User-centric IoT: challenges and perspectives

Wafa Abdelghani, Corinne Amel Zayani, Ikram Amous, Florence Sèdes

▶ **To cite this version:**

Wafa Abdelghani, Corinne Amel Zayani, Ikram Amous, Florence Sèdes. User-centric IoT: challenges and perspectives. Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2018), Jun 2019, Athens, Greece. pp.27-34. hal-02299242

HAL Id: hal-02299242
https://hal.science/hal-02299242

Submitted on 27 Sep 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

OATAO is an open access repository that collects the work of Toulouse researchers and makes it freely available over the web where possible

This is an author's version published in: http://oatao.univ-toulouse.fr/23843

To cite this version:

Abdelghani, Wafa and Zayani, Corinne Amel and Amous, Ikram and Sèdes, Florence : User-centric IoT: Challenges and Perspectives, UBICOMM 2018 : The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 02-06 juin 2019, Athens, Greece

Any correspondence concerning this service should be sent to the repository administrator: tech-oatao@listes-diff.inp-toulouse.fr

User-centric IoT: Challenges and Perspectives

Abdelghani Wafa*, Corinne Amel Zayani†, Ikram Amous† and Florence Sèdes*
*Paul Sabatier University, IRIT, Toulouse, France
Emails: {wafa.abdelghani, florence.sedes}@irit.fr
† Sfax University, MIRACL, Sfax, Tunisia
Emails: {corinne.zayani, ikram.amous}@isecs.rnu.tn

***Abstract*—The Internet of Things (IoT), this emerging technology connecting everyone, and everyones 'things', is not about objects, gadgets, databases, applications and profits t o b e m ade f rom it, but about people it enriches. Researchers, developers, industries, telecommunication companies, and scientific c ommunities have been interested in this paradigm and have proposed different solutions from different perspectives. They are mainly focused on the technical level, like performance, interoperability, integration, etc. However, whenever use cases are targeting human users, the focus must not be merely on these sides, but on human factors as well. Thus, it is essential to apply a user-centric approach allowing identification o f a pplication-specific features and understanding users needs, motivations and beliefs. This survey aims at encouraging other IoT system developers and researchers to pay attention to the relationship between people and IoT systems. We emphasize the value of adopting a user-centric vision. The goal is not to provide solutions, but rather to raise the right issues.**

Keywords–Internet of Things; User-centric Internet of Things; Social Internet of Things; Social Cyberspace; Internet of People.

I. Introduction

The Internet of Things is a computing concept that describes the idea of everyday physical objects being connected to the Internet and being able to identify themselves to other devices. IoT is expected to be dominated by huge content-oriented traffic, i ntensive i nteractions b etween b illions o f persons often on the move and heterogeneous communications among hosts and smart objects [1]. It provisions millions of services, with strict real-time requirements and striking flexibility i n c onnecting e veryone a nd everything.

Interconnected things, such as sensors or mobile devices sense, monitor and collect all kinds of data about human social life. Those data can be further aggregated, fused, processed, analyzed and mined in order to extract useful information to enable intelligent and ubiquitous services [2].

This paradigm is the result of the evolution of a whole range of new trends following undeniable progress at different levels, such as the evolution of mobile and ubiquitous technologies, the evolution of sensors, wireless and cellular communication networks, as well as the evolution of data storage and processing technologies (Cloud Computing, Big Data, etc.).

Researchers, developers, industries, telecommunication companies, and scientific c ommunities h ave b een interested in this paradigm and have proposed different solutions from different perspectives. They have tried to deal with different problems, such as the heterogeneity of involved devices and communication protocols [3] [4], the security of communications and the minimization of energy consumption [5].

Nevertheless, consumption of IoT products and services remains above expectations [6]. It must be admitted that the user is somewhat excluded. The user is at the heart of IoT systems. It is both the source of data and the consumer. Adopting a user-centric vision is, therefore, a promising new trend. Advantages are numerous. Navigability and resources discovery are improved [7]. Scalability and heterogeneity problems are addressed [8]. The quantity and the variety of contextual data are increased [7] and the community is exploited to establish trustworthiness [9].

We wish through this survey to focus on the user-centric IoT. We emphasize the value of adopting such a vision, we study the user-centric IoT environments, the user in such a context, his needs, and barriers and obstacles to the acceptance of IoT products and services from users' point of view. The goal is not to provide solutions, but rather to raise the right issues.

The remainder of the paper is organized as follows. In Section 2, we introduce and compare different visions of the IoT paradigm and we underline and classify its main challenges. In Section 3, we focus on the user-centric IoT. We define the user in such a context, we report related paradigms and we underline highlights and advantages of adopting such vision. In Section 4, we report and analyze IoT challenges from a user vision. In Section 5, we compare researchers challenges with users challenge to give a glance at the open issues on which research should focus more. Conclusion and future research hints are given in Section 6.

