemming from human, system, or context domain when using certain technology.

Security perception in terms of technology is the dimension/feature that vastly affects QoE and consequently QoL, as the number of security threats, risks, and vulnerabilities in cyber space, i.e., technology environment that we increasingly use, is constantly on rise. The dependency chain between perceived security and privacy, QoE, and QoL will be explained in the next subsection.

2.2. Dependencies Between QoL, QoE, Security Perception, and Influence Factors

In order to gain a deeper understanding of interplays between QoL, QoE, and security perception in the WoT, we firstly have to understand the chain of dependencies between them. The relation is illustrated in Figure 1.

Dependencies between QoL, QoE, security perception, and influence factors can be viewed through a layered framework. The top one refers to the QoL layer and includes all previously mentioned QoL dimensions (8+1), but detailed analysis in that direction is out of the scope of this paper and should be put on a to-do list for future interdisciplinary research studies which are required for QoL. Various

QoL dimensions are affected by WoT. In other words, WoT improves the users' QoL in the public and private area in terms of different dimensions, such as leisure and social interactions, education, health, etc.

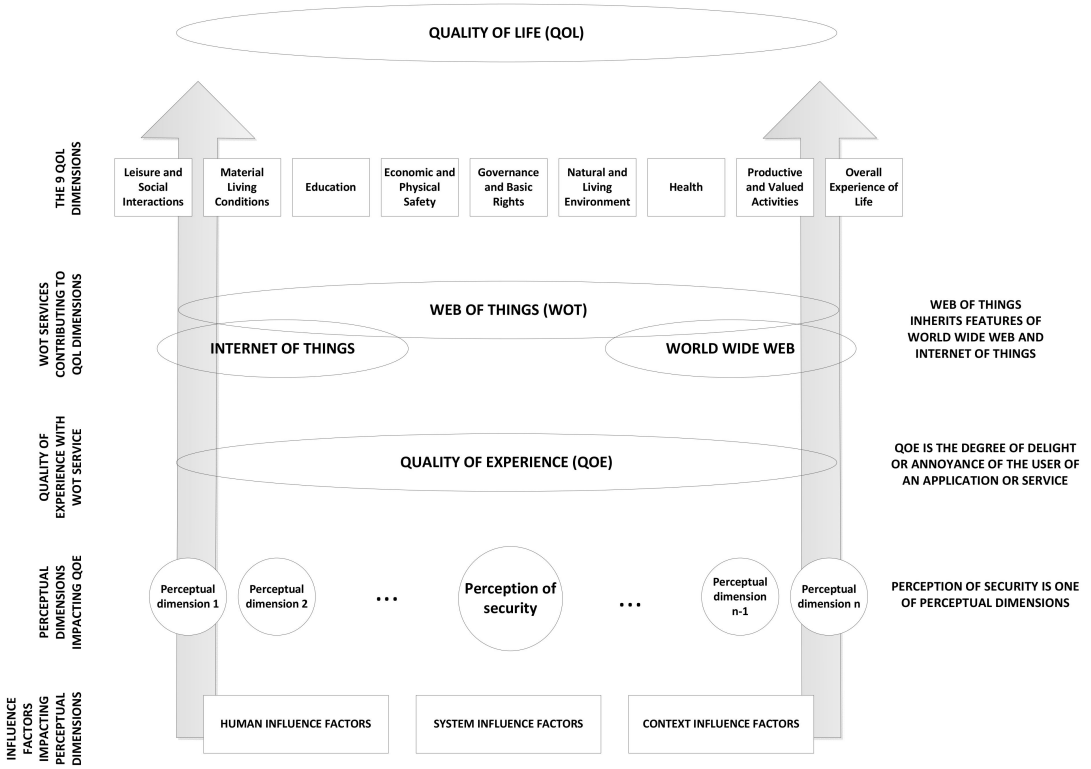

Figure 1. Dependencies between QoL, QoE, security perception, and influence factors in WoT—a layered framework.

The WoT layer is clearly related to QoE because services offered online are currently seen as a commodity and we rely on them every day in conducting activities and making decisions which affect our temporary, but also a long-term QoL. When a service is delivered with high QoE, the user takes it for granted and increasingly uses the subject service to facilitate and ease the tasks related to his or her daily communication, decision making process, entertainment, information, etc., thereby improving his or her QoL. On the other hand, if the services are not delivered at the satisfactory QoE level, user might create reserved stance and relation with the product, but also experiences negative effects in form of stress and dissatisfaction which results in current QoL level drop. Potentially, that momentary QoL fall can turn into long-term QoL decrease if the poor QoE in relation to the subject system affects outcomes of user tasks. As discussed in [23], if the individual relies on technologies to complete a task, his or her QoL can be affected negatively in two ways: (i) the QoE for a given service is constantly not at the satisfactory level thereby inducing stress and dissatisfaction, and (ii) technology fails to provide satisfactory QoE in critical conditions and then the individual does not complete the task at hand. This dependency between QoL and QoE will be more intensive in the future societies whose individuals will increasingly rely on WoT in their daily tasks. We live in an era where service providers are considered by the level at which they can affect the experience the user is perceiving—the so-called "experience economy" [23].

Having described the relation between QoL and QoE, we further move to the next layer of the framework below the QoE in Figure 1. According to the layered framework, QoE is influenced by multiple perceptual QoE dimensions represented by circles [24]. An example of those perceptual dimensions which is a central focus of this paper is security perception. All perceptual QoE dimensions, including the one that we focus on, are impacted by the cocktail of different QoE influence factors

(IFs) (previously defined) which are grouped in three classes: human influence factors (HIFs), system influence factors (SIFs), and context influence factors (CIFs). This effect is presented by three bottom squares, which are used for the qualitative and structured literature review and discussion with the aim of highlighting the areas that need increased attention on this field.

Although we address QoE from one aspect (i.e., security perception), QoE is a multidimensional concept and its consideration should encompass as many as possible perceptual QoE dimensions and QoE IFs relevant for a given service. In addition, it is important to stress that the abovementioned dependencies include the IoT and WWW services as well since, as already explained, the WoT inherits their issues and features.

3. Research Methodology

As stated earlier, the main goal of this paper is to contribute to the improvement of one's QoL in a future security-challenged WoT environment. In order to reach that goal, we need to achieve a better and more detailed understanding of relations between QoL, QoE, security perception, as well as influence factors affecting them. In order to have that understanding, we have started with gathering and analysing the literature that is concerned with the impact that various factors have on security perception and QoE, and consequently on QoL in the context of WoT, as well as mutual interplay and effects of security perception, QoE, and QoL. Afterwards, we survey and compare different studies contributing to this field.

Again, it is important to stress that we here also consider IoT and WWW (in sense of web 2.0, for example web browsing, web commerce, etc.). The justification for addressing the IoT- as well as WWW-related literature lies in the fact that the WoT is actually applying the existing and new techniques used on the WWW to the development of different innovative IoT scenarios. The WoT as a concept inherits the benefits, but also the security issues from the IoT and WWW, and therefore they need to be included.

To simplify and summarize, the main objectives on the path towards the main goal are:

1. to gain deeper understanding of the mutual dependencies between QoL, QoE, security perception, as well as influence factors in addressed context through proposed layered framework;
2. to organize and synthesize the existing research literature from the field;
3. to identify gaps and issues needed to be addressed by the future research activities and suggest novel and open investigation directions in the subject field.

Our methodology, which relies on guidelines given by authors in [25,26], is provided in Figure 2. It consists of four phases. Given the multidisciplinary nature of the addressed topic, we surveyed papers coming from both the technical sciences domain (telecommunications, computer science, electrical engineering) and the social sciences.

The methodology used in the phase I for selecting the papers was as follows. We searched relevant databases (Web of science, Scopus, and Xplore,) for papers with the following key words: quality of life, quality of experience, user experience, security, privacy, web of things, internet of things, trust, web. Then, we have identified the papers (i) addressing the impact of QoE on QoL, (ii) addressing the impact of security perception on QoE, and (iii) addressing the impact of various factors on security perception.

A total of 32 papers from Web of Science, Scopus, and Xplore databases were selected to be included in the review given their relevance to the topic. The number of selected items is as such due to several reasons. On one hand, the identification parameters were strict given that we were interested in a very specific and narrow topic (i.e., QoL, QoE, security, WoT). However, in order to include conclusions from the related research we have included the WWW and IoT as well. On the other hand, the combination of these domains that will play an important role in our future, i.e., QoL together with security in the WoT, has still not been sufficiently related, investigated, or treated. Of the search results, 59.3 % of those selected papers are journal papers, while the remaining 37.5 % are conference papers and only one material item is a report. Figure 3 gives the year distribution of the

selected papers. Initially, we researched the 20-year time span, i.e., 1999–2019, but found only relevant research in the second decade of the 21st century.

