Safe Use of the Internet of Things for Privacy Enhancing

Hodjat Hamidi*
Department of Industrial Engineering, K. N. Toosi University of Technology, Tehran, Iran
h_hamidi@kntu.ac.ir

Received: 28/Feb/2016 Revised: 27/May/2016 Accepted: 18/Jul/2016

Abstract

New technologies and their uses have always had complex economic, social, cultural, and legal implications, with accompanying concerns about negative consequences. So it will probably be with the IoT and their use of data and attendant location privacy concerns. It must be recognized that management and control of information privacy may not be sufficient according to traditional user and public preferences. Society may need to balance the benefits of increased capabilities and efficiencies of the IoT against a possibly inevitably increased visibility into everyday business processes and personal activities. Much as people have come to accept increased sharing of personal information on the Web in exchange for better shopping experiences and other advantages, they may be willing to accept increased prevalence and reduced privacy of information. Because information is a large component of IoT information, and concerns about its privacy are critical to widespread adoption and confidence, privacy issues must be effectively addressed. The purpose of this paper is which looks at five phases of information flow, involving sensing, identification, storage, processing, and sharing of this information in technical, social, and legal contexts, in the IoT and three areas of privacy controls that may be considered to manage those flows, will be helpful to practitioners and researchers when evaluating the issues involved as the technology advances.

Keywords: Security Issues; IoT; Information; Technology Advances; Privacy Enhancing.

1. Introduction

Security issues are central in Internet of Things as they may occur at various levels, investing technology as well as ethical and privacy issues. To ensure security of data, services and entire IoT system, a series of properties, such as confidentiality, integrity, authentication, authorization, non-repudiation, availability, and privacy, must be guaranteed [1]. This is extremely challenging due to the Internet of Things environmental characteristics. In the past privacy was of relatively little concern because location information was not pervasively and continuously available. Now that technology has radically altered information availability, privacy of location is closely tied to controlling access to this information, and people want to be in control of the information availability [2-3]. Privacy preferences are now quite well studied in the context of users carrying mobile devices [4] but not extended through an IoT context where device-to-device communication can carry location information far beyond users' awareness. Privacy concerns are becoming an increasingly critical issue in the IoT [5]. Without assurance of privacy in a world of interconnected sensors and systems, users will be unwilling to adopt these new technologies [6]. The International Telecommunications Union report on the Internet of Things notes that "Concerns about privacy and data protection are widespread, particularly as sensors and smart tags can track a user's movements, habits, and preferences on a perpetual basis." [7] Despite its relevance and importance, privacy is not yet receiving adequate attention in the enthusiasm to exploit the technical capabilities of the IoT. A recent survey of IoT literature covering 127 journal and conference papers [8] finds only nine security and three privacy-related documents in its category of IoT challenges [9] [5] [10]. A recent survey of IoT context aware computing describes security and privacy as a major concern, yet finds only 11 of 50 surveyed research prototypes incorporating security and privacy functionality [11].

The paper is organized as follows: Section 2 presents the components in the Internet of Things. In Section 3, the security in IoT and data confidentiality is explained. In Section 4, theory concepts of privacy in IoT is introduced. Phases and associated privacy for IoT is discussed in section 5. The challenges in IoT: privacy and security are presented in Section 6. The privacy and humanness is discussed in section 7. Section 8 gives the discussion of the study. Conclusion is given in Section 9.

2. Components in the Internet of Things

The IoT vision enhances connectivity from "any-time, any-place" for "any-one" into "any-time, any-place" for "any-*thing*" [12]. Once these things are plugged into the network, more and more smart processes and services are possible which can support our economies, environment, security and health.

Fig.1 provides a view of the IoT ecosystem [13]. Things could be tagged, and through scanners, identified, and the relevant location information could be

* Corresponding Author

communicated. Similarly, networked things with sensors become smaller, weaving themselves into our daily lives, while sensor and actuator networks act on the local environment, communicating status and events to a higher level service. Smart things sense activity and status, linking it to the IoT. Middleware and frameworks enabling application and service development which utilise data as received from (or about) things, most often living in the cloud provide the capability to add intelligence resulting in better services, which ultimately impact on the environment.