II. Internet of Things

The IoT is emerging as one of the major trends shaping the development of technologies in the information and communication sector at large [5]. The shift from an Internet used for interconnecting end-user devices to an Internet used for interconnecting physical objects that communicate with each other and/or with humans in order to offer a given service, implies to rethink again about conventional approaches usually used in networking, computing and service provisioning.

The IoT is a technological phenomenon generated by innovative advancements in information and communication technologies related to: (i) Ubiquity, (ii) Pervasiveness and (iii) Ambient Intelligence [10].

A. One Paradigm, Many Visions

Manifold definitions of IoT are suggested from the research community which testifies to the complexity and to the multi-disciplinarity of this paradigm. The term IoT is broadly used to refer to:

- The global network connecting smart things through extended Internet technologies.
- The set of technologies supporting such a vision (e.g., Radio Frequency IDentification (RFIDs), sensors, actuators, machine-to-machine communication devices, etc.)
- The set of applications and services leveraging such technologies to give birth to new industrial opportunities [5].

From a *device-centric perspective*, the IoT is based on the concept of smart things, which are able to sense, detect or measure physical phenomena (e.g., temperature, light, etc.) or to perform actions having an effect on the real world [5]. This encompasses devices considered in RFID research [11], as well as those considered in Wireless Sensor Networks and Sensor/Actuator Networks [12] [13].

From a *network-centric perspective*, the IoT can be considered as a highly heterogeneous, dynamic and distributed networked system, composed of a great number of smart objects generating and consuming data [5].

From a *data-centric perspective*, IoT refers to entities processing as providers and/or consumers of data related to the physical world. This fact motivates the adoption of content-centric network architectures and principles [5].

In literature, many architectures are suggested for representing the IoT. However, the most common and basic adopted architecture is composed of three layers: (i) Physical layer also called perception layer, device layer or sensing layer; (ii) Network layer; and (ii) Application layer also called Service layer. (i) Physical layer concerns identifying, naming, addressing and managing IoT objects. (ii) Network layer encompasses networks and protocols used for allowing IoT objects to communicate and to interact. (iii) Application layer encompasses Data Management and Services Management modules and offers final IoT services to end-users.

B. Underlined Challenges

Although well known for a while, the IoT paradigm is still in its infancy and the road ahead is long. Researchers, projects, and industries are focusing on different issues. We cite in this section the main underlined challenges.

a) ***Heterogeneity and interoperability****:* IoT is characterized by a high heterogeneity at different levels. From *devices level*, IoT is a set of heterogeneous devices expected to present dissimilar capabilities from computational and communication standpoints. Identifying, addressing, naming and managing such devices in a standardized way is the first c hallenge [3] [14].

From a *network-centric perspective*, allowing those devices with various communication capabilities to communicate and interact through various networks and using different communication protocols is the second challenge [4]. It covers basic connectivity issues from the physical layer to the application layer without considering the content of information.

From a *data-centric vision*, IoT is about exchanging and analyzing massive amounts of data, to transform them into useful information and to guarantee interoperability among various applications and services. It is essential to provide data with standardized formats, models and semantic descriptions (meta-data), using well-defined languages. This will enable IoT applications to support automated reasoning, a key feature for enabling the proliferation of such a technology on a wide scale [15].

From a *service-oriented vision*, the main challenge relates to how to integrate and compose functionality provided by smart objects into services. This requires designing: (i) architectures and methods for creating a standardized representation of smart objects able to resolve the heterogeneity of devices/resources and (ii) methods for seamlessly integrating and composing resources/services of smart objects into value-added services for end users [5]. Table I shows the main protocols used for each IoT layer.

TABLE I. PROTOCOLS IN DIFFERENT IOT LAYERS

Application Layer	HyperText Transfer Protocol (HTTP), Constrained Application Protocol (CoAP), Embedded Binary HTTP (EBHTTP), Licklider Transmission Protocol (LTP), Simple Network Management Protocol (SNMP), IP Flow Information Export (IPfix), Domain Name System (DNS), Network Time Protocol (NTP), Secure SHell Protocol (SSH), Device Language Message Specification(DLMS), Distributed Network Protocol (DNP),
Network Layer	Internet Protocol Version 6 (IPv6), Routing Protocol for Low-power (RPL), User Datagram Protocol (UDP), Universal Logging Protocol˜(uIP), Serial Line Internet Protocol (SLIP), IPV6 LowPower wireless Area Network (6LoWPAN)
Physical Layer	IEEE 802.11, IEEE 802.15, IEEE 802.16, Z-Wave, Ultra˜WideBand protocol˜(UWB), Highway Addressable Remote Transducer protocol (WirelessHART), Infrared Data Association protocol(IrDA), Konnex protocol (KNX)

b) ***Scalability****:* As daily objects become connected to a global networked infrastructure, scalability issue arises at different levels, including: *(i) identifying, addressing and managing* due to the size of the resulting system and to the constrained nature of typical IoT devices which do not enable quite memory and computing capabilities; *(ii) data communication and networking* due to the high level of interactions, communications and data exchanges among involved entities; *(iii) information and knowledge management* due to the massive amount of data and information sensed, detected, generated and analyzed and (iv) *service provisioning and management* due to the high number of real-time services execution options that could be available and the need to handle heterogeneous resources [5].