The phase II is the categorization of papers based on addressed influence on QoL, QoE, and security perception. In phase III, papers from each category were analyzed according to the selected parameters. The analysis and comparison of papers in the first category is done according to the following parameters: which QoL dimension has been addressed by QoE, which environment (WWW, IoT, or WoT), application used, and its users. Furthermore, the comparison addresses the study environment, research method, model, and type of impact. In the second category, we analyzed the same as in the previous case with difference in two first parameters. In this group of papers, we compared the works according to whether they address the impact on QoE and which security perception is addressed. The third category contains the same analysis as first and second, also with difference in two first columns. In the third category, we analyzed the studies according to which security perception they address and which influence factor they analyze. Additionally, the analysis for the third category contains statistics for each of addressed influence factors, with the aim to recognize the most and the least addressed ones. Finally, in phase IV, we extract the key findings based on a meta-analysis of collected work.

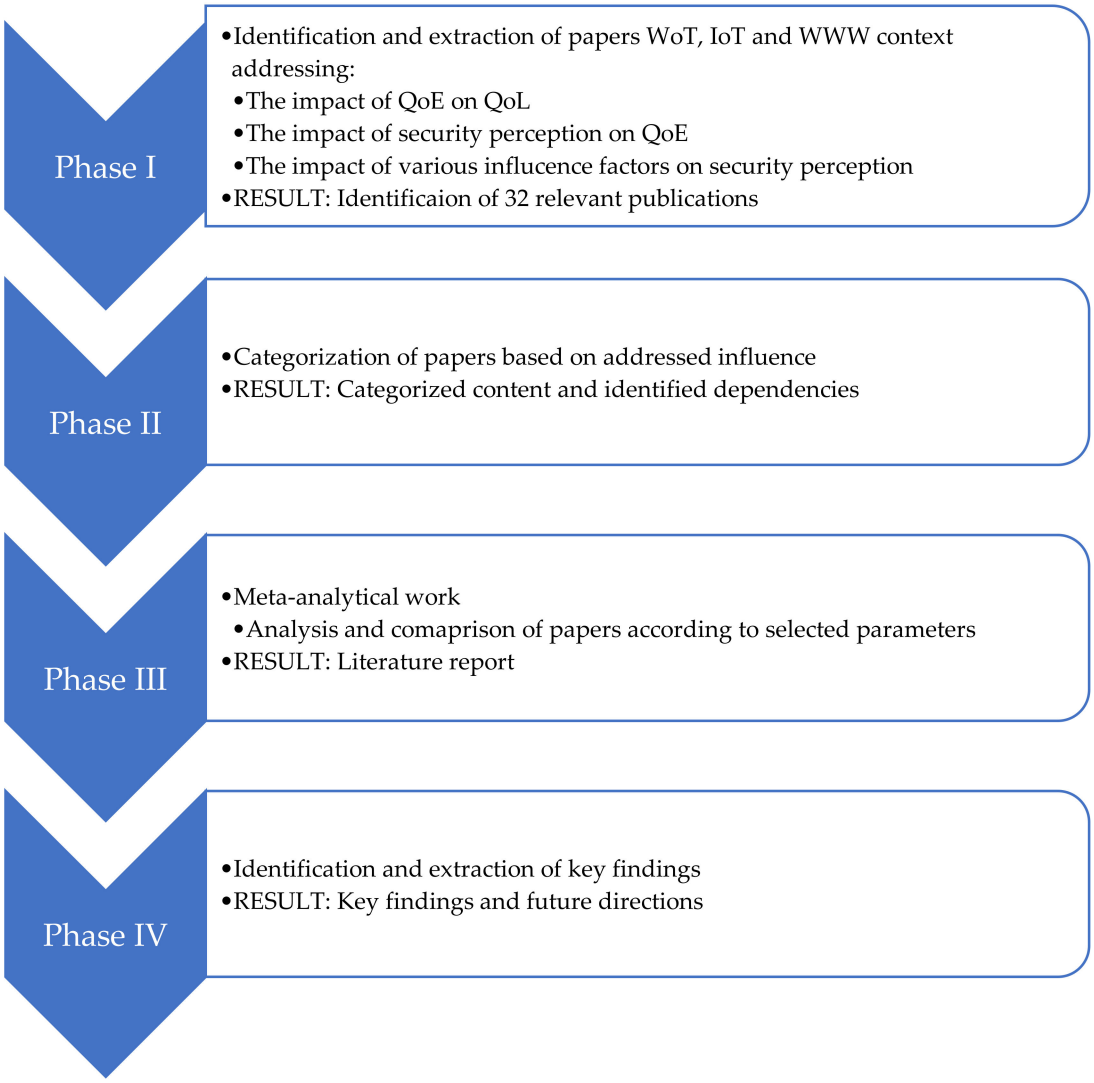

Figure 2. Phases of research methodology.

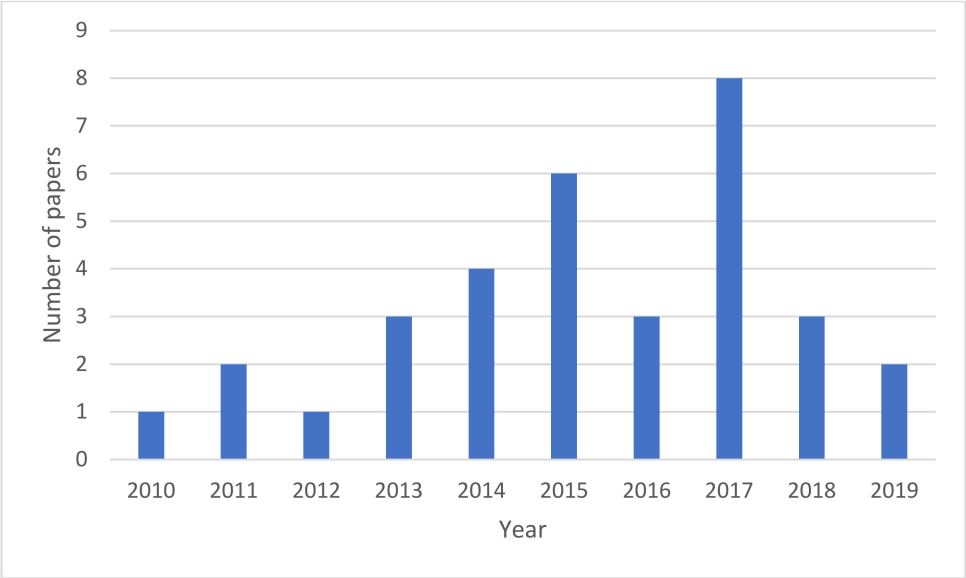

Figure 3. Distribution of selected papers by year.

4. Literature Analysis and Comparison

4.1. Impact of QoE on QoL

After having defined the framework and explained the logical dependencies between the considered terms, i.e., QoL, QoE, and security perception, as well as factors affecting them, we continue with the report of works addressing the influence of QoE on QoL in the WoT, IoT, and WWW context (phase I). The results of our literature review in this domain are given in Table A1 (Appendix A). We found only eight papers that address the subject influences, none in the WoT environment, but in the IoT and WWW (web 2.0) environment. The important finding is that the selected papers show high impact of QoE on overall experience of life (+1 QoL dimension) in IoT and WWW domains, but no other specific QoL dimension that is previously listed in the paper. Therefore, this leads to the conclusion that there is a need for studies that will address the impact of QoE on QoL and its dimensions in the WoT environment. Moreover, these relationships should be quantified and modelled.

The contribution of selected works reflects in provided models, frameworks, or optimization methods. They all provide models or frameworks either by using regression modelling by Baraković and Skorin-Kapov [27–29], formula-based estimation methods by Tsholkas et al. [30], data collection by Korhonen et al. [31], optimization techniques by Liu et al. [32], machine learning methods by Balachandran et al. [33], etc. The research environment in all considered studies is real and all age groups were addressed (i.e., young, adults, elderly), while applications that were used are mostly web browsing and multimedia IoT applications.

In general, the majority of the browsed and reviewed literature has been rejected for further consideration because they usually only mention in one sentence in the introduction section how the IoT or web QoE can improve a user's QoL in some form of smart context lacking deeper consideration of those influences [34–38].

4.2. Impact of Security Perception on QoE

Next, we move to discussion of review results in relation to the papers dealing with the impact of security perception on QoE in the WoT, IoT and WWW (web 2.0) contexts (phase I). The results of our literature review in this domain are papers given in Table A2 (Appendix B).

We only found one paper discussing security and privacy for WoT systems. Catuogno and Turchi [39] elaborate on concerns and regulatory frameworks as well as protection of the infrastructure

where they address topics such as achieving data confidentiality and integrity, trustworthiness, the quest for data privacy, omni-comprehensive identity management, flexible and fine-grained access control mechanisms. This is out of the scope of this paper, which indicates that the analysis of security perception effect on QoE in the WoT context is missing.

