Big Data Research 25 (2021) 100245

Contents lists available at ScienceDirect

Big Data Research

www.elsevier.com/locate/bdr

# Setting Privacy “by Default” in Social IoT: Theorizing the Challenges and Directions in Big Data Research

José Ramón Saura [a,*], Domingo Ribeiro-Soriano [b], Daniel Palacios-Marqués [c]

[a] *Rey Juan Carlos University, Madrid, Spain*
[b] *University of Alcalá, Spain*
[c] *Universitat Politecnica de Valencia, Spain*

ARTICLE INFO

*Article history:*
Received 20 April 2021
Received in revised form 10 June 2021
Accepted 4 July 2021
Available online 8 August 2021

*Keywords:*
Social IoT
Big Data analytics
Privacy by default
Users privacy

ABSTRACT

The social Internet of Things (SIoT) shares large amounts of data that are then processed by other Internet of Thing (IoT) devices, which results in the generation, collection, and treatment of databases to be analyzed afterwards with Big Data techniques. This paradigm has given rise to users' concerns about their privacy, particularly with regard to whether users have to use a smart handling (self-establishment and self-management) in order to correctly install the SIoT, ensuring the privacy of the SIot-generated content and data. In this context, the present study aims to identify and explore the main perspectives that define user privacy in the SIoT; our ultimate goal is to accumulate new knowledge on the adoption and use of the concept of privacy “by default” in the scientific literature. To this end, we undertake a literature review of the main contributions on the topic of privacy in SIoT and Big Data processing. Based on the results, we formulate the following five areas of application of SIoT, including 29 key points relative to the concept of privacy “by default”: (i) SIoT data collection and privacy; (ii) SIoT security; (iii) threats for SIoT devices; (iv) SIoT devices mandatory functions; and (v) SIoT and Big Data processing and analytics. In addition, we outline six research propositions and discuss six challenges for the SIoT industry. The results are theorized for the future development of research on SIoT privacy by “default” and Big Data processing.

## 1. Introduction

In recent years, considerable advances in technology have led to the rapid growth of the Internet-of-Everything (IoE) industry [1]. Accordingly, the collection, analysis and storage of data by companies are becoming an important part of their strategical and technological development [2,3]. The development of Internet, and specially the data transmission speed of the connected devices, has enabled sharing the data in real time and improved people's everyday lives [5]. These progresses boosted an exponential growth of the Big Data industry [6].

In this paradigm of interconnectivity afforded by the Internet of Things (IoT) industry [7], due to the capacity to data transfer by mobile and other connected devices in the smart homes [8], users have been encouraged to apply these devices to address their consumption needs and for their behavioral habits [9]. This increase in the use of mart devices has led companies to develop new strategies based on Big Data processing to improve their products, services, as well as functionalities of their connected devices [3]. Owing to these advances, companies now have the opportunity to collect more and more data from connected devices in terms of use, behavior and habits of users [4]. At this point, however, a question emerges: Do these opportunities impose privacy risks for SIot users?

In this context, there emerged the concept of Social IoT (SIoT), which has the characteristic of sharing the data processed by other IoT connected devices [11]. Therefore, SIoT links objects with their own social networks. SIoT can perform some specific interactions between the connected devices—such as, for instance, to ask a device like Google Home or Amazon Echo to connect the TV in a specific channel (the TV is also connected and collecting data), or command a smart coffeemaker to make a coffee next morning at a specific time. In both cases, there are two connected devices that interact to perform a specific action, one as the sender of the message, and the other as the receiver [8].

[*] Corresponding author.
*E-mail address:* joseramon.saura@urjc.es (J.R. Saura).

https://doi.org/10.1016/j.bdr.2021.100245

Thereby, SIot can boost the generation, collection, and treatment of data created due to the collective use of these devices [12]. However, many previous studies have highlighted privacy concerns of users of those devices [13,14]. For instance, it has been argued that, if one of these devices is hacked, its security is engaged due to its connection to other SIoT devices [15]. Therefore, in the smart ecosystems where these data are used, all processed information can suffer from breaches of both privacy and security [16].

Both on the personal and industry levels, in the event of an attack, the SIoT devices put the entire system at risk, since the devices are connected to the same network [17]. Accordingly, it is interesting to understand whether these SIoT devices require a smart handling (self-establishment and self-management by users) so that these devices can be installed in a way that ensure its privacy [18]. This makes further research on the SIoT privacy relevant and important in terms of preventing situations when user location or even behavior, among other data, can be leaked to other devices.

According to several previous studies [19,20], to avoid such situations, these privacy settings should be established "by default", since big enterprises collect and analyze the maximum amount of data generated by SIoT devices to improve their products with artificial intelligence (AI). To this end, the standard settings to achieve business and development's aims, rather than high user-privacy standards, are employed [21]. This approach also boosts the processing and storage of data.

The users who install SIoT devices become, without being aware of it, administrators of systems [22]; in fact, any user who installs a SIoT device is in charge of data storing, its functions and, sometimes, its transfer to third parties [23]. However, if users who become administrators of the SIoT systems are unable to appropriately manage this function due to the lack of knowledge of data privacy management, their privacy can be jeopardized [24]. The analysis of user data with Big Data techniques can provide enterprises with meaningful patterns, associations, and significant correlations, or even help predict how users will behave and use their SIoT devices. Therefore, these applications can directly violate user privacy [25].

To address these concerns, the present study aims to identify and explore the main aspects that characterize the privacy of the devices connected to a SIoT. The specific goals of the present investigation are as follows:

- To identify the perspectives on user privacy in SIot and Big Data
- To explore the uses of the SIot and Big Data regarding user privacy
- To create knowledge regarding the use of Big Data and SIot taking into account the concept of "privacy by default"
- To define future research directions, challenges and propositions for the use of SIot and its Big Data analysis techniques to ensure user privacy

To achieve the aforementioned objectives, in the present study, we undertook a comprehensive review of the main contributions published to date in this field. The remainder of this paper is structured as follows. The theoretical framework of the present study is outlined in Section 2. Section 3 presents the methodology. The results are reported in Section 4. In Section 5, we discuss the findings and outline future research directions and research challenges. Conclusions are drawn in Section 6.

## 2. Theoretical framework

According to Afzal et al. [11], the SIoT is an emergent paradigm where the devices interact with each other to reach their common objectives. As a result, the SIoT has changed the paradigm where these connected devices are structured [26]. Today, the SIoT has come to be understood as a service oriented to heterogeneous devices that can offer services and actions based on the data obtained from those devices [27]. However, this ability to interconnect processes through connected devices increases the concerns about both data security and user privacy [28].

These types of devices are connected to the same network or IP and work under the theoretical definitions of the SIot concept; accordingly, these devices sacrifice their individual interest [29] to collective services [30]. In parallel, the industry and manufacturers of these devices open new ways of cooperation and collaboration in terms of sharing data policies to offer their services [31].

These initiatives allow the SIot industry to develop new products and services based on technological communications among the devices [32]. This leads to the collection, analysis, processing, visualization, and selling of massive amounts of data (Big Data), as well increases the efficiency and scalability of those data to help to predict user behavior [28]. Therefore, the social IoT makes it possible to generate a global architecture where the connectivity and the platforms that manage these data become relevant to the Big Data industry [33]. Following Afzal et al. [11], in the present study, we focus on four characteristics of the SIoT that will be reviewed in Sections 2.1–2.4.

### 2.1. Service discovery of the SIoT

The development and systematic application of the SIot to industries facilitates the discovery of new services and the creation of new analysis offers based on the treatment and use of the collected data [34]. Accordingly, not only the IoT industry, but also the Big Data industry can be enriched by the application and exponential use of these novel technologies [10]. New business strategies for the creation of data-centric products are proposed by companies that collect data on the daily basis [31].

Using many connected devices that transfer information among them in real time makes it possible to not only connect the devices that previously worked individually, but also to add the newly connected devices [34] for a joint analysis and treatment of the data and, based on that, to offer an overview of the agreed targets in the SIoT industry.

In recent years, the creation and development of new SIot services has been exponential, and the higher becomes the number of the SIoT devices in smart homes and the industrial/professional field, the larger amount of applications will become available to discover new products and services linked to Big Data management, strategies, and innovation processes [35].

### 2.2. Network size in SIoT

Furthermore, the SIoT enables increasing the signal and the browsing network of the devices and the corresponding structure [36]. The joint work of the connected devices leads to the generation of data and the subsequent emergence and expansion of different networks, which increases connectivity of the devices [37]. In this way, the global coverage of the network expands, which facilitates access to the information in terms of data management and storage [38]. This expansion of networks definitely benefits companies and individuals, since large areas can be connected by sharing information between connected devices. This makes it possible to cover large industries or geographic areas for massive data acquisition and collection [39].

In this context, it becomes possible, on both the industrial and individual levels, to collect large amounts of data [40]. The analysis of these data can help to improve industrial processes, discover new ways of product development, and to offer new services of optimization and information processing from the SIoT [41]. On the individual level, numerous SIoT devices, such as smart cups, refrigerators, smart coffee machines, thermostats or vacuum cleaners, are currently used in smart homes. These devices offer a wide range of functionalities [42] and increase the signal and the network to which the devices are connected.