c) ***Energy-optimized solutions****:* For a variety of IoT entities, minimizing the energy to be spent on communication/computing purposes will be a primary constraint [5]. While techniques related to energy harvesting (through piezoelectric materials or micro solar panels) will alleviate devices from constraints imposed by battery, energy remains a scarce resource which may not be wasted and which may be properly and reasonably consumed. Thereby, energy optimization concerns also the network level, because communication is recognized as the most energy-consuming task. It concerns also the application layer which justifies the need to design services, applications, and solutions that tend to optimize energy consumption even at the expense of performance.

*d) **Trust, security and privacy**:* Trust is a multidimensional, multidisciplinary and multifaceted concept. The concept of trust covers a bigger scope than security, thus it is more complicated and difficult to establish. It is also related to the concept of privacy that is the ability of an entity to determine whether, when, and to whom personal information could be disclosed. Trust, security and privacy are highly related crucial issues in emerging information technology areas, such as IoT [16].

A number of studies aim to improve identity trust and achieve privacy preservation in ubiquitous systems such as IoT. Fongen [17] propose a framework for authentication and integrity protection designed for IoT environment in order to ensure scalability and lightweight requirements. Gambs et al. [18] propose an implementation of a specific inference attack called the de-anonymization attack, based on Mobility Markov Chain (MMC). They suggest some distance metrics in order to measure the similitude among two MMCs and aggregate these metrics to create de-anonymizers able to recognize users in an Anonymized Geo-located Data-set. In [19], the authors propose an extended trust protocol to support secure mobility management in order to adapt the network to changes of location and infrastructure. This extension aims to improve fault tolerance capacity, connectivity, dependability and scalability in IP-based Wireless Sensor Networks.

Some other works, focus on data transmission and communication trust which is strongly related to security. A security protocol to support data exchange amongst objects was proposed by [20] and combined with a security framework for enhancing security, trust, and privacy for embedded systems. Lightweight symmetric encryption and asymmetric encryption in Trivial File Transfer Protocol (TFTP) were proposed to make the given protocol appropriate to the constrained nature of IoT devices. In [21], the authors propose mechanisms to ensure security at the network layer and at the application layer and perform an experimental study to identify the most appropriate secure communication mechanism for current sensing platforms. Raza et al. [22] introduce SVELTE, an intrusion detection system for the IoT, implemented and evaluated to permit resiliency face to routing attacks, such as spoofed or altered information, sinkhole, and selective-forwarding.

Some other works aim to establish trust management of a whole and propose various trust frameworks and architectures. In [23], the authors propose a system architecture that offers a solution to several challenges, such as general system security, network security, and application security with respect to basic information security requirements (confidentiality, integrity, availability, authority, non-repudiation, and privacy preservation). Quan et al. [24] propose a trusted architecture for a farmland wireless sensor network which includes four layers: (i) a perception logical layer, (ii) a mark recognition logical layer, (iii) a decision-control logical layer and (v) a trusted interface logical layer. This architecture aims to afford trusted and reliable data transmission in Wireless Sensor Networks. An IoT architecture investigated by EU FP7 IoT-A project [25] aims to consider both service privacy and IoT access security aspects for dealing with service accommodation, identification, and IoT-A platform realizations. Gessner et al. [26] propose a set of trust-enhancing security functional components which covers both basic IoT resources access control and essential functions, such as identity, trust and reputation management. This component composition provides mechanisms for securing communications between subjects to ensure data integrity and confidentiality, service trust and privacy of users.

III. User-Centric Internet of Things

The IoT is a vision of ubiquitous connectivity. With sensors, code, and infrastructure, any object can become networked. But the question we need to ask is: should they be? And if so, how? Public debate over the IoT is polarized. Commentators tend to voice either excessive optimism or total pessimism, with precious little in between.

Optimists describe IoT as a magical realm of "enchanted objects", where our possessions gently anticipate our every need. The other camp paints a darker picture. They claim that, at best, the IoT is just another excuse for rampant consumerism, whose only contribution will be to clog basements with yet more unnecessary junk. They affirm that everyday household objects will be turned into enemy spies, placing us under constant surveillance. We will be nudged and manipulated at every moment. Our lives and possessions will be perpetually exposed to hackers.

The solution is intuitive: we need to forget about things. We need to stop obsessing over smart objects and start thinking smart about people. This is the true potential of the IoT. It could put our vast stores of tacit embodied knowledge to work online. It could unite the physical and digital worlds. It also could put us in control of our own information and contextual integrity, against a moral and political backdrop that is resolutely committed to human rights, the rule of law and social cohesion. It could become an Internet, not of smart things, but of smart empowered people.