Further on, the comprehensive search of IoT security perception resulted in many (nearly one thousand) quality review conference and journal papers as well as book chapters dealing with IoT security and privacy such as Hwang [40], Abomhara et al. [41], Sicari et al. [42], Sadeghi et al. [43], Roman et al. [44], Maple [45], Sivaraman et al. [46], Giraldo et al. [47], Makherjee et al. [48], Yang et al. [49], Lin et al. [50], Stergiou et al. [51], Zhou et al. [52], Frustaci et al. [53], Miorandi et al. [54], Hasan et al. [55], Mawgoud et al. [56], Tabassum et al. [57], Ataç et al. [58], Silaghi et al. [59], Guan et al. [60], etc. They provide overviews of current state in this domain and provide open research challenges and issues to be solved by future research, but all that is out of the scope of this paper, i.e., they do not address the impact of security perception on QoE in the IoT environment. Therefore, they are not included in the review.

Lastly, we found several papers addressing the topics close to ones of our interest, i.e., the impact of security perception on QoE in the WWW (web 2.0) context. These papers address trust in web activities, and as stated in [61], they showed that better trust, security, and privacy positively influences consumers' online/web behavior (usually shopping and commerce) and is influenced by many factors such as risk, web security, online privacy, experience, design, etc. [62–68].

After reviewing the available literature that focuses on the impact of security perception as a QoE dimension on QoE in WoT, IoT, and WWW (web 2.0) contexts, one can conclude that the number of studies addressing it is limited and that the research community should investigate and gain deeper understanding of these impacts for the ultimate goal of providing better QoL. Moreover, these influences as well as their interplay with other (given that QoE is multidimensional concept) should be adequately modelled and quantified.

4.3. Influence Factors Affecting Security Perception

4.3.1. Impact of System Factors on Security Perception

According to [22], System IFs refer to "properties and characteristics that determine the technically produced quality of an application or service." SIFs can be classified into content-, media-, network- and device-related. Since different content characteristics require different system properties, the content has a high influence on the overall QoE. The media-related SIFs are interrelated with content-related factors and refer to the media configuration factors, such as encoding, resolution, sampling, frame rate, etc. [69,70]. The resources for media transmission are usually limited. Therefore, it is necessary to limit the size of media, using different compression techniques. SIFs are usually related with network QoS. The main parameters, which affect the network Quality of Service (QoS), are bandwidth, delay, jitter, loss, throughput, etc. Network-related SIFs are affected by errors occurring during the data transmission over the network. Whereas, the device-related factors refer to the end user devices. The capacity and the performance of the end device will affect the user experience as well.

Constante et al. [71] have analyzed the user's perception of trust in a web environment. They developed a general trust perception model that contains a set of system and human factors as well. They studied system factors, which have a great impact in the perception of security and privacy in the web environment, such as brand name, usability and look and feel of web site, privacy, reliability and availability, reputation, risk and security, as well as third party seals.

In terms of the WoT, S. El Jaouhari et al. [72] went through the currently proposed architectures for securing the WoT. They have presented the authorization frameworks that allow a fine-grained and flexible access control to the resources. In order to guarantee the integrity and confidentiality of the data, they presented two models of implementing an access control mechanism in a WoT ecosystem. The first one is a centralized model, where all the access requests go through a server that decides

either to authorize or to block the access, and the second one is a decentralized model where the device itself decides either to authorize or to block the access.

It is known that users are not only worried about QoE, but also the personal data that they share with the smart objects and other users. They prefer to have full control of their personal information and to have enough security mechanisms to protect their data. Therefore, the authors in [72] have considered some of the main system SIFs on perceived security and privacy in terms of the WoT, such as access control, authorization, encryption, identity management, buffer overflow, etc.

The WoT technology enhances the interconnection of physical devices over Internet, ergonomics, and productivity of the IoT, but it also introduces new challenges of preserving data security and privacy. Deploying existing security and privacy technologies in the WoT is not straightforward because of its potential vastness, inhomogeneity and variety of entities involved. Therefore, every solution is considered a non-trivial trade-off among different aspects including security, availability and legal issues. In this regard, authors in [39] investigated the nature of this trade-off, pointing out the different kinds of security and privacy issues. They acknowledged the promises of novel public key technologies in enabling a data-center access control by including the policy in the cypher text and different other technologies, such as Virtual Private Network (VPN), Secure Sockets Layer/Transport Layer Security (SSL/TLS), etc.

In terms of the IoT, the authors in [73] have introduced a new a new access control framework for the IoT environment, precisely the WoT approach, called "SmartOrBAC", based on the OrBAC model. They have analyzed and extended the OrBAC model in order to specify collaboration access control rules; on the other hand, these security policies are enforced by applying web services mechanisms mainly the RESTful approach. Finally, they have discussed access control in IoT environment.

Security and privacy issues in IoT environment are discussed in [74]. The authors have proposed an integrated design to manage security and privacy concerns through the lifecycle of smart objects. As we can see, the existing studies have addressed SIF factors, including a large number of factors, which affect security and privacy.

In terms of IoT, Li et al. in [75] poses a three-layer QoS scheduling model for service oriented IoT. They found that at the application layer, the QoS scheme explores optimal QoS aware services composed by using the knowledge of each component service. At the network level, this proposed model aims to deal with scheduling of heterogeneous network environments. The authors have been focused on throughput, bandwidth, delays and performance of the protocols in use. The proposed QoS scheme for IoT architecture is able to optimize the overall performance of IoT network.

In a web environment, Sackl et al. in [76] have investigated the network bandwidth fluctuations and the impact on QoE. They presented the results of an empirical Web-QoE user study in order to provide insights into the impact of single outage events on subjective quality perception. They show that even short outages have influence in the user's annoyance level. Therefore, they concluded that the impact of outages is application dependent, but compared to video and music formats web-browsing QoE is less sensitive to outages. They also found that the end users do not always detect the outages.

Since web browsing is very important in cellular applications, web QoE in cellular networks is addressed by authors in [33]. The relationship between web QoE and network characteristics is a pre-requisite for cellular network operators to detect network degradation and the impact on QoE. They have implemented a machine-learning mechanism to infer QoE metrics from network traces. The results of this study show that improving signal to noise ratio, decreasing traffic load and reducing handovers will improve significantly the user experience.

As we can see, the existing studies have addressed SIF factors, including a large number of factors, which affect QoE. However, to the best of our knowledge, there is no other study which treats SIF factors in the WoT and security perception issues. Collected works that address system influence factors on the security perception are given in Table A3 (Appendix C) and Table A4 (Appendix D).

4.3.2. Impact of Human Factors on Security Perception

Human IFs are "any variant or invariant property or characteristic of a human user. The characteristic can describe the demographic and socio-economic background, the physical and mental constitution, or the user's emotional state" [22]. They can be grouped in (i) low-level IFs which are linked to physical, emotional, and mental state, and (ii) higher-level IFs such as knowledge, socio-economic context, needs, experiences, etc. As discussed by Baraković and Skorin-Kapov [29], because of the subjectivity and link to inner states, human IFs are every complicated and usually considered in combination with context factors.

One can conclude that, in the WoT environment, HIFs' impact of security perception has not been considered so far. However, in terms of the IoT, AlHogail [77] has, among other hypotheses, discussed the impact of security and risk associated with IoT technology on trust towards IoT adoption. The author has considered the ability of the trustee to achieve major security concerns such as confidentiality, integrity, and availability. He discusses that this factor could be affected by trustee reputation and earlier behaviors and performance, and also, that users trust IoT devices that enable identity authentication and access control. The other addressed factor is risk. The research showed that security-related factors are the most influential when it comes to IoT trust, specially product security. This is very important in terms of a future all-connected digital world and life, since attack vectors will have wider space to grow. In term of risk factor, people tend to think that bad things only happen to other people. This is an especially dominant way of thinking among the younger population that trusts the technology more. This leads to the conclusion that the age factor as well as personality and knowledge level may determine the security perception. In addition to other works, addressing the adoption of IoT, which is not the focus of the paper but may provide useful findings, Luqman and van Belle in their study [78] dealing with human factors that impact the adoption of IoT solutions in Cape Town have confirmed the importance of safety and security.

In a web environment, Constante et al. [71] have analyzed the perception of trust and treated the impacts of system factors such as brand name, usability and look and feel of web site, privacy, reliability and availability, reputation, risk and security, as well as third party seals. The research revealed that privacy and security impact the perceived trust more if the knowledge of a user is higher, while the reliability and availability, usability and look and feel's impact tend to decrease where the knowledge increases. This leads to the conclusion that knowledge as a human factor impacts the security perception in web environment.