### *2.3. Relation management in SIoT*

As mentioned previously, whenever professionals or ordinary users install their new devices at either smart factories or in smart homes, these individuals become the administrators of the SIoT network system [42]. Accordingly, these users should be aware of risk, vulnerabilities and possible privacy threats when connecting different devices that share the data collectively [43].

The numerous devices that work at the same time in the same place can give rise to new business relations among companies interested in comprehending new market niches [40]. Thus, the SIoT can be used for the development of business analysis and behavioral prediction tool of the users of these devices [44]. It is widely known that, in the Big Data ecosystem, the collection, analysis, and use of large databases from the SIot devices can change the privacy paradigm, make behavioral predictions, and even lead to online behavior modifications [45].

Accordingly, selling these data to third parties or their use to improve products or to provide sales forecasts is a promising possibility that remains open for the companies that use the same physical ecosystem of connected devices and the SIoT [32].

Therefore, owing to the SIoT use, the Big Data industry has expanded. Of note, many SIoT devices are bought with privacy clauses that enable data transfer to third parties. Due to these transfers, companies can create new business models focused on the management of data collected by SIoT devices [45].

### *2.4. Trustworthiness, establishment, and management of SIoT devices*

Trustworthiness of connected systems and appropriate establishment and management should be key priorities for the companies that use Big Data and the SIoT devices [28]. The SIot makes possible to greatly increase the number of data-based strategies for decision making, product improvement, or behavioral action prediction [39]. As all of the above depend on management and trustworthiness of the SIoT devices [46], users can have data privacy concerns. Accordingly, companies should agree on facilitating users to correctly understand the privacy policy of their devices. In addition, if companies use the data created through the use these devices, users should be informed about such use of their data [47].

In summary, the management of the SIoT devices requires ability and knowledge of both their performance and network maintenance [48]. On the professional or industrial levels, the ecosystems are usually strengthened with firewalls that increase user privacy. However, when the management and installation of the networks is linked to smart homes where the system administrator lacks appropriate knowledge, the management and maintenance of the processed information by the SIot devices should be carefully analyzed from the perspective of privacy [49]. Therefore, trust in the implementation of these devices and privacy is the key aspect of management strategies of companies working with SIoT devices [28].

### *2.5. Social IoT influence on Big Data*

As indicated in many previous studies, the SIoT adds new sources of information and data generation to the Big Data structures [50]. The multitude of interconnected devices allows for the installation of data sensors and transfer sensors, thereby increasing the databases generated as a result of the use of these devices [34].

The interconnectedness of different SIoT devices greatly improves their ability to collect and analyze data [9]. Therefore, Big Data takes advantage from the ability of collection to create repositories where the generated databases can be structured or nonstructures, and that could be analyzed to share their data and make correlations and predictions to identify new patterns [28]. In addition, analytical techniques based on Big Data facilitate creating reports, charts, and other outputs generated as result of the use of platforms based on AI [50].

Furthermore, the use of Big Data contributes to extending the analyzed metrics, settings, preferences, calendars, metadata, logs, transfer and social communications, as well as any other data from a SIot database [49]. Since the Big Data techniques work with systems improved with AI and perform the decision-making process, there is a direct relationship between Big Data and the SIot [41].

In this context, the increase of the data storage through the use of the SIoT allows Big Data to keep improving with the use of the systems boosted by machine learning, as well as to identify patterns, make predictions, or structure non-structured databases [6]. Therefore, the more SIoT devices are used and connected, the larger the expansion of the Big Data analytics industry will become, thus driving both the development of new techniques for data collection/analysis and user behavior forecasting [34].

### *2.6. Privacy "by default" in SIoT and Big Data*

The new General Data Protection Regulation of the European Commission—which went into effect on May 25, 2018, replacing the Data Protection Directive 95/46/EC—defines the concept of privacy as follows: "*Data protection by default is the principle according to which an organization* (*the data controller*) *ensures that only data strictly necessary for each specific purpose of the processing are processed by default* (*without the intervention of the user*)" [51].

The terms of privacy "by default" and "by design" are growing in the SIot and Big Data industry [52]. In this way, the SIoT users, or the companies that manage connected gadgets on an industrial level, become system managers, even if they lack knowledge on how to correctly set privacy settings. These settings are predefined by companies that develop the connected devices based on commercial and legal terms [53,54].

The concept of privacy by default presupposes that the connected devices, particularly the SIoT ones, should be predetermined with the settings that ensure user privacy. This sort of privacy and the concerns of both users and industry about these actions cause doubts about who is responsible for accessing the servers storing the data [29]. For the industry, intelligence services, governments, and third parties interested in the access to these SIoT servers are quite relevant with regard to improving strategies in the market and predicting any potential hazardous events [39].

Understood from the point of view of professional users and consumers, this constitutes not only an ethical challenge, but also an economic one, since both user and business data have an economic value [39]. When these data are filtered or accessed, their economic value disappears, which benefits interested third parties [45]. Similarly, from a moral and ethical point of view, consumer and professional associations require improvements of regulations in this area; however, in contrast to fast technological advances, regulations evolve slowly, causing a loophole in the legislation in different industries (such as digital marketing user's privacy based on cookies data, electric scooters riding in cities, etc.).

However, several authors argued that the privacy of these devices is compromised because individual users and companies who work with SIoT devices do not correctly inspect the instructions of the devices [43,46]. Said differently, many users of connected devices lack appropriate knowledge to understand the technical details related to the collection, extraction, and treatment of their data [52].

However, Michota and Katsikas [52] argued that the data privacy of the SIot devices is predefined for commercial and product development reasons, so there is neither priority on user privacy, nor to their information about it. This has to change, and privacy by default should be prioritized over business purposes. Regulatory institutions should require companies engaged in the development of SIoT devices to create privacy protocols that ensure privacy "by default" and not commercial purposes "by default". Therefore, the present study aims to identify and explore the main perspectives that define user privacy in the SIoT. Our ultimate goal is to accumulate new knowledge on the adoption and use of the concept of privacy "by default" in the literature.

## 3. Methodology

The concept of SIoT is relatively recent in the academic literature. Accordingly, relevant investigations on user privacy, SIoT, and its link to Big Data remain scarce. To fill this gap in the literature, the present study discusses the challenges and directions in this field. As argued by Milani and Navimipour [55] and Neilson et al. (2019) [56], a systematic literature review should take into account the nature of the study concepts. Accordingly, in the present study, the novelty and the emergent topic of SIoT with regard to privacy and Big Data should be linked and established both theoretically and empirically.

In order to accumulate knowledge on a new emergent topic on which no considerable research has been performed, a literature review has been argued to be an ideal approach (e.g., [56]). Likewise, authors such as [45] highlighted that a literature review is an appropriate methodological approach compared to other approaches. Overall, literature reviews allow researchers to employ previous scientific contributions or investigation propositions in their subsequent research [57]. Accordingly, literature reviews provide a theoretical conceptualization of the concepts under study, lines of research, and theoretical propositions for the future of the industry under study. Other methodological approaches empirically test the results, seek relationships of statistical significance, or link variables and indicators with the assistance of machine learning algorithms to test hypotheses. In a review, objectives or research questions are theorized and then the corresponding variables or constructs of statistical models can be for empirical significance [27].

In the present review, following the considerations proposed by Neilson et al. [56], Martinez et al. [58], Saura et al. [45], we aimed to accumulate knowledge of SIoT and privacy "by default", explore the main risks of connected devices, and outline future research directions for further research.

Our literature review unfolded in several steps. First, we focused on the theoretical foundations of the analyzed concepts. Our three main concepts were user privacy, SIoT, and Big Data. Second, we examined the scientific literature to find the most relevant contributions in this area [57]. This allowed us to prioritize the research questions, concepts, and definitions. Upon selection of the concepts to be used to obtain relevant results, the results were classified and filtered based on selection criteria. We focused on original papers, reviews, congress contributions, and book chapters [27].

Thirdly, we examined the identified articles to identify inadequate or non-inclusive terms. At this stage, the irrelevant descriptions and specifications were excluded [58]. In the present study, the searches were performed based on the following five databases: Web of Sciences (WOS), ScienceDirect, IEEExplore, ACM digital Library, and AIS electronic library. These databases were selected following several previous studies [39,59].

The concepts used in the search were selected to obtain the maximum number of relevant studies [58]. First of all, we used the search word "Social IoT" AND "Big data" AND "Privacy". The obtained results were then filtered with respect to their relevance for the present study. Following Ribeiro-Navarrete et al. [39], we also used the following combinations of the search terms: "Social IoT" AND "Big Data"; "Social IoT" AND "Privacy"; and finally, "Social IoT". This allowed us to identify all potentially relevant studies.

Filtering the obtained studies included the following three steps. First, based on the analysis of the tittle, abstract, and keywords, the most suitable articles were identified. Second, upon an in-depth analysis, several studies that were not related to the topic of the present study were excluded from the dataset. Thirdly and finally, we established a new filter for an in-depth analysis of the articles in order to find inadequate or non-inclusive terms.