A. The User in Intelligent Systems

The user is a human, defined by different characteristics: his name, his age, the country where he lives, his Job, his school level, but also his interests, his domains of expertise and his preferences. In computing systems, all these characteristics are classically represented by a profile. The user is also represented by the context where he evolves. A user context includes his location, his current activity, objects and other users in proximity but also his social context. The social context of a user is represented by a set of social relationships entertained with other users and forming the user social networks.

In intelligent systems, the user plays several roles. He is both the source of information, the provider of services and the consumer. The user is therefore in the heart of these processes. That is why some paradigms have appeared giving focus to the user. Several works focus on detecting user profile [27], user social characteristics [28] [29] and to adapting treatments and process to user context [30]. Those works can be reused to achieve a user-centric IoT.

B. Related Paradigms

In this section, we will address some new IoT paradigms aiming to give focus to the user.

1) Internet of People: Miranda et al. [31] define the Internet of People (IoP) as bringing the IoT closer to people in order to easily integrate into it and fully exploit its benefits. This new paradigm aims to put people at the center of innovation strategies and be able to make a profit from the power of

collective intelligence. More than just smart applications and smart cities, the potential of IoP resides in smart people. IoP includes numerous topics, such as Biometric Sensors and Identification Technology, Wearable Technology, Brain Informatics Processing, Body Area Network technology, Social Computing, and Collective Intelligence, Technology for Biomedical and healthcare application etc.

In [31], the authors define a set of features they believe are essential foundations for any approach to the IoP: (i) IoP should be social and let devices interact with each other and with people more socially than does the IoT; (ii) IoP should be personalized which mean that interactions must be personalized to users sociological profiles and contexts; (iii) IoP should be proactive and not manually commanded by the user; (iv) IoP should be predictable which means that interactions must be triggered according to a predictable context that the user has previously identified, and for which a specific behavior has been defined.

2) Social Internet of Things: IoT embodies a large number of smart objects that, through standard communication protocols and unique addressing schemes, provide information and services to final users. Making objects smart was only the first step of an evolutionary process that affected modern communication devices and has been triggered by the advent of IoT in the telecommunication scenarios [1].

The second step consists of the evolution of objects with a certain degree of smartness to objects with an actual social consciousness. These objects can interact with the surrounding environment and feature a pseudo-social behavior with neighbors or within circles and communities. The third step consists of the birth of social objects that act in a social community of objects and devices giving birth to the Social Internet of Things (SIoT) [1].

SIoT objects are able to autonomously establish relationships with other objects, to join communities and to build their own social network which may be different from their owner's ones. SIoT has the potential to support novel applications and networking services for the IoT in more effective and efficient ways. Thus, within a given social network of objects, a key objective will be to publish information/services, find them, and discover novel resources to better implement services also through an environmental awareness. This can be achieved by navigating a social network of friend objects instead of relying on typical Internet discovery tools that cannot scale to trillions of future devices [1].

Short, SIoT permit to address some IoT challenges, such as scalability and heterogeneity, to allow trust-based social relationships among people and objects, to improve objects navigability and discovery by narrowing down its scope to a manageable social network of everything and to increases the quantity and the variety of contextual data

3) Physical Cyber Social Computing: [32] propose Physical-Cyber-Social (PCS) computing, that takes a human-centric and holistic view of computing by analyzing observations, knowledge, and experiences from physical, cyber, and social worlds. Some of the main challenges in healthcare, sustainability, crime prevention, and mitigation require a holistic approach to computing for providing actionable information. With the increased digitization of the physical world culminating in a massive data generated from sensors, mobile devices, and personal/social observations has led to a deeper view into our physical, cyber, and social worlds. The data generation rate has surpassed the ability to store all observations. PCS computing is envisioned to derive insights from these observations to provide actionable information to humans. Providing actionable information by taking a human-centric approach is the vision of PCS computing.

4) People as a Service: [33] People as a Service (PeaaS) is a mobile-centric computing model that allows a users sociological profile to be generated, kept, and securely provided as a service to third parties directly from a Smart-phone. PeaaS emphasizes smart-phones capabilities and relies on them for inferring and sharing sociological profiles. These profiles are not disclosed and are preserved on the device, making it easier for owners to keep their virtual identity under their own control and to preserve them privacy while still enabling third parties to make profit from users identities.

Serving individuals virtual sociological profiles through Smart-phones are different from other mobile-centric models that only provide data, such as GPS localization and temperature. PeaaS allows a variety of information to be collected, such as moods, tendency, preferences, social statuses, daily habits and health habits of a group of peoples in order to delimit their digital projection. However, filtering and analyzing this information to infer users characteristics and specificity or to generate relevant information is not a trivial task. Various techniques, including activity recognition approaches and affective computing, are used in PeaaS for building the richest sociological profile possible [33].