In order to summarize, the existing studies have addressed HIFs to a limited extent: knowledge and age. One can understand this given that conducting user-based research is quite difficult. This opens a wide area for future research of these impacts of security perception in a WoT environment. Collected works that address user/human factors that impact on security perception are given in Table A3 (Appendix C) and Table A5 (Appendix E).

4.3.3. Impact of Context Factors on Security Perception

Context IFs are defined as "factors that embrace any situational property to describe the user's environment in terms of physical, temporal, social, economic, task, and technical characteristics" [22]. As they refer to the universal framework for analyzing different IFs that are considered as contextual, it is challenging to conduct a critical and comprehensive review of topic papers. The impact of CIFs on security perception in the IoT and WoT has been analyzed by a few research papers given in Table A3 (Appendix C) and Table A6 (Appendix F).

Context IFs enable better understanding of perceived security, while in the same time increase the security threats due to possible misuse of the contextual data. The IoT paradigm increases security and privacy issues, since IoT sensors collect more contextual data. In addition, recognizing context from the sensors data is important in adding value to the raw sensor data [49]. In this regard, Perera et al. [79] have summarized different context categorization schemes in terms of IoT and identified context IFs (i.e., location, activity, identity, and behavior) that contribute to the security perception. Furthermore,

they have stressed that security and privacy issues need to be addressed at several IoT layers, going from sensor hardware level to context-aware application level. Since the adoption of the IoT paradigm depends on user perception on QoL, security and privacy issues have to be resolved in order to win the trust of the users. Therefore, Ben Saied et al. [80] have proposed a context-aware and multi-service trust management system considering technical context IFs with the aim to manage cooperation in a heterogeneous IoT architecture.

Generally, context IFs may be used as intrusion to user privacy, while in the same time can be used to protect the users concerns [81]. Therefore, Perera et al. [82] have proposed several recommendations on preserving user privacy in the IoT marketplace that include device manufacturers, IoT cloud services and platform providers, and third-party application developers. In addition, they identified three different context-aware features (i.e., presentation, execution, and tagging) referring to the IoT technical context that may affect the security perception.

Although context IFs and their influence on security and privacy are among the most attractive research areas, they have been mainly discussed in terms of IoT. However, addressing security and privacy issues in the WoT, as the software layer on top of the IoT, is certainly direction that the research community should follow in the future [83]. The WoT integrates the underlying IoT with the web, so it requests additional security and privacy protection. The WoT is narrowly associated with its context [84] including environment context (location, temperature, humidity, etc.), temporal context, user context (user profile, user's body temperature, etc.), and system context (bandwidth, battery, etc.). Contextual data in the WoT may be organized in four levels, i.e., physical level, application level, communication level, and social level [85].

Since the WoT is designed to be context-aware, the aforementioned context IFs have to be analyzed in terms of security and privacy issues. For example, El Jaouhari et al. [72] have identified security issues of the WoT and reviewed existing architectures for securing the WoT. On the other hand, Shafik and Matikhah in [86] have summarized privacy issues in the Social WoT (SWoT) and recommended appropriate solutions to address them. Similarly, Javaid et al. [87] considered different categories of context while designing Context Aware Trustworthy Social Web of Things System (CATSWoTS) including who (identity), what (type of service, activity, capability), where (location) and when (time) types of context.

Summarizing the abovementioned, one may notice that various context IFs have been analyzed in existing studies due to their potential to affect the security perception in WoT. This raises some open questions to be answered in the future research, as security is important QoE perceptual dimension that can improve the QoL.

4.4. Summary of the Literature Report

In order to summarize the literature analysis on dependencies between QoL, QoE, and security perception, as well as influence factors affecting them in the WoT, IoT, and WWW (web 2.0) context conducted on the basis of the proposed framework, several findings are given in Table 1. These findings which represent the gaps of the existing literature according to the proposed framework given in Figure 1 will serve us as a basis to draw conclusions about the state-of-the-art literature review in a given context.

Table 1. Summary of results and discussion on dependencies between QoL, QoE, and security perception, as well as influence factors affecting them in WoT, IoT, and WWW context.

Quality Metrics and Factors		Findings	References
QoL and its dimensions		• There is high impact of QoE on QoL in the IoT and WWW domain. • There is a need for studies addressing the impact of QoE on QoL and its dimensions in the WoT domain. • These relationships should be quantified and modelled.	[27,28,30,31,33,88–90]
QoE	Security perception	• There is limited number of studies addressing the impact of security perception on QoE in the WoT, IoT and WWW domain. • There is need for studies addressing the impact of various QoE dimensions (including security perception) and their -interplay on QoE in the given context. • These relationships should be quantified and modelled.	[39]
IF	System	• There is a great number of studies addressing the influence of system factors on QoE in the IoT and WWW domain. • There are no studies which treat the systems factors and security perception (as QoE dimension) in the WoT domain. • These relationships should be quantified and modelled.	[39,49,71–74,77–80,83–85,87]
	Human	• There is a limited number of studies addressing the influence of human factors on QoE in the IoT and WWW domain. • There is a need for studies investigating the impact of human factors and interplay with other factors on QoE and security perception (as QoE dimension) in the WoT domain. • These relationships should be quantified and modelled.	[49,71,77–80,83–85,87]
	Context	• There exist studies considering the context factors in terms of IoT and WoT security. • There is a need for studies investigating the impact of context factors and their interplay with other factors on QoE and security perception (as QoE dimension) in the WoT domain. • These relationships should be quantified and modelled.	[49,71,77–80,83–85,87]

Legend: IF (Influence Factors), IoT (Internet of Things), QoE (Quality of Experience), QoL (Quality of Life), WoT (Web of Things), WWW (World Wide Web).

5. Key Findings and Research Opportunities

The existing literature analysis conducted in this research paper resulted in findings presented in Table 1. They provide the basis for a set of research findings and opportunities for future investigations which are summarized and illustrated in Figure 4. The story starts with the finding that there is a limited amount of papers dealing with use of the WoT for improving QoL and its dimensions. Therefore, the future interdisciplinary research activities should address.

Research opportunity I: how the WoT contributes to the improvement of QoL and its dimensions in smart context.

Research opportunity II: what are the available the WoT solutions on which QoL and its dimensions rely on.

In order to be able to improve QoL, which should be the ultimate goal for researchers in this domain, we have to identify and understand in more detail how the WoT concept will contribute to it. We need to recognize and define a place of WoT in future smart concept that is intertwined with QoL and its dimensions. By that we will be able to identify possible usage scenarios for WoT solutions and their contribution to material living conditions, health, education, productive and valued activities, governance and basic rights, leisure and social interactions, natural and living environment, and economic and physical safety, as well as life overall.

Making a list of the existing WoT solutions aids the analysis of areas of their functionality that need improvement thereby contributing to QoL. If we know how WoT solutions contribute to QoL and its dimensions, we will be able to enhance both the acceptance and performance of WoT systems and life conditions. The first one is important for interested stakeholders in this service delivery chain such as device production factories, designers, connection service providers, etc., while the other is important to all of us who plan to continue living more quality life in the future.

In Figure 1., we have illustrated the dependency chain between QoE and QoL. The basis of this relation lies in the simple math: QoL and its dimensions rely on technology in general nowadays, and if a service is delivered with high QoE, then the QoL of a user is improved. Our investigation of the studies addressing the impact of QoE on QoL and its dimensions in the WoT (as well as in the IoT and WWW context) revealed that these issues are addressed to a limited extent. Therefore, researchers should use the opportunity to be among the first to address the following area of study: **Research opportunity III: investigate how QoE affects QoL overall and all its dimensions in WoT context.**

This recommendation for future research relies on the fact that if the service is delivered with high QoE, then QoL will rise. If we have increased QoL influenced by high QoE during the usage of a given WoT system, consequently the system will be increasingly used, which results in many other benefits for the WoT service delivery providers. Otherwise, the negative impact of QoE on QoL during the usage of the WoT results in service rejection leaving the stakeholders unsatisfied. Having better understanding of the interplay between QoE and QoL in a WoT context will be beneficial to all stakeholders in order to do their part of the job better. One possible way to gain deeper understanding of the abovementioned relations with the aim to enhance QoE and QoL is to **Research opportunity IV: model and quantify the relations between QoE and QoL and its dimensions in a WoT context including their multidimensional nature.**