The results of the article filtering process were as follows. First, in the WOS database, we found a total of 170 articles. For the four searches discussed above ("Social IoT AND Big data AND Privacy", "Social IoT AND Big Data", "Social IoT AND Privacy", and "Social IoT"), we obtained 2, 13, 19, and 126 papers, respectively. In the fourth group, 8 studies were selected as relevant for the present study.

Second, in the ScienceDirect databased, we found a total of 329 articles. For the four searches ("Social IoT AND Big data AND Privacy", "Social IoT AND Big Data", "Social IoT AND Privacy", and "Social IoT"), we obtained 51, 63, 89, and 126 studies, respectively. In the fourth group, 7 studies were selected as relevant for the present study.

Third, in the IEEExplore, we found a total of 111 articles. For the four searches ("Social IoT AND Big data AND Privacy", "Social IoT AND Big Data", "Social IoT AND Privacy", and "Social IoT"), we found 1, 7, 7, and 96 studies, respectively. In the fourth group, 7 studies were included in the final dataset. Forth, in the ACM Digital Library database, we found a total of 60 articles. For the four searches ("Social IoT AND Big data AND Privacy", "Social IoT AND Big Data", "Social IoT AND Privacy"), we found 5, 6, 12, and 31 studies, respectively. In the fourth group, 4 studies were included in the final dataset. Finally, in the AIS electronic library, we found a total of 14 articles. For the four searches ("Social IoT AND Big data AND Privacy", "Social IoT AND Big Data", "Social IoT AND Privacy", and "Social IoT"), we found 1, 3, 3, and 7 studies, respectively. In the last group, 2 were included in the final dataset.

In summary, the final sample of studies to review included a total of 26 studies of which 17 were examined from the SIoT privacy perspective, and 10 from the perspective of the link between IoT and Big Data. The searches were performed on April 8-12, 2021. The search criteria were as follows: (1) scientific journals, books, chapters, communications or prestigious conferences; (2) publications in English (see Table 3).

Then the results were classified based on their risk bias, following the PRISMA method indications. Specifically, we considered the following differentiating factors: (i) study design; (ii) random sequence generation; (iii) blinding of outcome assessment; (iv) withdraw and drop out; (v) inclusion-exclusion criterion; and (vi) reporting adverse event. In this way, if the selected studies met each characteristic, this was marked with + (with - otherwise, and with ? in questionable cases) (see Tables 1–2).

With regard to (i) study design, we evaluated the quality of the study, whether it respects the scientific values, and whether the rigor is high. As to (ii) random sequence generation, we checked whether the authors correctly assigned the participants to the sample. We also assessed if the analyzed sample was random, and whether these values were indicated. With regard to (iii) blinded outcome assessment, we checked whether the study reported a

**Table 1**
Risk bias for articles included from social lot privacy classification.

| Description | Afzal et al. [11] | Gan et al. [13] | Gao et al. [14] | Baccarelli et al. [36] | Bi et al. [60] | Sun et al. [61] | Romdhani et al. [62] | Nitschke et al. [63] | Savaglio et al. [64] | Riahi Sfar et al. [65] | Zhang et al. [66] | Lee et al. [67] | Chang et al. [68] | Narang et al. [69] | Thangavel et al. [70] | Iqbal et al. [71] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (i) Whether the study and its methodology were correctly presented and linkage with the research objectives | - | + | + | + | + | + | ? | + | + | + | + | ? | + | + | + | + |
| (ii) Inspected whether researchers randomly assigned participants/sample into groups | ? | ? | + | ? | - | + | ? | ? | ? | - | ? | ? | ? | + | ? | + |
| (iii) Assessed whether the study reported a blinded outcome assessment or who assessed the outcome | ? | + | + | + | + | + | ? | - | + | - | ? | ? | + | + | + | + |
| (iv) Inspected the articles for potential errors in the systematic attribution | + | ? | + | ? | + | + | ? | ? | + | + | + | + | + | - | - | + |
| (v) Checked whether the inclusion/exclusion criteria used in reviewed studies were valid and justified | + | ? | + | ‘ | ? | + | ? | - | + | + | ? | + | + | - | + | + |
| (vi) Reviewed whether the reviewed studies have significant limitations that compromised the reliability | + | + | + | ? | + | + | ? | + | + | + | + | + | + | - | + | + |

blinded outcome assessment or whether the study identified who was in charge of performing the processes of creating the outcomes. Next, concerning (iv) withdraw and drop out, we checked whether a test was carried out to make sure that the articles do not have potential mistakes on the theoretical, developmental, and sampling levels. As to (v) inclusion-exclusion criterion, we examined if the study performed quality processes in terms of the inclusion or exclusion of variables making up the study sample and its justification. Finally, as concerns (vi) reporting adverse event, we checked whether the study had any limitations that could jeopardize its contributions.

## 4. Results

Based on the results of the reviewing process, we identified five categories of perspectives and SIoT uses that must be taken into account to preserve user privacy "by default" in terms of Big Data analysis and processes: SIoT data collection and privacy, SIoT-generated content security, Threats for SIoT devices, SIoT devices required features and SIoT and Big Data processing and analytics. These categories are discussed further in Sections 4.1–4.5.

### 4.1. SIoT data collection and privacy

One of the main issues found in the review of main scientific contributions was the relationship between the data collection processes and user privacy [29]. There are concerns about how data will be used or whether these databases will be transferred to third parties for commercial purposes or behavioral prediction aims by default [45]. In addition, the nature and type of data collected with SIoT devices were found to be diverse and applied in the processes of different industries [16]. Accordingly, it is necessary to establish the parameters that would allow for the identification of which data users share and how these data should be anonymized [82,83] to guarantee user privacy rights. In this respect, the following conditions linked to SIoT, data collection, and privacy were identified:

1. Identification of the data requested by SIoT devices at installation: How will these data be used? How long and where will they be stored? Will users know which information is collected?

**Table 2**
Risk bias for articles included from social Iot Big Data classification.

| Description | Goad et al. [72] | Santos et al. [73] | Mendhurwar et al. [74] | Ahmed et al. [75] | Tavana et al. [76] | Kinesis et al. [77] | Sheridan et al. [78] | Kumaran et al. [79] | Bansal et al. [80] | Babar et al. [81] |
|---|---|---|---|---|---|---|---|---|---|---|
| (i) Whether the study and its methodology were correctly presented and linkage with the research objectives | + | + | + | + | + | + | + | + | + | + |
| (ii) Inspected whether researchers randomly assigned participants/sample into groups | ? | ? | ? | ? | ? | + | ? | ? | + | + |
| (iii) Assessed whether the study reported a blinded outcome assessment or who assessed the outcome | + | + | + | ? | + | + | + | + | + | + |
| (iv) Inspected the articles for potential errors in the systematic attribution | + | + | + | + | + | + | - | + | + | + |
| (v) Checked whether the inclusion/exclusion criteria used in reviewed studies were valid and justified | + | + | - | + | + | + | - | + | + | + |
| (vi) Reviewed whether the reviewed studies have significant limitations that compromised the reliability | + | + | + | + | + | + | + | + | + | + |

2. Definition of the explicit and non-explicit data, which results from the correlation analysis with other SIoT devices that these devices have access to.
3. Information about data property rights should be indicated, along with a specification whether these rights will change in the future.
4. Reporting any risk of sharing the collected data with third parties and the purposes of such sharing.
5. Guarantees of confidentiality, integrity, and availability of the devices linked to user data collection when requested.

### 4.2. SIoT-generated content security

Furthermore, other interest areas for the experts are SIoT privacy and security of devices with regard to possible attacks to collect SIoT-generated content [46]. In this respect it is necessary to implement protocols that increase security of digital signatures or cryptography [84]. Likewise, in order to avoid frauds, it is necessary to complement "default" settings by role-based access control and intrusion detection systems, as well as other technologies that increase the SIoT devices' security [31]. The algorithms that work with Big Data analysis and that control the analysis processes and data collection must be examined to increase the devices' security [48]. There is a direct relationship between devices' security and privacy of the SIoT-generated content. Accordingly, the following points should be considered with regard to SIoT device security and user privacy:

1. Adding cryptography and digital signatures to SIoT devices.
2. Adding role-based or mandatory access control to prevent intruders in SIot devices.
3. Increasing protocols for device authentication (e.g., biometrics, facial recognition, intrusion detection systems, gateways, network address translators, among others).
4. Mandatory use of firewalls and IPS systems in professional environments or in smart homes.
5. Use of encryption algorithms to improve the secure transmission of information among the SIot devices.

### 4.3. Threats for SIoT devices

As argued by Abdul-Ghani and Konstantas [21], when the SIoT devices are installed in different ecosystems, such as factories, smart homes, or smart cities [85], various risks can emerge, ranging social engineering risks to attacks on the networks that the devices are connected to [86,87]. In connected networks, privacy "by default" must strictly respect the protocols of both security and possible attack to protect user information and strategical processes of companies [39]. Accordingly, internal dashboards and data monitoring panels should be created to track the information and identify threats in SIoT devices. With regard to the threats for SIoT devices, the following issues were identified:

1. Attacks known as DoS (Denial of services) where the attackers' aim is to spoil/violate the availability of varied services.
2. Malicious codes in software that work in smartphones and that can carry out XSS attacks, remote code execution, and Trojan deployments to steal information or to disrupt functioning.
3. Identification of social engineering threats in order to get information from users.
4. The physical capture threats that put at risk user information.
5. Attacks to collective networks of the SIoT devices.