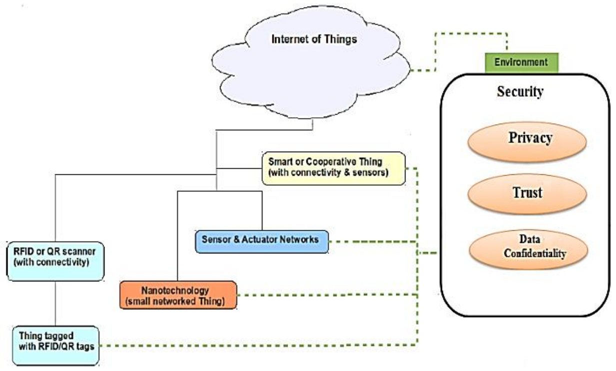
Internet of Things
Environment
Security
Privacy
Trust
Data Confidentiality
Smart or Cooperative Thing (with connectivity & sensors)
Sensor & Actuator Networks
RFID or QR scanner (with connectivity)
Nanotechnology (small networked Thing)
Thing tagged with RFID/QR tags

Fig. 1. Components in the Internet of Things

3. Security in IoT and Data Confidentiality

Security represents a critical component for enabling the widespread adoption of IoT technologies and applications. Security is divided into three parts (Fig. 2): (1) Data confidentiality, (2) privacy and (3) trust

3.1 Data Confidentiality

Data confidentiality represents a fundamental issue in IoT scenarios, indicating the guarantee that only authorized entities can access and modify data. The main research challenges for ensuring data confidentiality in an IoT scenario relate to: (1) Definition of suitable mechanisms for controlling access to data streams generated by IoT devices. (2) Definition of an appropriate query language for enabling applications to retrieve the desired information out of a data stream. (3) Definition of a suitable smart objects' identity management system.

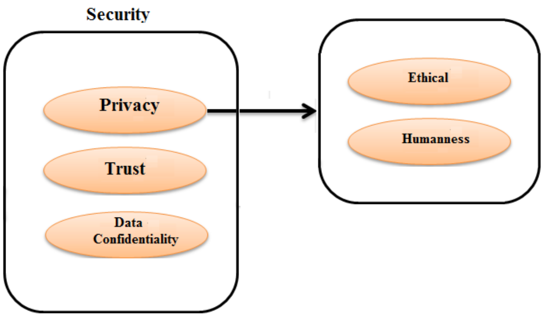

Fig. 2. Security is divided into three parts

4. Theory Concepts of Privacy in IoT

This paper follows and borrows from prior work investigating issues in the development of privacy theory general [14], and extends it to the particular environment of the IoT. Theory concepts has five desirable goals [15]:

1. A method of organizing and categorizing "things," a typology;
2. Predictions of future events;
3. Explanations of past events;
4. A sense of understanding about what causes events; and occasionally mentioned as well:
5. The potential for control of events.

At this early stage we can hardly purport to fully explain and predict the eventual evolution of the recently-emerged IoT, let alone control it—however we can begin to organize and categorize important "things" such as components and concepts.

Consistent with the above, a number of strategies may be used to construct theories, one of which is a classificatory strategy seeking a taxonomy of elements both within and outside the phenomenon [16]. In early stages of theory construction, classification strategies are particularly important and a prerequisite to other strategies [17]. This method follows recommendations from related fields [18], emphasizing discovery and description, where key research questions are "Is there something interesting enough to justify research?" and "What are the key issues?" in both cases with categorization suggested as a procedure to be used [19]. The methods described below will attempt to discover, classify, and describe a number of key issues that relate the IoT and big data to location privacy, and justify the need for additional research.

4.1 Privacy

The privacy may be viewed from many conceptual perspectives [20] and in the context of the present work related to the IoT and big data, we will consider it from an informational privacy perspective.

The informational perspective is key to most privacy theories in a technological context, describing privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [21]. In keeping with this approach, we will look at location privacy in terms of information flows, from sensing to use and including a number of other activities typically in between (including more complex interactions between flows).

Tables 1 and 2 use the five phases of information flow enumerated in Table 1 and identifies example privacy controls for each phase. The five phases extend early work from more than 45 years ago identifying three phases of input, storage and output [22]. They also extend five phases discussed in [23] by explicitly adding the "processing" phase to acknowledge the important of inference capabilities and data analytical techniques that may deduce location from other available evidence.