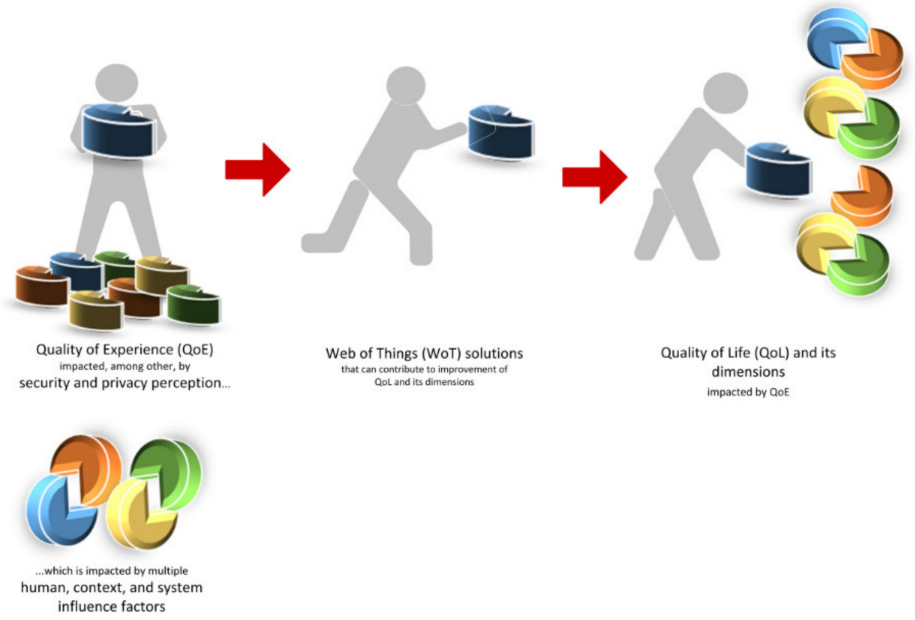

Figure 4. Research steps for future.

Further on, in our framework, we described that QoE is a multidimensional concept influenced by a mixture of multiple perceptual QoE dimensions. The dimensions that have been addressed in this paper due to their importance in todays' and future challenging cyber security environment is the security perception. Following the logic of previous recommendations and story given in Figure 4, an opportunity for future researchers lies in **Research opportunity V: examining, modelling, and quantifying the influence of security perception on QoE in a WoT context.**

QoE is a multidimensional concept and by quantifying and modelling the mutual relations between it and its multiple perceptual dimensions in WoT context, one is able to identify the importance of distinct dimensions in terms of considered perceptions and overall user perceived QoE in a given environment. Therefore, if specially addressing the security perception, we will be able to know to what extent they impact QoE in the WoT. Stakeholders of interest may use the knowledge of these impacts, as well as impacts between QoE and QoL and its dimensions, to become aware of and to understand how their work affects others in the WoT delivery chain or how their products are being affected by others. In addition, they can utilize the findings to enhance their part of the WoT and improve QoE and QoL.

Further on, having in mind that QoE perceptual dimensions are affected by multiple different factors, the opportunities extend to tackling the issue of **Research opportunity VI: extending the multidimensional models with the quantification of examined impact of the most prominent CIFs, HIFs, and SIFs on security perception in WoT context**.

By developing models which describe the interplay between factors and security perception as QoE dimensions in a WoT context, one will be able to identify the importance of distinct factors in terms of considered perceptions and consequently overall QoE and QoL. Additionally, the full QoE model for the WoT containing the description of mutual relations between QoE, security perception, and influence factors that should be developed will contribute to a more accurate prediction of the values of QoE and QoL. Furthermore, interested stakeholders will have even better insight on impacts of distinct factors on security perception, and ultimately QoE and QoL in a WoT context, that can influence their role or describe their influence on others.

However, identifying the factors to address and to model in terms of their influence on perceptual dimensions and QoE is a difficult task. In our analysis, we have found a limited number of papers researching the impact of various human, context, or system factors on security perception, and consequently QoE and QoL. This especially refers to human- and context-related factors, given that technology studies in general investigate system factors impact, instead of including the whole package. With the aim of easing the factor analysis and selection, we provide the list of factors that should be examined in future research studies in Table 2. All of this ultimately contributes to the complex task of QoE and QoL management and improvement. Table 2. The matrix of factors whose impact on security perception should be addressed.

Table 2. List of influence factors to be considered when addressing security perception in WoT context with the aim of improving QoE and QoL.

Influence Factor Type	Web of Things	
Context influence factors	Price Mobility Time of day/week/month/year Type of task Location Environment Economic state Technical and information context Device context Social context Spatial context Data confidentiality Affiliation Access control	User Who (Identity) Where (Location) When (Time) What (Activity, Service, Capability) Why Physical Application Communication System Presentation Execution Tagging

Table 2. *Cont.*

Influence Factor Type	Web of Things	
Human influence factors	Age Lifestyle User routine Gender Culture Emotional state Prior experience	Mood Physical disabilities Mental state Knowledge Education level Personality Health state Productivity
System influence factors	WoT device characteristics Terminal device characteristics Battery lifetime Computational resources Storage capacity Operating system Usability Physical phenomena of wireless/wired channel – variability Wireless/wired channel reliability Wireless/wired capacity Wireless/wired channel variability Handover Brand Security Encryption Access control Risk 3rd party seal Quality Aesthetics/visual representation of elements	Availability Reliability Reputation Delay Ease of use Access Control IPSEC Authorization SSL/TLS VPN Encryption Identity management Non-repudiation Identification Buffer overflow Access Decision Facility SmartOrBAC (organization-based access control) Authentication

Legend: IPSEC (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/Transport Layer Security), VPN (Virtual Private Network), WoT (Web of Things).

6. Summary and Conclusions

As a technology, the WoT has a significant impact on many aspects of our lives, enabling us to have cleaner air and water, smarter cities, smarter agriculture, connecting patients, etc. This technology allows real-world objects and IoT-enabled devices that are increasingly being used to improve the quality of life to be part of the WWW. With the rapid advancement of the WoT, the number of devices connected to the Internet is expected to exceed 70 billion by 2021, which has also attracted the attention of attackers seeking to exploit the benefits of this technology. There are many security and privacy threats in the WoT, such as attacks against systems, unauthorized access to private information, etc. Some of them are the characteristic of the WoT itself, while a portion of them are inherited from IoT and WWW. Nevertheless, it is very important to address the security challenges and their perception in designing future WoT systems.

Having in mind that if users can be sure that WoT will not damage them, violate their privacy or negatively influence their lives, i.e., if they have good perception of WoT security, only then the full potential of it can be used to improve their everyday life. A user's QoE, expectations, perceptions, and needs with respect to technology is what matters today and determines, on one hand, the adoption of the technology, and on the other hand, contributes to their QoL.

Therefore, this paper aims to address and discuss the relationships and interplay between QoL, QoE, security perception, and influence factors affecting security perception in the WoT in a timely manner. The ultimate goal is to contribute to the improvement of QoL of individuals who will increasingly use the WoT in a security challenged future by listing the issues that need to be addressed in future investigations.

The contribution of this review is three-fold. Firstly, we have proposed the framework and explained the dependencies between the considered terms, i.e., QoL, QoE, security perception, and factors affecting them in WoT. As stated multiple times, it is important to include the IoT and WWW

researches because the WoT inherits all their benefits and issues. Secondly, based on that framework, the literature analysis and comparison has been conducted. The findings indicate that this field has been addressed up to a limited extent so far and needs detailed investigation of interplay and influence of different factors on security perception, security perception on QoE, and QoE on QoL dimensions and QoL in the WoT environment. Stakeholders of interest may use the knowledge of these impacts, as well as relations between QoE and QoL, to understand how their work affects others in the WoT delivery chain or how others are affecting their products. Thirdly, we have identified the gaps and issues needed to be addressed by the future research activities and suggested the novel and open investigation directions. It is very important to find how WoT will improve QoL and its dimensions in smart context and what are the WoT solutions on which QoL and its dimensions rely on. In addition, it is important to model the relations between QoE and QoL and its dimensions in the WoT as well as modelling the influence of security perception on QoE in a WoT context. Extending the multidimensional models with the quantification of examined impact of the most prominent CIFs, HIFs, and SIFs on security perception in the WoT context is another research opportunity for the future studies.

Author Contributions: S.B. and J.B.H. suggested the design of the study and wrote the methodology, supervised whole research; S.B., J.B.H., D.M. and A.M. searched the databases, prepared the tables, interpreted the results, visualized and wrote the original draft of the manuscript; S.B., J.B.H., O.K., P.M. and F.J.M. reviewed the manuscript, project administration and funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the project COST Action CA16226 "Living Indoor Space Improvement: Smart Habitat for the Elderly", supported by COST (European Cooperation in Science and Technology), and by SPEV project 2103 at University of Hradec Kralove, FIM, Czech Republic (2020).

Acknowledgments: This publication is based upon work from COST Action CA16226 "Living Indoor Space Improvement: Smart Habitat for the Elderly", supported by COST (European Cooperation in Science and Technology). COST is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career and innovation. www.cost.eu. The authors would like to acknowledge Little Mama Labs research laboratory. This work was also supported by project SPEV 2103 at University of Hradec Kralove, FIM, Czech Republic (2020). We are also grateful for the support of student Pavla Matulova in consultation regarding application aspects.