5) Social Devices: Social Devices is an IoT model, introduced by [34]. The motivation behind the model was that smart-phones have not only a lot of information about their owners, but also modalities that enable them to resemble humans. They can translate text into speech, for example. At present, Social Devices concept is supported by a middleware platform. This allows proactive triggering of interactions between devices of co-located people. Additionally, it offers a complete set of Web-based tools to define interactions and their triggering contexts.

6) Social Sensing: Social Sensing is an integral paradigm of the IoT when objects being tracked are associated with individual people. Mobile phones, smart watches, smart glasses, and wearable sensors are good examples of sensing objects. Such paradigms have tremendous value in enabling social networking paradigms in conjunction with sensing. The growing capability of basics hardware to track a wide variety of daily data, such as location, speed, and video leads to tremendous opportunity in enabling a connected and pervasive world of users that are ubiquitously connected to the Internet [35].

C. Highlights and Advantages

Adopting a user-centric vision is, therefore, a promising new trend. Advantages are numerous.

- Navigability and resources discovery are improved by narrowing down them scopes to a manageable social network of everything [7].
- Some IoT challenges, such as scalability and heterogeneity are addressed [7].
- The scalability is guaranteed like in human social networks [8] and the heterogeneity of devices, network

and communication protocols is resolved by the use of social networks.

- A larger data source becomes available as it comes from a set of users, a network of users, or a community rather than from a single user.
- The continuous feed of data from communities gives us big data team [9] and the quantity and the variety of contextual data is increased allowing improved services intelligence and adaptability to users' situational needs [7].
- A better user adaptation that will lead to the increased consumption of IoT products [9] and a better information filtering become possible, because communities of objects collaborate to provide a common view [36].
- Models designed to study social networks can be reused to address IoT related issues (intrinsically related to extensive networks of interconnected objects) [8].
- The focus and the consideration of user-side challenges will increase the acceptability of IoT products.
- The community is exploited to rate the trustworthiness of potential providers of information and services [36]. So, a level of trustworthiness can be established for leveraging the degree of interaction among things that are friends [8].

IV. IoT Challenges and Perspectives: A User Vision

The high cost of intelligent devices is one of the problems posed by users. According to statistics [37] drawn up in 2014 on a sample of 2000 French users, 59 % of users consider the price of IoT devices as one of the greatest constraints. High prices are not the only constraint. Indeed, the price constraint can disappear if these objects become useful and necessary. We expose in this section the main IoT challenge from the users point of view. We have relied on statistics and have chosen in this section the most cited users' problems, including the usefulness and usability of connected objects but also and above all, their ability to respect the users' privacy.

A. Utility

The majority of users find that these smart objects are not useful enough and that they do not bring much to their daily lives. The same statistic [37] show that 45 % of all users questioned and 52 % of users who are older than 50 years old do not see the usefulness of objects being conveyed, although the number of applications and IoT objects for the health and well-being of the elderly is quite high. Developers, designers, and creators of IoT objects and services are faced with a new challenge: developing more useful and interesting scenarios that can meet the specific need of users.

A study from LAPOSTE [38] carried out with a national sample of 1032 peoples classified areas of IoT applications according to users' expectations. This study revealed that proximity services are at the forefront, followed by home automation services and then health-care and wellness services. According to the same analysis, proximity services allow the rapid intervention of trusted personnel for isolated persons, the keep of elderly or dependents people at home or the safety of children. For home automation services, 77 % of users surveyed place an emphasis on security and protection against theft and intrusion. 74 % place more emphasis on fire risk services and energy-saving services. As for the field of health and well-being, 45 % of users give importance to services that make it possible to practice a sporting activity regularly. Another study [6], classifies health-care services on the first position, security management services on the second position and home automation and energy consumption management services in the third position.

The cited study [37] tried to clarify which prototype of users are most willing to use connected objects and which connected objects are most used. This study found that 23% of users interviewed have at least one intelligent object. For the most part, the latter are men, receiving a wage of more than 1500 euro and living for the most part in the Paris region. This study ranked the object "connected weather station" at the top of the list of most used intelligent objects. In the second position are connected gas, electricity and water meters, connected watches and bracelets, and connected alarm systems. In the third position, connected sphygmomanometers and scales, connected sockets and remotely controllable heating systems. Other objects are also used, such as connected refrigerators, but also connected baby monitors (which monitors babies quality of sleep) and connected baby scales (which monitor the growth curve of a baby).

Note that other areas are neglected and little known by users. Let us mention, for example, the field of transport and vehicular networks, although it is quite developed. We also note that applications and devices using the social environment of the user or the notion of collaboration are few.