### 4.4. SIoT devices required features

With respect to maintaining privacy by default in the devices, as well as preserving user security over the years [11], diverse actions to be taken by manufacturers were identified [88]. Specifically, manufacturers should develop products with minimum data protection characteristics. In this way, if there is an intention to propose actions or protocols focused on respecting the concepts of "privacy by default", the quality of the products and the monitoring of the responsible manufacturers and companies will not allow the SIoT to be compromised by attacks to illegally obtain information from the devices. Moreover, when the data collected by the SIoT devices is further analyzed and processed using Big Data analytics [6], the following protocols to preserve data privacy and protect user information should be followed:

1. Checking software updates
2. Continuous installing of security patches
3. Frequent requests of password changes
4. Information about how user data will be shared with others
5. Rules to show how to turn down previously taken actions
6. Full adjustable settings, allowing for changes in the settings by default
7. Obligation to inform about any change in the user data management, storage, and transfer

### *4.5. SIoT and Big Data processing and analytics*

Regarding the process and analysis through algorithms and platforms based on Big Data [89] and cloud analysis and processing [90], as well as the databases of SIoT-generated content, there remain challenges and issues about data sources, data structures, as well as their processing and analysis [34]. In some cases, there are incompatibilities [28] due to the fact that platforms and sources of information work with different management software (e.g., Apache Hadoop, Cloudera Data Hub, SAP-Hana, HP-HAVEn, 1010data, Hortonworks, Pivotal big data suite, Infobright or MapR, etc.). Another issue is that different data management systems can be developed by the companies themselves, or rented to third parties, which, as users of these management systems, can also have access to the processed and analyzed data. Accordingly, the following indications to maintain data privacy and to properly and securely collect, process, and analyze information from the SIoT devices were formulated:

1. Data format challenges as the Big Data can be in shape of semantic, type, and representation.
2. Creating protocols to separate valuable and helpful data from noisy data and to increase data security
3. Controlling the SIoT devices that may be loosely controlled to prevent out-of-range values and impractical data collection
4. Avoiding missing data and ensuring timely processing of data
5. Creating protocols to ensure decision making and improve efficiency
6. Measuring the value-added applications of the SIoT in Big Data when privacy is set by default
7. Check the incompatibilities and possible management breaches in the different Big Data systems used by companies working with SIoT data.

## 5. Discussion

As argued by Gupta and Quamara [91] and Martinez et al. [58], the SIoT has different applications in a wide range of industries. For instance, the SIoT can be used to monitor the environment, run industrial plants, in 4.0 Industry such as city or smart homes management, or in gamification. In all these processes and development actions, the privacy of users and professionals who use these devices is a central priority on both the industrial and personal levels [43].

According to Patil and Seshadri (2014) [47], these processes produce large amounts of live data that are communicated among different devices using the SIoT technology [10]. This bidirectional interconnection among data generates large databases that, afterwards, are analyzed with Big Data to establish correlations, analyze trends, and identify patterns [92]. However, as indicated by Yu et al. [16], when these actions are not correctly developed, user privacy and database security, as well as the protocols to solution of breaches and attacks, can be jeopardized [19].

As argued by Foukia et al. [20], privacy by default in the SIoT is one of the main issues in the development of strategies that compromise decision making, data processing, user behavior predictions [13]. While the management of privacy settings is the responsibility of users, companies are responsible for strengthening the privacy by default in their devices [44].

Since companies work under business competition and always try to reduce the costs of their devices [42], the entire industry should agree on a standard to correctly manage and process data, as well as define security and privacy by default actions [26]. Also, in industries such as telemedicine or e-health, issues related to the behavior users if privacy by default is not guaranteed, as it could put at risk the information of users and companies when products and services are used [1].

Therefore, as argued by Milani and Navimipour [54], the automation and connection between the devices must be trustworthy and it should be obvious who will be the proprietary of the data [24] and how these data will be used [23]. Taking these considerations into account and based on our results, in the next section, we formulate relevant research propositions [58].

### *5.1. Research propositions*

As argued by Jin et al. [2] and Saura et al. [93], open-source solutions to develop improvements in the security of connected devices are a relevant option for the SIoT sector [53]. Through creating a feedback between developers and the industry, the solutions can be strengthened, shared, and globally implemented [48]. Accordingly, we formulate the following research proposition:

**Proposition 1.** *Open-source security solutions can prevent attacks and privacy violations on global collective levels.*

As argued by Ding et al. [94], the consent and legitimization of user data lacks appropriate regulations and collective security protocols [8,95]. Furthermore, the treatment, processing, and transfer of data from these databases analyzed with Big Data techniques lack common procedures and protocols for manufacturers and companies [7,33]. Based on the above, we put forward the following research proposition:

**Proposition 2.** *New procedures for the establishment of consent/legitimacy of user data can be globally applied to the SIoT and the treatment of Big Data databases generated by these devices.*

In the present-day global market were the SIoT devices are distributed and commercialized, a global self-regulation to boost the privacy by default protocols should be in place [27]. Therefore, propositions concerning global regulations' frameworks are needed to avoid conflicts in privacy policies [5]. Nowadays, each manufacturer has its own regulation, which leads to conflicts in terms of data treatment [56], application of Big Data analytics techniques [50], or data transfer. Accordingly, we formulate the following research proposition:

**Proposition 3.** *A privacy "by default" protocol that would prevent the self-regulation in the SIoT privacy globally and that would generate analysis, processing, and management of data incompatibilities should be set and discussed.*

As indicated by Baccarelli et al. [36] and Rehman et al. [38], efforts should be made towards making consensual the definition, responsibilities and security in both data analysis and data processing of the SIoT-generated content [96]. Doing so will enhance user knowledge about the management of the data and their transfer to third parties [97]. Accordingly, we put forward the following research proposition:

**Proposition 4.** *In defining trust and security responsibilities when using SIoT devices based on privacy protection, the notions of privacy awareness, data association, and data utility of the SIoT-generated content should be priorities for researchers and law regulators.*

As indicated by Michota and Katsikas [51], it is necessary to establish protocols to develop standard models in the SIoT devices based on the concept of privacy "by default" and solutions linked to interoperability, scalability, analysis of Big Data, and data security [20]. The protocols linked to the development of new devices based on privacy by default must be a request for the manufacturers [25]. Therefore, our proposition is as follows:

**Proposition 5.** *SIoT models providing "by default/design" solutions for interoperability, security/privacy, and scalability in Big Data should be set internationally.*

Since Big Data processing and analytics platforms can be used to measure large amounts of SIoT-generated data, in the SIoT, processing and analytics can be performed closer to data sources using the services of different systems of data processing [28]. However, a scientific framework should be defined that would help to understand how the processing of the privacy of SIoT-generated data with Big Data platforms ensures the information's privacy without the risks of data leaks, incompatibilities, and other issues [57]. In this respect, our proposition is as follows:

**Proposition 6.** *An internationally recognized compliance standard to evaluate Social IoT privacy protection should be proposed and discussed.*

### 5.2. Future research challenges for the SIoT privacy and Big Data

Following previous studies that analyzed the current state of SIoT technology and its link to similar industries [50,54], we identified the challenges where the SIoT industry and researchers should cooperate on improving privacy and security of data collected from connected devices, as well as their treatment, processing and prediction with Big Data techniques and platforms [57,86]. The challenges are summarized in Table 4.

## 6. Conclusions

In this study, we reviewed major scientific contributions in the SIoT industry up to date. Specifically, upon reviewing a large number of relevant publications and upon selecting the best publications using a set of filters, we focused on the review of a total of 26 studies of which 17 were conducted from the SIoT perspective, and 10 focused on the link between the SIoT and with Big Data.

Our specific focus was on the following five areas composed by 29 key points: (i) SIoT data collection and privacy (5 key points); (ii) SIoT security (5); (iii) Threats for SIoT devices (5 key points); (iv) SIoT devices mandatory functions (7 key points); and (v) SIoT and Big Data processing and analytics (7 key points). These areas or analysis perspectives for the SIoT have common features related to security, functionality, and risk of use and configuration of SIoT devices if they are not correctly configured under the proposed parameters of privacy by default concept.

Furthermore, based on the results and upon identification of six challenges for the industry about privacy by default in SIoT and data processing that researchers and practitioners should take into account in the future developed actions, we formulated six research proposals to develop SIoT and privacy "by default" and its link to Big Data analysis.

To conclude, the direction of setting privacy 'by default' in SioT should seek to achieve a satisfactory balance between: (i) quality of service and protection of user data privacy; (ii) agreements between software and products that share information for security protocols focused on privacy by default; (iii) regulations aimed at avoiding conflicts between companies in terms of the interests of data owners; (iv) the obligation of providing SIoT device users with explicit information on privacy by default characteristics. In addition, the following aspects should be carefully considered: (v) the development of action protocols in relation to Big Data processing technologies and their adaptation to privacy by default; (vi) the implementation of specific regulations for the collection of SIoT data, processing with Big Data technologies, and (vii) the use of data by companies, governments and other intelligence services or companies that could use this type of data to fraudulently obtain insights.