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

Appendix A

Table A1. The influence of QoE on QoL and its dimensions.

Ref.	QoL Dimension	WWW/IoT/WoT	Application	Users	Environment	Research Method	Model/Framework	Type of Impact
[27]	Overall Experience of Life	WWW	Mobile Web Browsing	ALL	REAL	Regression modelling	YES	HIGH
[28]	Overall Experience of Life	WWW	Mobile Web Browsing	ALL	REAL	Regression modelling	YES	HIGH
[30]	Overall Experience of Life	WWW	Multimedia	ALL	REAL AND LAB	Formula-based QoE estimation methods, and collecting KPIs for most popular services	YES	HIGH
[31]	Overall Experience of Life	WWW	Mobile products	ALL	REAL	Data collection and triggering context analysis	YES	HIGH
[33]	Overall Experience of Life	WWW	Cellular Networks	ALL	REAL	Intuitive and accurate machine-learning models for capturing complex relationship between different network parameters	YES	HIGH
[88]	Overall Experience of Life	IoT	IoT Multimedia	ALL	REAL	Framework for the evaluation and management of the QoE provided by multimedia	YES	HIGH
[89]	Overall Experience of Life	IoT	Multimedia	ALL	REAL	QoE optimization using Data Fusion	YES	HIGH
[90]	Overall Experience of Life	IoT	Social IoT	ELDERLY	REAL	SIoT to leverage the degree of nteraction among things	YES	HIGH

Legend: IoT (Internet of Things), QoE (Quality of Experience), QoL (Quality of Life), SIoT (Social IoT), WoT (Web of Things), WWW (World Wide Web).

Appendix B

Table A2. The influence of perceived security on QoE.

Ref.	QoE	Security Perception	WWW/IoT/WoT	Application	Users	Environment	Research Method	Model/Framework	Type of Impact
[39]	QoE	Security and privacy	WoT	Web applications, healthcare, RFID	ALL	REAL	A case study based on some recent studies from WoT framework	YES	HIGH

Legend: IoT (Internet of Things), QoE (Quality of Experience), RFID (Radio-frequency Identification), WoT (Web of Things), WWW (World Wide Web).

Appendix C

Table A3. The impact of influence factors on perceived security.

Ref.	Security Perception	Type of Influence Factor	Influence Factor	WWW/IoT/ WoT	Users	Environment	Research Method	Model/Framework	Type of Impact
[49]	Privacy	CIF	User, User profile, state of device, environment information	IoT	ALL	BOTH	Context-aware system using through device-oriented modeling for the IoT	YES	HIGH
[71]	Trust	HIF	Realiability, Look&Feel, Availabilty, privacy, security, 3rd party seal, risk, reputatin	WWW	ALL	REAL	Survey	YES	HIGH
[77]	Trust	HIF	Social influence related factors, Product related factors, Security related factors	IoT	ALL	REAL	Statistical analysis	YES	HIGH
[78]	Security	HIF	Gender, basic need, scepticism, safety and security, care for community	IoT	ALL	REAL	A qualitative research methodology employing interviews and thematic analysis	YES	HIGH

Table A3. *Cont.*

Ref.	Security Perception	Type of Influence Factor	Influence Factor	WWW/IoT/ WoT	Users	Environment	Research Method	Model/Framework	Type of Impact
[79]	Security/ privacy	CIF	Data acquisition, Distribution	IoT	ALL	REAL	Context-aware computing	YES	HIGH
[80]	Trust	CIF	Information gathering, Transaction, Reward and punish, Entity selection, Learning	IoT	ALL	LAB	Design	YES	HIGH
[83]	Security	CIF	Data acquisition, Integration, Interoperability	IoT/ WoT	ALL	REAL	Proof-of-concept DaaS	YES	HIGH
[84]	Security/privacy	CIF	Environment, User, Temporal	WoT	ALL	REAL	Design	YES	HIGH
[85]	Security/privacy	CIF	Location, Social component, Used application	WoT	ALL	REAL	Modelling	YES	MEDIUM
[87]	Trust	CIF	Location, Identity, Time, Activity	WoT	ALL	BOTH	Design	YES	MEDIUM

Legend: CIF (Context Influence Factor), HIF (Human Influence Factor), IoT (Internet of Things), QoE (Quality of Experience), SIF (System Influence Factor), WoT (Web of Things), WWW (World Wide Web).

Appendix D

Table A4. The list of SIFs impacting security perception.

Reference	Access Control	IPSEC	Authorization	SSL/TLS	VPN	Encryption	Identity Management	Non-Repudiation	Identification	Buffer Overflow	Access Decision Facility	SmartOrBAC (Organization-Based Access Control)	Authentication
[39]	x	x		x	x				x				
[72]	x		x			x	x	x		x	x		
[73]	x											x	
[74]			x										x

Legend: IPSEC (Internet Protocol Security),SIF (System Influence Factor), SSL/TLS (Secure Sockets Layer/Transport Layer Security), VPN (Virtual Private Network).

Appendix E

Table A5. The list of HIFs impacting security perception.

Reference	Gender	Basic Need	Scepticism	Safety and Security	Care for Community	Social Infuence	Product	Knowledge
[71]								x
[77]				x		x	x	
[78]	x	x	x	x	x			

Legend: HIF (Human Influence Factor).

Appendix F

Table A6. The list of CIFs impacting security perception.

Reference	Location	Identity	When (Time)	What (Activity)	Why	Information Gathering	Transaction	Reward and Punish	Learning	Entity Selection	Social Component	Used Application
[49]	x	x										
[79]	x	x	x	x	x							
[80]						x	x	x	x	x		
[84]	x	x	x									
[85]	x										x	x
[87]	x	x	x	x								

Legend: CIF (Context Influence Factor).

References

1. Juniper Research. The number of connected devices by 2021: Impressive growth ahead, December 2016. Available online: https://www.juniperresearch.com/press/press-releases/%E2%80%98internet-of-things%E2%80%99-connected-devices-triple-2021 (accessed on 11 April 2020).
2. Mattern, F.; Floerkemeier, C. From the Internet of Computers to the Internet of Things. In *Computer Vision*; Springer Science and Business Media LLC: New York, NY, USA, 2010; Volume 6462, pp. 242–259.
3. Guinard, D. A web of Things Application Architecture: Integrating the Real-World into the Web. Ph.D. Thesis, ETH Zurich, Zurich, Switzerland, 2011.
4. Heuer, J.; Hund, J.; Pfaff, O. Toward the Web of Things: Applying Web Technologies to the Physical World. *Computer* **2015**, *48*, 34–42. [CrossRef]
5. Guinard, D.; Trifa, V. *Building the Web of Things*; Manning Publications: New York, NY, USA, 2016.
6. Guinard, D.; Trifa, V.; Mattern, F.; Wilde, E. From the Internet of Things to the Web of Things: Resource-oriented Architecture and Best Practices. In *Architecting the Internet of Things*; Springer Science and Business Media LLC: New York, NY, USA, 2011; pp. 97–129.
7. Guinard, D.; Trifa, V. Towards the Web of Things: Web mashups for Embedded Devices. In Proceedings of the WWW (International World Wide Web Conferences), Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), Madrid, Spain, 20–24 April 2019; Volume 15, p. 8.
8. Sheng, Q.Z.; Qin, Y.; Yao, L.; Benatallah, B. *Managing the Web of Things*; Elsevier Inc.: Amsterdam, The Netherlands, 2017.
9. Trifa, M.V. Building Blocks for a Participatory Web of Things: Devices, Infrastructures, and Programming Frameworks. Ph.D. Thesis, ETH Zurich, Zurich, Switzerland, 2011.
10. Guinard, D.; Trifa, V.; Pham, T.; Liechti, O. Towards physical mashups in the Web of Things. In Proceedings of the 2009 Sixth International Conference on Networked Sensing Systems (INSS), Pittsburgh, PA, USA, 17–19 June 2009; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2009; pp. 1–4.
11. El Jaouhari, S. A Secure Design of WoT Services for Smart Cities. Ph.D. Thesis, Comue Universite Bretagne Loire, Ecole Nationale Superieure Mines-Telecom Atlantique, Rennes, France, 2019.
12. Spirito, M.A.; Delgao, M.T. Internet of Things application scenarios, pilots and innovation. In *Building the Hyperconnected Society: IoT Research and Innovation Value Chains, Ecosystems and Markets*, 1st ed.; Vermesan, O., Friess, P., Eds.; River Publishers: Aalborg, Denmark, 2015; pp. 119–144.
13. Ferrera, E.; Pastrone, C.; Brun, P.E.; Besombes, R.D.; Loupos, K.; Kouloumpis, G.; O'Sullivan, P.; Papageorgiou, A.; Katsoulakos, P.; Karakostas, B.; et al. IoT European security and privacy projects: Integration, architectures and interoperability. In *Next Generation Internet of Things: Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation*, 1st ed.; Vermesan, O., Bacquet, J., Eds.; River Publishers: Aalborg, Denmark, 2018; pp. 207–294.
14. Baldini, G.; Peirce, T.; Botterman, M.; Talacchini, M.C.; Pereira, A.; Handte, M.; Rotondi, D.; Vermesa, O.; Baddii, A.; Copigneaux, B.; et al. *Internet of Things: IoT Governance, Privacy and Security Issues*, 1st ed.; IERC–European Research Cluster on the Internet of Things: Valencia, Spain, 2015.
15. Ahmad, A.; Baldini, G.; Cousin, P.; Garcia, S.N.M.; Skarmeta, A.; Fourneret, E.; Legeard, B. Large scale IoT security testing, benchmarking and certification. In *Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution*, 1st ed.; Vermesan, O., Bacquet, J., Eds.; River Publishers: Aalborg, Denmark, 2017; pp. 189–220.
16. Husic, J.B.; Baraković, S.; Dinarević, E.C. Smart Ageing: Are We Succeeding? In Proceedings of the World Congress on Medical Physics and Biomedical Engineering 2006, Seoul, Korea, 27 August–1 September 2019; Springer Science and Business Media LLC: New York, NY, USA, 2019; pp. 387–393.
17. WHOQOL Group. The World Health Organization quality of life assessment (WHOQOL): Position paper from the World Health Organization. *Soc. Sci. Med.* **1995**, *41*, 1403–1409. [CrossRef]
18. Power, M. The Whoqol Group Development of the World Health Organization WHOQOL-BREF Quality of Life Assessment. *Psychol. Med.* **1998**, *28*, 551–558. [CrossRef] [PubMed]
19. Eurostat. Available online: https://ec/eusopa.eu/eurostat/documents/8131721/8131772/TF3-Final-report-Quality-of-Life.pdf (accessed on 19 September 2019).
20. Tyuichi, M.; Takahisa, S.; Takuki, K. A WoT Gateway with Legacy Devices Virtualization. In Proceedings of the Second W3C Workshop on the Web of Things, Munich, Germnay, 3–5 June 2019.