B. Usability

The usability or the ease of use of connected objects and IoT services is also one of the brakes to the acceptability of these products by consumers. Indeed, a study [38] affirms that 74 % of users perceive the multiplication of applications to control each object as a brake on the purchase and use of the latter. Another study [39] shows that nearly 12 % of users who do not have connected objects say that it is useless to buy objects that are not compatible with all types of computers and Smart-phones. 15% say it is not easy to manage multiple connected objects at the same time. 9 % say they do not know how to operate these objects.

Establishing interoperability is a potential solution. It makes intelligent objects reconfigurable and autonomous, thus minimizing human intervention. It also allows easier control and management when it comes to a large number of objects. Integration of the social component and contextualization also present possible solutions to increase the quantity and variety of data in order to offer more intuitive, intelligent, personalized and adapted services.

C. Trust and Privacy

The mentioned study [39] tries to classify the brakes to the acceptance of IoT objects by users. 43% of users queried say they are afraid of the use that can be made of their personal data. 18 % find that the connected objects are not operational. 8 % believe they are unreliable. The second cited survey [6] joins the first one and states that: 33 % of the users questioned are afraid of what is done with the data collected by IoT objects; 19 % find that these objects quickly become obsolete and 17 % find they are not very efficient and very reliable.

The number increases when it comes to some more critical areas, especially the health field. Indeed, a barometer [40] was established in 2016 by the company VIDAL (company dedicated to information on health products), on a sample of 1402 doctors, revealed the following percentages: 33% of doctors surveyed say they have no confidence in healthcare applications and services in terms of securing personal data. 84 of the doctors questioned would not recommend connected health objects to their patients. However, there are a number of factors that could encourage them to advocate benefits, such as certification and labeling of the object (39%), its therapeutic area (37%) and the profile of its manufacturer or designer (8%). Doctors first trust their peers to make healt-related connected objects (scientists societies 67%, university doctors 53% and confreres developers 42%). In addition, certain promotional arrangements are more likely to convince doctors of the adoption of connected health objects. Recommendations made by scientists societies (67%), medical press (58%) and medical congresses (51%) are the most convincing.

Those apprehensions are not unjustified. Some past events confirm the fear of users. The first examples of dysfunctions observed date back to 2011. A pharmaceutical company had to warn its users that the rheumatology calculator application it had developed produced erroneous scores [41]. The following year, another laboratory had to recall its application of calculation of doses of insulin [42]. Then, Apple announced the removal of blood glucose monitoring from its health management application [42]. This has drawn attention to the fact that these solutions are not so simple to implement even for a technology champion.

According to these different statistics, we distinguish two major problems: trust and privacy. We also distinguish three levels of trust: trust in the object or IoT devices, trust in IoT services and applications, trust in the service provider or in the designer of the devices. We also distinguish a fourth level: trust in the recommender of the service or IoT object. We believe that trust management in IoT environments should necessarily consider these four levels in order to improve users' acceptability of IoT products and allow them to overcome their fears and apprehensions.

Several properties can allow measuring trust for each dimension. For example, reliability, connectivity, energy rates permit to measure trust in IoT devices and objects. Quality of Services (QoS), functional characteristics and non-functional characteristics (delay, availability, throughput, response time, etc.) permit to measure trust in IoT services and applications [43]. Expertise, past experiences, and QoS can be used to measure trust in service providers [44]. And centrality, honesty, and similarity of profile and interest can be used to measure trust in services and objects recommenders [45].

The problem of privacy concerns the protection of users' personal data. Indeed, the huge amounts of data that are collected by the connected objects with sensors, are usually stored on the Cloud and thus become exposed. The user must be able to control and choose whether or not to give access to his information. The de-anonymization techniques also make it possible to reduce this problem. Indeed, with these techniques, the majority of the data remains exposed, but the data which makes it possible to identify to whom they belong (name, address, age, etc.) are suppressed or hidden.

V. Synthesis

Some users' challenges are addressed by researchers, such as trust and privacy. However, the proposed solutions remain intangibles by users. Giving users the hand to participate in setting their own rules, the same way as proposed in social media, might be a potential solution. Reusing works and researches conducted in the context of usable security [46] [47] and usable privacy [48] [49] allows to resolve those challenges.

Ensuring interoperability and resolving heterogeneity can help to improve the usability of connected objects, but this is not a radical solution. We can have different solutions, such as applying HMI solutions [50] [51] which permit to have cognitive and adaptable users' interfaces, especially when use cases are targeting elderly and disabled persons.

Utility is a problem that is almost neglected, although it may be the key to improving the acceptability of connected objects by users. Researchers should focus on finding scenarios and use cases that can interest and motivate users.

VI. Conclusion

The IoT is emerging as one of the major trends shaping the development of the technologies sector at large. Researchers, developers and, industries have been interested in the IoT paradigm and have proposed different solutions for different issues, such as heterogeneity, scalability, and energy optimization.

Nevertheless, consumption of IoT products and services remains below expectations. Indeed, according to several studies and statistics, users claim other problems such as the cost of connected objects, but also and above all, their utility and usability. These problems are not addressed by researchers. Users also express their fears about the privacy of their personal data and do not trust connected objects. The problems of privacy and trust are addressed in the literature, however, the proposed solutions remain intangible by users.