### 6.1. Theoretical implications

The results of the present study contribute to available knowledge about the SIoT, privacy by default in the connected devices in this industry, and the processing and analysis with Big Data. Our results offer several important theoretical implications about the main uses, industries, social challenges, and research proposals identified in the literature [104,106], some of them different currently due pandemic [105].

First, the results of the present study can be used to criticize and discuss other proposed models, protocols or technologies that do not respect privacy "by default". Similarly, the challenges and research propositions should be used as a basis for further research in this industry.

Second, the theoretical challenges addressed in the present study should be taken into account in the development of new scientific contributions identified as propositions and challenges, that should be tested in experimental or empirical studies as their main aim is to maintain privacy "by default" in the SIoT devices or similar ones.

### 6.2. Practical implications

With regard to practical implications of our results, the main contributions are as follows. First, the results of the present study can be used by developers, manufacturers, and public agents in charge of legislation in this field. Our results provide meaningful insights into how the SIoT industry has raised concerns about privacy of the SIoT-generated content and data, and how the scientific industry has worked to address these issues.

Second, based on our results, new methodologies that consider Big Data analysis and data collection from the SIoT devices can be developed, which can assist in promotion of new products linked to the SIoT industry.

Third, manufacturers can use our discussion of challenges as point of reference to reduce their costs or to appropriately maintain the privacy "by default" in their devices [51]. The challenges highlighted in the present study put at risk security and privacy of the SIoT devices and should be taken into account by manufactures, policy makers and interested third parties.

### 6.3. Limitations

The present study has several limitations. First, the data analyzed in the present study were also used in similar investigations [45]. The second limitation of the present study is a possible linkage to the exponential development of the analyzed technology and Big Data actions applied to this industry. Third, the present study proposes only theoretical propositions that should be empirically validated in future research.

**Table 3**
Articles identification in social IoT, privacy and Big Data.

| Research studies | Journal/Conference | Main contributions | Key concepts | Privacy | Big Data |
|---|---|---|---|---|---|
| Afzal et al. [11] | Future Generation Computer Systems | This paper identifies performance metrics to select suitable operation systems for specific hardware platforms in SIoT applications. | Social IoT, Operating systems, Microcontroller architecture, Embedded systems, Resource-constrained devices | ✓ | |
| Gan et al. [13] | IEEE Internet of Things Journal | This study proposes a design of a multi-hop routing incentive mechanism that can also preserve task requester's privacy considering both user privacy and budget. | Crowdsourcing, incentive mechanism, privacy preserving, social Internet of Things (IoT) | ✓ | ✓ |
| Gao et al. [14] | Security Communication Networks | This paper outlined a framework to preserve user privacy against inference attacks on social network data in social IoT. | Social Internet of Things, Security, Privacy, Polymorphic Value Set | ✓ | |
| Baccarelli et al. [35] | IEEE Network | This study discusses Integration of the Social Internet of Things and Fog Computing through use cases in order to describe the architecture and the main resource-management functions of the SoIT technological platform. | SIoT, Fog Computing, | ✓ | |
| Bi et al. [60] | Wireless Communications and Mobile Computing | This paper proposes a privacy-preserving personalized service framework to provide privacy protection to users in the social IoT is proposed. | Privacy-Preserving Personalized Service Framework, Bayesian Model, Social IoT, User's privacy | ✓ | |
| Sun et al. [61] | Security Communication Networks | This study presents an online Service Function Chaining deployment algorithm that can support security and privacy of social IoT applications is outlined. | Network function virtualization, IoT application, Service Function Chaining, Security, Privacy | ✓ | |
| Romdhani [62] | Securing the Internet of Things | In this paper, it is argued that SIoT must enforce additional security mechanisms to preserve the amount of data generated and used by these devices. | SIoT, Data privacy, Security mechanisms | ✓ | ✓ |
| Nitschke and Williams [63] | Procedia Computer Science | This study identifies the characteristics and challenges of data supply in the IoT. | IoT, Data Supply, Value Capturing, Shallow Data, Provenance Data | ✓ | ✓ |
| Savaglio et al. [64] | Future Generation Computer Systems | This paper highlights the synergy of Agent-based Computing paradigm and other IoT-related paradigms and technologies. | IoT, Agent-based Computing paradigm, Software agents | ✓ | |
| Riahi Sfar et al. [65] | Digital Communications and Networks | This study presents an overview of the IoT security roadmap where role of each component of the approach, its interactions with the other main components, and their impact are explained. | IoT, Systemic and cognitive approach, Security, Privacy, Trust, Identification, Access control | ✓ | |
| Zhang et al. [66] | 11th International Conference on Wireless Communications and Signal Processing | This paper proposes a novel approach to monitor various parameters of the entire site from the IoT devices as well as to provide guidance for privacy protection in this environment. | Internet of Things, Data Privacy, Social network sites, Smart devices | ✓ | |
| Lee and Kwon [67] | International Conference on Disaster Recovery and Business Continuity (DRBC) | This study develops an architecture of the system for information sharing in the environment of IoT. | SIoT, IoT, Information sharing, Social networks, Self-configuration wireless sensor networks | ✓ | ✓ |
| Chang et al. [68] | ACM Computing Surveys | This paper analyzes the Business Process Management Systems of IoT and their limitations in their drawbacks based on a Mobile Cloud Computing perspective. | Mobile Cloud Business Process, IoT, Information systems | ✓ | |
| Narang and Kar [69] | Proc. of the 24th Annual Inter. Conference on Mobile Computing and Networking | This study evaluates accuracy of using tie information from Facebook Friend Graph in order to establish a method for ranking the strength of ties in a SIoT network. | Social Networks, Internet of Things, Social IoT, Trust Management | ✓ | |
| Thangavel et al. [70] | AMCIS 2019 Proceedings | This paper performs a differentiation of Social IoT into devices that part of human social loop and have a role in human social network, and objects from social networks. | Social IoT, Social Web of Things, IoT, Social Network | ✓ | |
| Iqbal et al. [71] | Enabling the IoT: Fundamentals, Design and Applications | This study argues that the SIoT provides an emergent paradigm of Internet of Things (IoT), where devices are able to interact with other smart things due to Big Data. | Internet of Things, Computer architecture, Social networking | ✓ | |
| Goad and Gal [72] | AMCIS 2017 | This paper identifies IoT design challenges and establishes solutions in SIoT that can be used as standards in IoT designs to reduce Architectural Heterogeneity. | SIoT, IoT, Architectural Heterogeneity | ✓ | |
| Santos et al. [73] | Ad Hoc Networks | In this study, a routing protocol where the device mobility favors the IoMT and SIoT implementation is designed. | IoT, Mobility, Routing protocol | | ✓ |
| Mendhurwar and Mishra [74] | Enterprise Information Systems | This study identifies the synergies between the Internet of Things and the SIoT l in order to detect interactions and key challenges with the focus on cybersecurity and privacy. | SIoT, Cybersecurity, Digital Transformation, Artificial Intelligence, Cyber Physical Social Systems | | ✓ |
| Ahmed et al. [75] | Computer Networks | This paper discusses opportunities resulting from the convergence of Big Data, analytics, and SIoT in order to show the key requirements for enabling analytics in an IoT environment. | IoT, Big Data, Distributed computing, Smart city | ✓ | ✓ |
| Tavana et al. [76] | Internet of Things | This study reviews the challenges, open issues, applications, and architecture of the IoT-based ERP to show that sensors and devices connected to the Internet can manage the stored data processed in the cloud through ERP due to Big Data. | IoT, Enterprise resource planning (ERP), Cloud computing | | ✓ |

(continued on next page)

**Table 3** (*continued*)

| Research studies | Journal/Conference | Main contributions | Key concepts | Privacy | Big Data |
|---|---|---|---|---|---|
| Kasnesis et al. [77] | Computers & Elect. Engineering | In this study, a combination of semantic web technologies and smart software agents using Big Data techniques is sued to achieve cognitive friendship and goal management. | Cognitive IoT, SIoT, Decision making, Machine learning | | ✓ |
| Sheridan et al. [78] | 2019 Inter. Confe. on Sensing and Instrum. in IoT Era | This paper offers a solution for interconnecting users and devices through the use of Twitter that allows human-to-machine connection through IoT protocols. | Human-to-machine connection, Social networks, IoT, SIoT | ✓ | ✓ |
| Kumaran and Sridhar [79] | 2020 4th Inter. Conf. on Trends in Elect. and Informatics | This study presents different modeling approaches in terms of social-instance connections and communication in the SIoT linked to Big Data, as well as methods, models and techniques involved in the SIoT. | SIoT techniques, SIoT applications, IoT | | ✓ |
| Bansal et al. [80] | ACM Computing Surveys | This paper summarizes the state of the art in IoT and Big Data management in various domains in order to propose a taxonomy for IoT Big Data management. | IoT, Big Data, Smart cities, IoTBD management, IoTBD challenges | ✓ | ✓ |
| Babar and Arif [81] | Proc. of the 2017 ACM Inter. Joint Conf. on Pervasive and Ubiq. Comp. | This study proposes an IoT-based smart urban architecture using Big Data analytics to improve real-time data processing and decision making. | Smart City, IoT, Big Data Analytics | ✓ | ✓ |