21. Global Web Index. Available online: https://thenextweb.com/tech/2019/01/31/study-shows-were-spending-an-insane-amount-of-time-online/ (accessed on 19 September 2019).
22. Le Callet, P.; Möller, S.; Perkis, A. Qualinet White Paper on Definitions of Quality of Experience. *Eur. Netw. Qual. Exp. Multimed. Syst. Serv. (COST Action IC 1003)* **2012**, *3*, 1–25.
23. Wac, K.; Fiordelli, M.; Gustarini, M.; Rivas, H. Quality of Life Technologies: Experiences from the Field and Key Challenges. *IEEE Internet Comput.* **2015**, *19*, 28–35. [CrossRef]
24. Husic, J.B.; Baraković, S.; Cero, E.; Slamnik, N.; Oćuz, M.; Dedović, A.; Zupčić, O. Quality of experience for unified communications: A survey. *Int. J. Netw. Manag.* **2019**. [CrossRef]
25. Bandara, W.; Mikson, S.; Fieli, E. A Systematic, Tool-supported Method for Conducting Literature Reviews in Information Systems. In Proceedings of the 19th European Conference on Information Systems (ECIS), Helsinki, Finland, 9–11 June 2013.
26. Levy, Y.; Ellis, T.J. A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Sci. Int. J. Emerg. Transdiscipl.* **2006**, *9*, 181–212. [CrossRef]
27. Baraković, S.; Skorin-Kapov, L. Multidimensional modelling of quality of experience for mobile Web browsing. *Comput. Hum. Behav.* **2015**, *50*, 314–332. [CrossRef]
28. Baraković, S.; Skorin-Kapov, L. Modelling the relationship between design/performance factors and perceptual features contributing to Quality of Experience for mobile Web browsing. *Comput. Hum. Behav.* **2017**, *74*, 311–329. [CrossRef]
29. Baraković, S.; Skorin-Kapov, L. Survey of research on Quality of Experience modelling for web browsing. *Qual. User Exp.* **2017**, *2*, 6. [CrossRef]
30. Tsolkas, D.; Liotou, E.; Passas, N.; Merakos, L. A survey on parametric QoE estimation for popular services. *J. Netw. Comput. Appl.* **2017**, *77*, 1–17. [CrossRef]
31. Korhonen, P.; Tainio, R.; Wallenius, J. Value efficiency analysis of academic research. *Eur. J. Oper. Res.* **2001**, *130*, 121–132. [CrossRef]
32. Liu, X.H.; Shan, M.Y.; Zhang, R.L.; Zhang, L.H. Green vehicle routing optimization based on carbon emission and multi objective hybrid quantum immune algorithm. *Math. Probl. Eng.* **2018**, *2018*. [CrossRef]
33. Balachandran, A.; Aggarwal, V.; Halepovic, E.; Pang, J.; Seshan, S.; Venkataraman, S.; Yan, H. Modeling web quality-of-experience on cellular networks. In Proceedings of the the 20th Annual International Conference, Maui, HI, USA, 11–13 September 2014; Association for Computing Machinery (ACM): New York, NY, USA, 2014; pp. 213–224.
34. Bellavista, P.; Giannelli, C.; Lanzone, S.; Riberto, G.; Stefanelli, C.; Tortonesi, M. A Middleware Solution for Wireless IoT Applications in Sparse Smart Cities. *Sensors* **2017**, *17*, 2525. [CrossRef]
35. Krejcar, O.; Maresova, P.; Selamat, A.; Melero, F.J.; Barakovic, S.; Husic, J.B.; Herrera-Viedma, E.; Frischer, R.; Kuča, K. Smart Furniture as a Component of a Smart City—Definition Based on Key Technologies Specification. *IEEE Access* **2019**, *7*, 94822–94839. [CrossRef]
36. Galinina, O.; Andreev, S.; Komarov, M.; Maltseva, S. Leveraging heterogeneous device connectivity in a converged 5G-IoT ecosystem. *Comput. Netw.* **2017**, *128*, 123–132. [CrossRef]
37. Mora, H.; Pont, M.T.S.; Gil, D.; Johnsson, M. Collaborative Working Architecture for IoT-Based Applications†. *Sensors* **2018**, *18*, 1676. [CrossRef]
38. Poncela, J.; Vlacheas, P.; Giaffreda, R.; De, S.; Vecchio, M.; Nechifor, S.; Barco, R.; Aguayo-Torres, M.C.; Stavroulaki, V.; Moessner, K.; et al. Smart Cities via Data Aggregation. *Wirel. Pers. Commun.* **2014**, *76*, 149–168. [CrossRef]
39. Catuogno, L.; Turchi, S. The Dark Side of the Interconnection: Security and Privacy in the Web of Things. In Proceedings of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Blumenau, Brazil, 8–10 July 2015; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2015; pp. 205–212.
40. Hwang, Y.H. IoT Security & Privacy. In Proceedings of the 1st ACM workshop on Cognitive Radio Architectures for Broadband-CRAB '13, Singapore, 14–17 April 2015; Association for Computing Machinery (ACM): New York, NY, USA, 2015; p. 1.
41. Abomhara, M.; Koien, G.M. Security and privacy in the Internet of Things: Current status and open issues. In Proceedings of the 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, 11–14 May 2014; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 014; pp. 1–8.