We tried in this work to address these problems and to indicate some solution and some horizons of research.

Acknowledgment

This work was financially supported by the PHC Utique program of the French Ministry of Foreign Affairs and Ministry of higher education and research and the Tunisian Ministry of higher education and scientific research in the CMCU project number 18G1431.

References

[1] W. Abdelghani, C. Zayani, I. Amous, and F. Sèdes, "Trust management in social internet of things: a survey," in Conference on e-Business, e-Services and e-Society. Springer, 2016, pp. 430–441.

[2] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social internet of things," in Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on. IEEE, 2012, pp. 18–23.

[3] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. IEEE, 2012, pp. 1282–1285.

[4] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, "A cross-layer communication module for the internet of things," Computer Networks, vol. 57, no. 3, 2013, pp. 622–633.

[5] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad hoc networks, vol. 10, no. 7, 2012, pp. 1497–1516.

[6] OpinionWay, "Les franais et les objets connectés (french people and connected objects)," https://drive.google.com/file/d/0B6mEkutxBkwnXzlvQmpKLWZSNHc/view, 03 2016, accessed: 2018-02-09.

[7] D. H. Ali, "A social internet of things application architecture: applying semantic web technologies for achieving interoperability and automation between the cyber, physical and social worlds," Ph.D. dissertation, Institut National des Télécommunications, 2015.

[8] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer networks, vol. 56, no. 16, 2012, pp. 3594–3608.

[9] S. Geetha, "Social internet of things," World Scientific News, vol. 41, 2016, p. 76.

[10] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in Seventh International Conference on Information Technology: New Generations (ITNG). IEEE, 2010, pp. 804–809.

[11] G. Roussos and V. Kostakos, "Rfid in pervasive computing: state-of-the-art and outlook," Pervasive and Mobile Computing, vol. 5, no. 1, 2009, pp. 110–131.

[12] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, 2002, pp. 393–422.

[13] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges," Ad hoc networks, vol. 2, no. 4, 2004, pp. 351–367.

[14] C. Sun, "Application of rfid technology for logistics on internet of things," AASRI Procedia, vol. 1, 2012, pp. 106–111.

[15] D. Singh, G. Tripathi, and A. J. Jara, "A survey of internet-of-things: Future vision, architecture, challenges and services," in Internet of things (WF-IoT), 2014 IEEE world forum on. IEEE, 2014, pp. 287–292.

[16] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," Journal of network and computer applications, vol. 42, 2014, pp. 120–134.

[17] A. Fongen, "Identity management and integrity protection in the internet of things," in 2012 third international conference on emerging security technologies. IEEE, 2012, pp. 111–114.

[18] S. Gambs, M.-O. Killijian, and M. N. del Prado Cortez, "De-anonymization attack on geolocated data," Journal of Computer and System Sciences, vol. 80, no. 8, 2014, pp. 1597–1614.

[19] A. J. Jara, L. Marin, A. F. Skarmeta, D. Singh, G. Bakul, and D. Kim, "Mobility modeling and security validation of a mobility management scheme based on ecc for ip-based wireless sensor networks (6lowpan)," in 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. IEEE, 2011, pp. 491–496.

[20] M. A. M. Isa, N. N. Mohamed, H. Hashim, S. F. S. Adnan, J. Manan, and R. Mahmod, "A lightweight and secure tftp protocol for smart environment," in Computer Applications and Industrial Electronics (ISCAIE), 2012 IEEE Symposium on. IEEE, 2012, pp. 302–306.

[21] J. Granjal, E. Monteiro, and J. S. Silva, "On the effectiveness of end-to-end security for internet-integrated sensing applications," in Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, 2012, pp. 87–93.

[22] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," Ad hoc networks, vol. 11, no. 8, 2013, pp. 2661–2674.

[23] H. Ning, H. Liu, and L. Yang, "Cyber-entity security in the internet of things," Computer, 2013, p. 1.

[24] Z. Quan, F. Gui, D. Xiao, and Y. Tang, "Trusted architecture for farmland wireless sensor networks," in Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. IEEE, 2012, pp. 782–787.

[25] D. Seal, ARM architecture reference manual. Pearson Education, 2001.

[26] D. Gessner, A. Olivereau, A. S. Segura, and A. Serbanati, "Trustworthy infrastructure services for a secure and privacy-respecting internet of things," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012, pp. 998–1003.

[27] R. Z. Rebaï, L. Ghorbel, C. A. Zayani, and I. Amous, "An adaptive method for user profile learning," in East European Conference on Advances in Databases and Information Systems. Springer, 2013, pp. 126–134.

[28] M. Mezghani, A. Péninou, C. A. Zayani, I. Amous, and F. Sèdes, "Analyzing tagged resources for social interests detection," International Conference on Enterprise Information Systems, 04 2014, pp. 340 – 345.