**Table 4**
Future research challenges for SIoT privacy and Big Data.

| Authors | Challenges | Description |
|---|---|---|
| Ausloos et al. [53]<br>Bahirat et al. [19] | 1. Achieving a satisfactory balance between quality of service and privacy protection. | Achieving a balance in the cost-effective strategies to reduce the SIoT devices' costs and maintaining user privacy. |
| Amato et al. [98]<br>Tewari and Gupta [99] | 2. Agreement on the use of a unique software/platform that manages all SIoT devices in the connected ecosystems. | Manufacturers should allow the use of one single management device to avoid using their own management software in a device/manufacturer level instead of allowing to collectively manage these devices. |
| Foukia et al. [20]<br>Finch et al. [23] | 3. Avoid conflicting (corporate) interests to share a standard framework about quality of the devices regarding privacy by default, as well as the data storage time and its transfer to third parties. | The quality of the Internet-of-Thing devices and the privacy "by default" should be standardized on the industrial level. This will help to avoid conflicts and preserve the quality of privacy protocols in these devices. |
| Geneiatakis et al. [44]<br>Tao et al. [100]<br>Quamara et al. [97] | 4. To drive and promote the integration of computing paradigms for SIoT in different applications and contexts (e.g., smart homes and smart factories) through guidelines, best practices, protocols, technologies, and white books | Quality and security regulations for the SIoT should be developed. There is also need for guidelines and propositions of best practices, as well as protocols that would allow for the integration of new computational paradigms in different SIoT applications |
| Gahi et al. [101]<br>Perrot et al. [102] | 5. Boost the diversity issues when working with SIoT and Big Data | The actual SIoT protocols usually have several initiatives, such as CoAP, MQTT, XMPP, DDS, STOMP, HTTP, and AMQP. However, the IoT paradigms do not have a universal protocol, which leads to diversity that arises from several SIoT requests. Accordingly, SIoT systems may be unable to support multiple protocols. While the standardization of several organizations (ITU-T, IETF, ISO/IEC, IEEE, ETSI, and 3GPP) has boosted some efforts, this challenge still has to be addressed. |
| Ribeiro-Navarrete et al. [39]<br>Saura et al. [39]<br>Kerber [103] | 6. Development of the regulation of the data collection with SIoT from governance and intelligences services | The use of SIoT in governance, regulation, and intelligences services remains a challenge. While this industry can be relevant to governments, listening and surveillance actions must be regulated considering it as a challenge for privacy "by default" strategies and concepts, not only in the surveillance industry but also in smart cities or industries, among others. |

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

In gratitude to the Ministry of Science, Innovation and Universities and the European Regional Development Fund: RTI2018-096295-B-C22.

## References

[1] M.H. Miraz, M. Ali, P.S. Excell, R. Picking, A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT), in: 2015 Internet Technologies and Applications (ITA), IEEE, 2015, September, pp. 219–224.

[2] X. Jin, B.W. Wah, X. Cheng, Y. Wang, Significance and challenges of big data research, Big Data Res. 2 (2) (2015) 59–64, https://doi.org/10.1016/j.bdr.2015.01.006.

[3] S. Rouhani, S. Rotbei, Big data platforms: in the lens of selection and evaluation approach, J. Decis. Syst. (2021) 1–30, https://doi.org/10.1080/12460125.2020.1869432.

[4] S. Hodges, S. Taylor, N. Villar, J. Scott, D. Bial, P.T. Fischer, Prototyping connected devices for the Internet of things, Computer 46 (2) (2012) 26–34, https://doi.org/10.1109/MC.2012.394.

[5] D. Mourtzis, E. Vlachou, N.J.P.C. Milas, Industrial big data as a result of IoT adoption in manufacturing, Proc. CIRP 55 (2016) 290–295, https://doi.org/10.1016/j.procir.2016.07.038.

[6] H. Cai, B. Xu, L. Jiang, A.V. Vasilakos, IoT-based big data storage systems in cloud computing: perspectives and challenges, IEEE Int. Things J. 4 (1) (2016) 75–87, https://doi.org/10.1109/jiot.2016.2619369.

[7] Y. Hajjaji, W. Boulila, I.R. Farah, I. Romdhani, A. Hussain, Big data and IoT-based applications in smart environments: a systematic review, Comput. Sci. Rev. 39 (2021) 100318, https://doi.org/10.1016/j.cosrev.2020.100318.

[8] M.R. Alam, M.B.I. Reaz, M.A.M. Ali, A review of smart homes—past, present, and future, IEEE Trans. Syst. Man Cybern., Part C, Appl. Rev. 42 (6) (2012) 1190–1203, https://doi.org/10.1109/tsmcc.2012.2189204.

[9] J.R. Saura, Using Data Sciences in Digital Marketing: framework, methods, and performance metrics, J. Innov. Knowl. 6 (2) (2021) 92–102, https://doi.org/10.1016/j.jik.2020.08.001.

[10] Y. Saleem, N. Crespi, M.H. Rehmani, R. Copeland, D. Hussein, E. Bertin, Exploitation of social IoT for recommendation services, in: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), IEEE, 2016, December, pp. 359–364.

[11] B. Afzal, M. Umair, G.A. Shah, E. Ahmed, Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges, Future Gener. Comput. Syst. 92 (2019) 718–731, https://doi.org/10.1016/j.future.2017.12.002.

[12] V. Beltran, A.M. Ortiz, D. Hussein, N. Crespi, A semantic service creation platform for Social IoT, in: 2014 IEEE World Forum on Internet of Things (WF-IoT), IEEE, 2014, March, pp. 283–286.

[13] X. Gan, Y. Li, Y. Huang, L. Fu, X. Wang, When crowdsourcing meets social IoT: an efficient privacy-preserving incentive mechanism, IEEE Int. Things J. 6 (6) (2019) 9707–9721, https://doi.org/10.1109/JIOT.2019.2930659.

[14] Y. Gao, N. Zhang, Social security and privacy for social IoT polymorphic value set: a solution to inference attacks on social networks, Secur. Commun. Netw. (2019), https://doi.org/10.1155/2019/5498375.

[15] A.A. Mawgoud, M.H.N. Taha, N.E.M. Khalifa, Security threats of social internet of things in the higher education environment, in: Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications, Springer, Cham, 2020, pp. 151–171.

[16] S. Yu, G. Wang, X. Liu, J. Niu, Security and privacy in the age of the smart Internet of Things: an overview from a networking perspective, IEEE Commun. Mag. 56 (9) (2018) 14–18, https://doi.org/10.1109/MCOM.2018.1701204.

[17] A. Singh, S. Batra, Ensemble based spam detection in social IoT using probabilistic data structures, Future Gener. Comput. Syst. 81 (2018) 359–371, https://doi.org/10.1016/j.future.2017.09.072.

[18] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2017, March, pp. 618–623.

[19] P. Bahirat, Y. He, A. Menon, B. Knijnenburg, A data-driven approach to developing IoT privacy-setting interfaces, in: 23rd International Conference on Intelligent User Interfaces, 2018, March, pp. 165–176.

[20] N. Foukia, D. Billard, E. Solana, PISCES: a framework for privacy by design in IoT, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2016, December, pp. 706–713.

[21] H.A. Abdul-Ghani, D. Konstantas, A comprehensive study of security and privacy guidelines, threats, and countermeasures: an IoT perspective, J. Sens. Actuator Netw. 8 (2) (2019) 22, https://doi.org/10.3390/jsan8020022.

[22] T. Sommestad, A. Hunstad, Intrusion detection and the role of the system administrator, Inf. Manag. Comput. Secur. (2013), https://doi.org/10.1108/09685221311314400.

[23] J. Finch, S. Furnell, P. Dowland, Assessing IT security culture: system administrator and end-user perspectives, in: Proceedings of ISOneWorld 2003 Conference and Convention, Las Vegas, Nevada, USA, 2003, April.

[24] R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, M.D. Mickunas, Towards security and privacy for pervasive computing, in: International Symposium on Software Security, Springer, Berlin, Heidelberg, 2002, November, pp. 1–15.

[25] Y. Gahi, M. Guennoun, H.T. Mouftah, Big data analytics: security and privacy challenges, in: 2016 IEEE Symposium on Computers and Communication (ISCC), IEEE, 2016, June, pp. 952–957.

[26] M. Lippi, M. Mamei, S. Mariani, F. Zambonelli, An argumentation-based perspective over the social IoT, IEEE Int. Things J. 5 (4) (2017) 2537–2547, https://doi.org/10.1109/JIOT.2017.2775047.

[27] S. Madakam, V. Lake, V. Lake, V. Lake, Internet of Things (IoT): a literature review, J. Comput. Commun. 3 (05) (2015) 164, https://doi.org/10.4236/jcc.2015.35021.

[28] P. Jain, M. Gyanchandani, N. Khare, Big data privacy: a technological perspective and review, J. Big Data 3 (1) (2016) 1–25, https://doi.org/10.1186/s40537-016-0059-y.

[29] M. Adams, Big data and individual privacy in the age of the internet of things, Technol. Innov. Manag. Rev. 7 (4) (2017) 12–24, http://timreview.ca/article/1067.