42. Sicari, S.; Rizzardi, A.; Grieco, L.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
43. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd Annual Design Automation Conference on-DAC '15, San Francisco, CA, USA, 8–12 June 2014; Association for Computing Machinery (ACM): New York, NY, USA, 2015; pp. 1–6.
44. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
45. Maple, C. Security and privacy in the internet of things. *J. Cyber Policy* **2017**, *2*, 155–184. [CrossRef]
46. Sivaraman, V.; Gharakheili, H.H.; Fernandes, C.; Clark, N.; Karliychuk, T. Smart IoT Devices in the Home: Security and Privacy Implications. *IEEE Technol. Soc. Mag.* **2018**, *37*, 71–79. [CrossRef]
47. Giraldo, J.; Sarkar, E.; Cardenas, A.A.; Maniatakos, M.; Kantarcioglu, M. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Des. Test* **2017**, *34*, 7–17. [CrossRef]
48. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and Privacy in Fog Computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
49. Yang, K.; Cho, S.-B. A context-aware system in Internet of Things using modular Bayesian networks. *Int. J. Distrib. Sens. Netw.* **2017**, *13*. [CrossRef]
50. Lin, H.; Bergmann, N. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
51. Stergiou, C.; Psannis, K.; Kim, B.-G.; Gupta, B. Secure integration of IoT and Cloud Computing. *Futur. Gener. Comput. Syst.* **2018**, *78*, 964–975. [CrossRef]
52. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet Things J.* **2019**, *6*, 1606–1616. [CrossRef]
53. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet Things J.* **2017**, *5*, 2483–2495. [CrossRef]
54. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [CrossRef]
55. Hasan, M.; Islam, M.; Zarif, I.I.; Hashem, M.; Islam, I. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet Things* **2019**, *7*, 100059. [CrossRef]
56. Mawgoud, A.A.; Karadawy, A.I.; Tawfik, B.S. A Secure Authentication Technique in Internet of Medical Things through Machine Learning. *arXiv* **2019**, arXiv:1912.12143.
57. Tabassum, A.; Lebda, W. Security Framework for IoT Devices against Cyber-attacks. In Proceedings of the 6th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2019), Zurich, Switzerland, 23–24 November 2019; Academy and Industry Research Collaboration Center (AIRCC): Zurich, Switzerland, 2019; pp. 249–266.
58. Ataç, C.; Akleylek, S. A Survey on Security Threats and Solutions in the Age of IoT. *Eur. J. Sci. Technol.* **2019**, *15*, 36–42. [CrossRef]
59. Silaghi, V.D.; Silaghi, M.; Mandiau, R. Privacy of Existence of Secrets: Introducing Steganographic DCOPs and Revisiting DCOP Frameworks. *arXiv* **2019**, arXiv:1902.05943.
60. Guan, Z.; Zhang, Y.; Wu, L.; Wu, J.; Li, J.; Ma, Y.; Hu, J. APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *J. Netw. Comput. Appl.* **2019**, *125*, 82–92. [CrossRef]
61. Al-Shukri, H.K.H.; Udayanan. Factors Influencing Online Shopping Intention: A study among shoppers in Oman. *Int. J. Acad. Res. Bus. Soc. Sci.* **2019**, *9*, 691–709.
62. Wu, W.Y.; Ke, C.C. An online shopping behaviour model integrating personality traits, perceived risk, and technology acceptance. *Soc. Behav. Personal. Int. J.* **2015**, *43*, 85–97. [CrossRef]
63. Topaloğlu, C. Consumer motivation and concern factors for online shopping in Turkey. *Asian Acad. Manag. J.* **2012**, *17*, 1–19.
64. Shadkam, M. An empirical study on influence factors of online purchasing. *Int. J. Arts Sci.* **2012**, *5*, 479.
65. Hsu, C.-L.; Lin, J.C.-C.; Chiang, H.-S. The effects of blogger recommendations on customers' online shopping intentions. *Internet Res.* **2013**, *23*, 69–88. [CrossRef]
66. Hsu, M.-H.; Chuang, L.-W.; Hsu, C.-S. Understanding online shopping intention: The roles of four types of trust and their antecedents. *Internet Res.* **2014**, *24*, 332–352. [CrossRef]

67. Amin, M.; Rezaei, S.; Abolghasemi, M. User satisfaction with mobile websites: The impact of perceived usefulness (PU), perceived ease of use (PEOU) and trust. *Nankai Bus. Rev. Int.* **2014**, *5*, 258–274. [CrossRef]
68. Seckler, M.; Heinz, S.; Forde, S.; Tuch, A.N.; Opwis, K. Trust and distrust on the web: User experiences and website characteristics. *Comput. Hum. Behav.* **2015**, *45*, 39–50. [CrossRef]
69. Zinner, T.; Hohlfeld, O.; Abboud, O.; Hoßfeld, T. Impact of frame rate and resolution on objective QoE metrics. In Proceedings of the Second International Workshop on Quality of Multimedia Experience (QoMEX), Trondheim, Norway , 21–23 June 2010; 2010; pp. 29–34. [CrossRef]
70. Jammeh, E.; Mkwawa, I.-H.; Khan, A.; Goudarzi, M.; Sun, L.; Ifeachor, E.C. Quality of experience (QoE) driven adaptation scheme for voice/video over IP. *Telecommun. Syst.* **2010**, *49*, 99–111. [CrossRef]
71. Costante, E.; Hartog, J.D.; Petković, M. On-line trust perception: What really matters. In Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), Milan, Italy, 8 September 2011; Volume 59. [CrossRef]
72. El Jaouhari, S.; Bouabdallah, A.; Bonnin, J.M. Security Issues of the Web of Things. In *Managing the Web of Things*; Elsevier BV: New York, NY, USA, 2017; pp. 389–424.
73. Ouaddah, A.; Bouij-Pasquier, I.; Abou, A.; Abdellah, E.; Ouahman, A.A. Security analysis and proposal of new access control model in the Internet of Thing. In Proceedings of the 2015 International Conference on Electrical and Information Technologies (ICEIT), Marrakech, Morocco, 25–27 March 2015; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2015; pp. 30–35.
74. Skarmeta, A.; Hernandez-Ramos, J.L.; Bernabe, J.B. A required security and privacy framework for smart objects. *2015 ITU Kaleidosc. Trust Inf. Soc. (K-2015)* **2015**, 1–7. [CrossRef]
75. Li, L.; Li, S.; Zhao, S. QoS-Aware Scheduling of Services-Oriented Internet of Things. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1497–1505. [CrossRef]
76. Sackl, A.; Casas, P.; Schatz, R.; Janowski, L.; Irmer, R. Quantifying the impact of network bandwidth fluctuations and outages on Web QoE. In Proceedings of the Seventh International Workshop on Quality of Multimedia Experience (QoMEX), Pylos-Nestoras, Greece, 26–29 May 2015; 2015; pp. 1–6. [CrossRef]
77. AlHogail, A. Improving IoT Technology Adoption through Improving Consumer Trust. *Technology* **2018**, *6*, 64. [CrossRef]
78. Luqman, A.; Van Belle, J.-P. Analysis of human factors to the adoption of Internet of Things-based services in informal settlements in Cape Town. In Proceedings of the 2017 1st International Conference on Next Generation Computing Applications (NextComp), Mauritius, 19–21 March 2015; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2017; pp. 61–67.
79. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context Aware Computing for The Internet of Things: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 414–454. [CrossRef]
80. Ben Saied, Y.; Olivereau, A.; Zeghlache, D.; Laurent, M. Trust management system design for the Internet of Things: A context-aware and multi-service approach. *Comput. Secur.* **2013**, *39*, 351–365. [CrossRef]
81. Dey, A.K.; Abowd, G.; Salber, D. A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications. *Hum. Comput. Interact.* **2001**, *16*, 97–166. [CrossRef]
82. Perera, C.; Liu, C.H.; Jayawardena, S.; Chen, M. A Survey on Internet of Things From Industrial Market Perspective. *IEEE Access* **2015**, *2*, 1660–1679. [CrossRef]
83. Lehmann, M.; Biørn-Hansen, A.; Ghinea, G.; Grønli, T.-M.; Younas, M. Data Analysis as a Service: An Infrastructure for Storing and Analyzing the Internet of Things. In Proceedings of the Lecture Notes in Computer Science, Paris, France, 3–5 November 2015; Springer Science and Business Media LLC: New York, NY, USA, 2015; Volume 9228, pp. 161–169.
84. Bai, G.; Yan, L.; Gu, L.; Guo, Y.; Chen, X. Context-aware usage control for web of things. *Secur. Commun. Netw.* **2012**, *7*, 2696–2712. [CrossRef]
85. Terdjimi, M.; Médini, L.; Marissa, M. Towards a Meta-model for Context in the Web of Things. In Proceedings of the Karlsruhe Service Summit Workshop, Karlsruhe, Germany, 25–26 February 2016.
86. Shafik, W.; Matinkhah, S. Privacy Issues in Social Web of Things. In Proceedings of the 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 April 2019; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2019; pp. 208–214.
87. Javaid, S.; Afzal, H.; Arif, F.; Iltaf, N.; Abbas, H.; Iqbal, M.M.W. CATSWoTS: Context Aware Trustworthy Social Web of Things System. *Sensors* **2019**, *19*, 3076. [CrossRef] [PubMed]

88. Floris, A.; Atzori, L. Managing the Quality of Experience in the Multimedia Internet of Things: A Layered-Based Approach †. *Sensors* **2016**, *16*, 2057. [CrossRef]
89. Huang, X.; Xie, K.; Leng, S.; Yuan, T.; Ma, M. Improving Quality of Experience in multimedia Internet of Things leveraging machine learning on big data. *Futur. Gener. Comput. Syst.* **2018**, *86*, 1413–1423. [CrossRef]
90. Miori, V.; Russo, D. Improving life quality for the elderly through the Social Internet of Things (SIoT). In Proceedings of the Global Internet Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; 2017; pp. 1–6. [CrossRef]