[29] D. Tchuente, M.-F. Canut, N. Jessel, A. Péninou, and F. Sèdes, "Dérivation de profils utilisateurs à partir de réseaux sociaux: une approche par communautés de réseaux égocentriques (derivation of user profiles from social networks: a community approach of egocentric networks)," Ingénierie des systèmes d'information, vol. 18, no. 1, 2013, pp. 11–37.

[30] E. Khanfir, C. El Hog, R. B. Djmeaa, and I. A. B. Amor, "A web service selection framework based on user's context and qos," in Web Services (ICWS), 2014 IEEE International Conference on. IEEE, 2014, pp. 708–711.

[31] J. Miranda et al., "From the internet of things to the internet of people," IEEE Internet Computing, vol. 19, no. 2, 2015, pp. 40–47.

[32] A. Sheth and P. Anantharam, "Physical cyber social computing for human experience," in Proceedings of the 3rd International Conference on Web Intelligence, Mining and Semantics. ACM, 2013, p. 1.

[33] J. Guillen, J. Miranda, J. Berrocal, J. Garcia-Alonso, J. M. Murillo, and C. Canal, "People as a service: a mobile-centric model for providing collective sociological profiles," IEEE software, vol. 31, no. 2, 2014, pp. 48–53.

[34] N. Mäkitalo et al., "Social devices: collaborative co-located interactions in a mobile cloud," in Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia. ACM, 2012, p. 10.

[35] C. C. Aggarwal, N. Ashish, and A. Sheth, "The internet of things: A survey from the data-centric perspective," in Managing and mining sensor data. Springer, 2013, pp. 383–428.

[36] L. Atzori, A. Iera, and G. Morabito, "From" smart objects" to" social objects": The next evolutionary step of the internet of things," IEEE Communications Magazine, vol. 52, no. 1, 2014, pp. 97–105.

[37] IFOP, "Les franais et la mobilité digitale (the french and digital mobility)," http://www.ifop.com/media/poll/2846-1-study_file.pdf, 04 2014, accessed: 2018-02-09.

[38] LaPoste, "Objets connectés: Ce qu'en attendent les franais (connected objects: What the french expect)," https://www.docapost.com/wp-content/uploads/2015/01/infographie-la-poste-generique.pdf, 12 2014, accessed: 2018-02-09.

[39] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," IEEE Transactions on knowledge and data engineering, vol. 26, no. 5, 2014, pp. 1253–1266.

[40] VIDAL, "L'utilisation de smartphones par les médecins (the use of smartphones by doctors)," http://www.vidalfrance.com/wp-content/download/info/Barometre_Mobile-VIDAL-CNOM-2016.pdf, 3 2016, accessed: 2018-02-09.

[41] A. Morris, Medical Research and Technology, ser. Cutting-Edge Science and Technology. ABDO Publishing Company, 2016. [Online]. Available: https://books.google.tn/books?id=N1kgCwAAQBAJ

[42] B. Patrick and L. Jacques, "Connected health: From e-health to connected health," CNOM, Tech. Rep., 06 2015.

[43] J. B. Bernabe, J. L. H. Ramos, and A. F. S. Gomez, "Taciot: multidimensional trust-aware access control system for the internet of things," Soft Computing, vol. 20, no. 5, 2016, pp. 1763–1779.

[44] N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, "From personal experience to global reputation for trust evaluation in the social internet of things," in GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017, pp. 1–7.

[45] R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," IEEE transactions on dependable and secure computing, vol. 13, no. 6, 2016, pp. 684–696.

[46] S. Lee, "A study on the need of the usable security in the corelation between it security and user experience," International Journal of Internet, Broadcasting and Communication, vol. 9, no. 4, 2017, pp. 14–18.

[47] P. Realpe-Muñoz, C. A. Collazos, T. Granollers, J. Muñoz-Arteaga, and E. B. Fernandez, "Design process for usable security and authentication

using a user-centered approach," in Proceedings of the XVIII International Conference on Human Computer Interaction. ACM, 2017, p. 42.

[48] H. Harkous, "Data-driven, personalized usable privacy," EPFL, Tech. Rep., 2017.

[49] J. Angulo, S. Fischer-Hübner, E. Wästlund, and T. Pulls, "Towards usable privacy policy display and management," Information Management & Computer Security, vol. 20, no. 1, 2012, pp. 4–17.

[50] U. E. Manawadu, M. Kamezaki, M. Ishikawa, T. Kawano, and S. Sugano, "A multimodal human-machine interface enabling situation-adaptive control inputs for highly automated vehicles," in Intelligent Vehicles Symposium (IV), 2017 IEEE. IEEE, 2017, pp. 1195–1200.

[51] J. D. Bauer, H. F. I. Kenneth, and R. N. Flores, "Intelligent human-machine interface," Jun. 21 2011.