[30] M.A. Alsmirat, F. Al-Alem, M. Al-Ayyoub, Y. Jararweh, et al., Impact of digital fingerprint image quality on the fingerprint recognition accuracy, Multimed. Tools Appl. 78 (3) (2019) 3649–3688, https://doi.org/10.1007/s11042-017-5537-5.

[31] C. Stergiou, K.E. Psannis, B.B. Gupta, Y. Ishibashi, Security, privacy & efficiency of sustainable cloud computing for big data & IoT, Sustain. Comput. Inform. Syst. 19 (2018) 174–184, https://doi.org/10.1016/j.suscom.2018.06.003.

[32] J.R. Saura, B. Rodriguez Herráez, A. Reyes-Menendez, Comparing a traditional approach for financial Brand Communication Analysis with a Big Data Analytics technique, IEEE Access 7 (1) (2019) 37100–37108, https://doi.org/10.1109/ACCESS.2019.2905301.

[33] N.N. Misra, Y. Dixit, A. Al-Mallahi, M.S. Bhullar, R. Upadhyay, A. Martynenko, IoT, big data and artificial intelligence in agriculture and food industry, IEEE Int. Things J. (2020), https://doi.org/10.1109/JIOT.2020.2998584.

[34] A.E. Khaled, S. Helal, A framework for inter-thing relationships for programming the social IoT, in: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), 2018, February, pp. 670–675.

[35] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I.A.T. Hashem, A. Siddiqa, I. Yaqoob, Big IoT data analytics: architecture, opportunities, and open research challenges, IEEE Access 5 (2017) 5247–5261, https://doi.org/10.1109/ACCESS.2017.2689040.

[36] E. Baccarelli, M. Scarpiniti, P.G.V. Naranjo, L. Vaca-Cardenas, Fog of social IoT: when the fog becomes social, IEEE Netw. 32 (4) (2018) 68–80, https://doi.org/10.1109/MNET.2018.1700031.

[37] M.S. Roopa, A. Siddiq, R. Buyya, K.R. Venugopal, S.S. Iyengar, L.M. Patnaik, Dynamic management of traffic signals through social IoT, Proc. Comput. Sci. 171 (2020) 1908–1916, https://doi.org/10.1016/j.procs.2020.04.204.

[38] A. Rehman, A. Paul, M.A. Yaqub, M.M.U. Rathore, Trustworthy intelligent industrial monitoring architecture for early event detection by exploiting social IoT, in: Proceedings of the 35th Annual ACM Symposium on Applied Computing, 2020, March, pp. 2163–2169.

[39] S. Ribeiro-Navarrete, J.R. Saura, D. Palacios-Marqués, Towards a new era of mass data collection: assessing pandemic surveillance technologies to preserve user privacy, Technol. Forecast. Soc. Change 167 (2021) 120681, https://doi.org/10.1016/j.techfore.2021.120681.

[40] I. Ahmed, M. Ahmad, G. Jeon, F. Piccialli, A framework for pandemic prediction using big data analytics, Big Data Res. 25 (2021) 100190, https://doi.org/10.1016/j.bdr.2021.100190.

[41] M.S. Roopa, S. Pattar, R. Buyya, K.R. Venugopal, S.S. Iyengar, L.M. Patnaik, Social Internet of Things (SIoT): foundations, thrust areas, systematic review and future directions, Comput. Commun. 139 (2019) 32–57, https://doi.org/10.1016/j.comcom.2019.03.009.

[42] P.P. Gaikwad, J.P. Gabhane, S.S. Golait, A survey based on Smart Homes system using Internet-of-Things, in: 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), IEEE, 2015, April, pp. 0330–0335.

[43] P.E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L.F. Cranor, N. Sadeh, Privacy expectations and preferences in an IoT world, in: Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017), 2017, pp. 399–412.

[44] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, G. Baldini, Security and privacy issues for an IoT based smart home, in: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2017, May, pp. 1292–1297.

[45] J.R. Saura, D. Palacios-Marqués, A. Iturricha-Fernández, Ethical design in social media: assessing the main performance measurements of user online behavior modification, J. Bus. Res. 129 (2021) 271–281, https://doi.org/10.1016/j.jbusres.2021.03.001.

[46] K.R. Sollins, IoT big data security and privacy versus innovation, IEEE Int. Things J. 6 (2) (2019) 1628–1635, https://doi.org/10.1109/JIOT.2019.2898113.

[47] H.K. Patil, R. Seshadri, Big data security and privacy issues in healthcare, in: 2014 IEEE International Congress on Big Data, IEEE, 2014, June, pp. 762–765.

[48] W.S. Jeong, S.H. Kim, K.S. Min, An analysis of the economic effects for the IoT industry, J. Internet Comput. Serv. 14 (5) (2013) 119–128, https://doi.org/10.7472/jksii.2013.14.5.119.

[49] B.O. Vikas, Internet of things (iot): a survey on privacy issues and security, Int. J. Sci. Res. Sci. Eng. Technol. 1 (3) (2015) 168–173.

[50] A.P. Plageras, K.E. Psannis, C. Stergiou, H. Wang, B.B. Gupta, Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings, Future Gener. Comput. Syst. 82 (2018) 349–357, https://doi.org/10.1016/j.future.2017.09.082.

[51] European Data Protection Supervisor EDPS, Privacy by default, retrieved April 11, 2021, from https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en, 2020.

[52] A. Michota, S. Katsikas, The evolution of privacy-by-default in Social Networks, in: Proceedings of the 18th Panhellenic Conference on Informatics, 2014, November, pp. 1–6.

[53] J. Ausloos, E. Kindt, E. Lievens, P. Valcke, J. Dumortier, Guidelines for privacy-friendly default settings, ICRI Res. Pap. 12 (2013), https://doi.org/10.2139/ssrn.2220454.

[54] B.C. Gallego, J. Drexl, IoT connectivity standards: how adaptive is the current SEP regulatory framework?, IIC – Int. Rev. Intellect. Prop. Compet. Law 50 (1) (2019) 135–156, https://doi.org/10.1007/s40319-018-00774-w.

[55] B.A. Milani, N.J. Navimipour, A systematic literature review of the data replication techniques in the cloud environments, Big Data Res. 10 (2017) 1–7, https://doi.org/10.1016/j.bdr.2017.06.003.

[56] A. Neilson, B. Daniel, S. Tjandra, Systematic review of the literature on big data in the transportation domain: concepts and applications, Big Data Res. 17 (2019) 35–44, https://doi.org/10.1016/j.bdr.2019.03.001.

[57] O.Y. Al-Jarrah, P.D. Yoo, S. Muhaidat, G.K. Karagiannidis, K. Taha, Efficient machine learning for big data: a review, Big Data Res. 2 (3) (2015) 87–93, https://doi.org/10.1016/j.bdr.2015.04.001.

[58] I. Martinez, E. Viles, I.G. Olaizola, Data science methodologies: current challenges and future approaches, Big Data Res. 24 (2021) 100183, https://doi.org/10.1016/j.bdr.2020.100183.

[59] J.R. Saura, D. Ribeiro-Soriano, D. Palacios-Marqués, From user-generated data to data-driven innovation: a research agenda to understand user privacy in

digital markets, Int. J. Inf. Manag. (2021) 102331, https://doi.org/10.1016/j.ijinfomgt.2021.102331.

[60] R. Bi, Q. Chen, L. Chen, J. Xiong, D. Wu, A privacy-preserving personalized service framework through Bayesian Game in Social IoT, Wirel. Commun. Mob. Comput. 2020 (2020), https://doi.org/10.1155/2020/8891889.

[61] J. Sun, G. Huang, A.K. Sangaiah, G. Zhu, X. Du, Towards supporting security and privacy for social IoT applications: a network virtualization perspective, Secur. Commun. Netw. 2019 (2019) e4074272, https://doi.org/10.1155/2019/4074272.

[62] I. Romdhani, Security concerns in social IoT, in: Securing the Internet of Things, Elsevier, 2017, pp. 131–132.

[63] P. Nitschke, S.P. Williams, Conceptualizing the internet of things data supply, Proc. Comput. Sci. 181 (2021) 642–649, https://doi.org/10.1016/j.procs.2021.01.213.

[64] C. Savaglio, M. Ganzha, M. Paprzycki, C. Bădică, M. Ivanović, G. Fortino, Agent-based Internet of Things: state-of-the-art and research challenges, Future Gener. Comput. Syst. 102 (2020) 1038–1053, https://doi.org/10.1016/j.future.2019.09.016.

[65] A. Riahi Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the Internet of Things, Digit. Commun. Netw. 4 (2) (2018) 118–137, https://doi.org/10.1016/j.dcan.2017.04.003.

[66] L. Zhang, X. Zhu, X. Han, J. Ma, Differentially privacy-preserving Social IoT, in: 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP), 2019, pp. 1–6.

[67] H. Lee, J. Kwon, Survey and analysis of information sharing in social IoT, in: 2015 8th International Conference on Disaster Recovery and Business Continuity (DRBC), 2015, pp. 15–18.

[68] C. Chang, S.N. Srirama, R. Buyya, Mobile cloud business process management system for the internet of things: a survey, ACM Comput. Surv. 49 (4) (2017) 1–42, https://doi.org/10.1145/3012000.

[69] N. Narang, S. Kar, Utilizing social networks data for trust management in a social internet of things network, in: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, 2018, pp. 768–770.

[70] G. Thangavel, M. Memedi, K. Hedström, A systematic review of Social Internet of Things: concepts and application areas, in: AMCIS 2019 Proceedings, 2019, https://aisel.aisnet.org/amcis2019/meta_research_is/meta_research_is/1.

[71] M.A. Iqbal, S. Hussain, H. Xing, M.A. Imran, Social IoT, in: Enabling the Internet of Things: Fundamentals, Design and Applications, IEEE, 2021, pp. 195–211.

[72] D. Goad, U. Gal, IoT design challenges and the social IoT solution, in: AMCIS, 2017.

[73] B.P. Santos, O. Goussevskaia, L.F.M. Vieira, M.A.M. Vieira, A.A.F. Loureiro, Mobile Matrix: routing under mobility in IoT, IoMT, and Social IoT, Ad Hoc Netw. 78 (2018) 84–98, https://doi.org/10.1016/j.adhoc.2018.05.012.

[74] S. Mendhurwar, R. Mishra, Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges, Enterp. Inf. Syst. 15 (4) (2021) 565–584, https://doi.org/10.1080/17517575.2019.1600041.

[75] E. Ahmed, I. Yaqoob, I.A.T. Hashem, I. Khan, A.I.A. Ahmed, M. Imran, A.V. Vasilakos, The role of big data analytics in Internet of Things, Comput. Netw. 129 (2017) 459–471, https://doi.org/10.1016/j.comnet.2017.06.013.

[76] M. Tavana, V. Hajipour, S. Oveisi, IoT-based enterprise resource planning: challenges, open issues, applications, architecture, and future research directions, Internet of Things 11 (2020) 100262, https://doi.org/10.1016/j.iot.2020.100262.

[77] P. Kasnesis, C.Z. Patrikakis, D. Kogias, L. Toumanidis, I.S. Venieris, Cognitive friendship and goal management for the social IoT, Comput. Electr. Eng. 58 (2017) 412–428, https://doi.org/10.1016/j.compeleceng.2016.09.024.

[78] D. Sheridan, A.A. Simiscuka, G.-M. Muntean, Design, implementation and analysis of a Twitter-based social IoT network, in: 2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI), 2019, pp. 1–6.

[79] P. Kumaran, R. Sridhar, Social Internet of Things (SIoT): techniques, applications and challenges, in: 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), 2020, pp. 445–450.

[80] M. Bansal, I. Chana, S. Clarke, A survey on IoT big data: current status, 13 V's challenges and future directions, ACM Comput. Surv. 53 (6) (2020) 131:1–131:59, https://doi.org/10.1145/3419634.

[81] M. Babar, F. Arif, Smart urban planning using big data analytics-based internet of things, in: Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers, 2017, pp. 397–402.

[82] V.A. Memos, K.E. Psannis, Y. Ishibashi, B.G. Kim, B.B. Gupta, An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework, Future Gener. Comput. Syst. 83 (2018) 619–628, https://doi.org/10.1016/j.future.2017.04.039.

[83] R. Hu, Z. Yan, W. Ding, L.T. Yang, A survey on data provenance in IoT, World Wide Web 23 (2) (2020) 1441–1463, https://doi.org/10.1007/s11280-019-00746-1.

[84] V. Adat, B.B. Gupta, Security in Internet of Things: issues, challenges, taxonomy, and architecture, Telecommun. Syst. 67 (3) (2018) 423–441, https://doi.org/10.1007/s11235-017-0345-9.

[85] C. Esposito, M. Ficco, B.B. Gupta, Blockchain-based authentication and authorization for smart city applications, Inf. Process. Manag. 58 (2) (2021) 102468, https://doi.org/10.1016/j.ipm.2020.102468.

[86] I. Lee, K. Lee, The Internet of Things (IoT): applications, investments, and challenges for enterprises, Bus. Horiz. 58 (4) (2015) 431–440, https://doi.org/10.1016/j.bushor.2015.03.008.

[87] D. Li, L. Deng, B.B. Gupta, H. Wang, C. Choi, A novel CNN based security guaranteed image watermarking generation scenario for smart city applications, Inf. Sci. 479 (2019) 432–447, https://doi.org/10.1016/j.ins.2018.02.060.

[88] M. Du, K. Wang, Y. Chen, X. Wang, Y. Sun, Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things, IEEE Commun. Mag. 56 (8) (2018) 62–67, https://doi.org/10.1109/MCOM.2018.1701148.

[89] C.L. Stergiou, K.E. Psannis, B.B. Gupta, IoT-based Big Data secure management in the Fog over a 6G Wireless Network, IEEE Int. Things J. (2020), https://doi.org/10.1109/JIOT.2020.3033131.

[90] A. Al-Qerem, M. Alauthman, A. Almomani, B.B. Gupta, IoT transaction processing through cooperative concurrency control on fog–cloud computing environment, Soft Comput. 24 (8) (2020) 5695–5711, https://doi.org/10.1007/s00500-019-04220-y.

[91] B.B. Gupta, M. Quamara, An overview of Internet of Things (IoT): architectural aspects, challenges, and protocols, Concurr. Comput., Pract. Exp. 32 (21) (2020) e4946, https://doi.org/10.1002/cpe.4946.

[92] C. Esposito, M. Ficco, F. Palmieri, A. Castiglione, A knowledge-based platform for Big Data analytics based on publish/subscribe services and stream processing, Knowl.-Based Syst. 79 (2015) 3–17, https://doi.org/10.1016/j.knosys.2014.05.003.

[93] J.R. Saura, D. Ribeiro-Soriano, D. Palacios-Marqués, Evaluating security and privacy issues of social networks based information systems in Industry 4.0, Enterp. Inf. Syst. (2021) 1–17, https://doi.org/10.1080/17517575.2021.1913765.

[94] J. Ding, M. Nemati, C. Ranaweera, J. Choi, IoT connectivity technologies and applications: a survey, arXiv preprint, arXiv:2002.12646, https://doi.org/10.1109/ACCESS.2020.2985932, 2020.

[95] X. Caron, R. Bosua, S.B. Maynard, A. Ahmad, The Internet of Things (IoT) and its impact on individual privacy: an Australian perspective, Comput. Law Secur. Rev. 32 (1) (2016) 4–15, https://doi.org/10.1016/j.clsr.2015.12.001.

[96] R. Montella, D. Di Luccio, S. Kosta, A. Castiglione, A. Maratea, Security and storage issues in Internet of floating things edge-cloud data movement, in: International Conference on Parallel Processing and Applied Mathematics, Springer, Cham, 2019, September, pp. 111–120.

[97] K.M. Law, A.W. Ip, B.B. Gupta, S. Geng (Eds.), Managing IoT and Mobile Technologies with Innovation, Trust, and Sustainable Computing, CRC Press, 2021.

[98] F. Amato, A. Mazzeo, V. Moscato, A. Picariello, A recommendation system for browsing of multimedia collections in the internet of things, in: Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence, Springer, Berlin, Heidelberg, 2013, pp. 391–411.

[99] A. Tewari, B.B. Gupta, Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework, Future Gener. Comput. Syst. 108 (2020) 909–920, https://doi.org/10.1016/j.future.2018.04.027.

[100] M. Tao, J. Zuo, Z. Liu, A. Castiglione, F. Palmieri, Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes, Future Gener. Comput. Syst. 78 (2018) 1040–1051, https://doi.org/10.1016/j.future.2016.11.011.

[101] M. Quamara, B.B. Gupta, S. Yamaguchi, MQTT-driven remote temperature monitoring system for IoT-based smart homes, in: 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), IEEE, 2019, October, pp. 968–970.

[102] A. Perrot, R. Bourqui, N. Hanusse, F. Lalanne, D. Auber, Large interactive visualization of density functions on big data infrastructure, in: 2015 IEEE 5th Symposium on Large Data Analysis and Visualization (LDAV), IEEE, 2015, October, pp. 99–106.

[103] W. Kerber, Data sharing in IoT ecosystems and competition law: the example of connected cars, J. Compet. Law Econ. 15 (4) (2019) 381–426, https://doi.org/10.1093/joclec/nhz018.

[104] M. Méndez-Picazo, M. Galindo-Martín, M. Castaño-Martínez, Effects of sociocultural and economic factors on social entrepreneurship and sustainable development, J. Innov. Knowl. 6 (2) (2021) 69–77, https://doi.org/10.1016/j.jik.2020.06.001.

[105] K.S. Al-Omoush, V. Simón-Moya, J. Sendra-García, The impact of social capital and collaborative knowledge creation on e-business proactiveness and organizational agility in responding to the COVID-19 crisis, J. Innov. Knowl. 5 (4) (2020) 279–288, https://doi.org/10.1016/j.jik.2020.10.002.

[106] A. Ghahtarani, M. Sheikhmohammady, M. Rostami, The impact of social capital and social interaction on customers' purchase intention, considering knowledge sharing in social commerce context, J. Innov. Knowl. 5 (3) (2020) 191–199, https://doi.org/10.1016/j.jik.2019.08.004.