The privacy-enhancing controls fall into technical, social, and legal measures, represented in columns of the table. Technical controls are those that control the actual processing of the information and may block, filter, modify, etc. that information. Examples include authenticating, blocking, encrypting, and other privacy protections for RFID tags [24]. Social controls affect privacy information through the influence of accepted business practices, social norms, and similar nontechnical means. These include not only such things as formal privacy policies from system providers, but also behaviors of system users, which have been found to vary considerably according to context such as who the information is exchanged with, whether the person is at home or in a public place, and what means is used to share the information [25]. Legal measures are those that impose formal prohibitions or regulations on activities related to location information flows. These vary greatly by region. In the EU the privacy Directive directly addresses location privacy, while in the US federal law addresses location only indirectly and incompletely [26].

5. Phases and Associated Privacy for IoT

The phases and associated privacy controls are described:

(1) Sensing may be technically blocked by any means that prevents signal transmission or reception.

This includes RFID-blocking wallets, RF blocker tags generating simulated or false RFID tags, etc.

(2) Identification in the IoT has already received significant attention [27] [28]. Legal enforcement of anonymity is almost universally expected and enforced in particular contexts such as election ballot casting.

(3) Storage privacy is enabled through several technical methods, including merely not providing a storage facility and encryption of any stored data. The Snap chat service was touted as an ephemeral means of photo sharing, but was quickly and easily defeated [29]. Social control of stored information is often accomplished (with varying degrees of success and user satisfaction) through user privacy settings in social media. Various jurisdictions may enforce formal legal restrictions on the type, amount, and duration of stored data. A “right to quantitative privacy” has even been proposed [30].

(4) Processing phase technical privacy includes a number of design principles that also apply to other phases [31] and various anonymizing and privacy-enhancing and privacy-preserving technologies [32-34]. It may also be affected on a social and free market level in software terms of service agreements. Formal legal measures include prohibitions or restrictions on database matching and sharing of information between commercial entities.

(5) Sharing phase privacy may be technically implemented by restricting the communications channels available, e.g., not implementing or turning off facilities such as Bluetooth and Wi-Fi. Social measures are largely the responsibility of users to control application settings and follow recommended norms for appropriate sharing. Legal controls for sharing have recently received significant attention—for example the US Federal Trade Commission has just recommended that Congress give consumers more control over the data brokerage industry [35-37] and European courts have required that search engines implement a “right to be forgotten” [38].

Table 1. Information flow phases and associated privacy controls for IoT

Phases	Methods
Identification	-Unique identifier detection -Facial recognition -Vehicle license plate recognition
Processing	-Self-contained inference -Communication and matching
Sharing	-Intentional -Unintentional
Storage	-Object data -Meta data
Sensing	-Triangulation -Scene analysis -Proximity -Indirect inference

Table 2. Privacy measures for IoT

Phases	Social privacy	Technical privacy	Legal privacy
Identification	Anonymous letters to newspaper editors or postings to online discussion forums	address randomization	“Secret” ballots for voting
Processing	Vendor-customer terms of service	Privacy-enhancing technologies: anonymizing, etc.	Restrictions of database matching
Sharing	User and application sharing settings	Restriction or no provision of communication facilities	The “right to forget” Data broker restrictions
Storage	User social media privacy settings	No physical storage -Encryption -Ephemeral storage	Formal limits on amount and duration of stored data
Sensing	Socially acceptable uses for Google Glass [39]	RF blocking wallets	Prohibition of cell phone and camera use at customs [40]

6. Challenges in IoT: Privacy and Security

This section discusses challenges in IoT development by enterprises. As with any disruptive innovation, the IoT will present multiple challenges to adopting enterprises. For example, due to the explosion of data generated by IoT machines, in [40] suggested that data centers will face challenges in security and consumer privacy. This section discusses two technical and managerial challenges: privacy and security.

6.1 Privacy Challenge

As is the case with smart health equipment and smart car emergency services, IoT devices can provide a vast amount of data on IoT users’ location and movements, health conditions, and purchasing preferences-all of which can spark significant privacy concerns. Protecting privacy is often counter-productive to service providers in this scenario, as data generated by the IoT is key to improving the quality of people's lives and decreasing service providers' costs by streamlining operations. The IoT is likely to improve the quality of people's lives. According to the 2014 TRUST Internet of Things Privacy Index, only 22% of Internet users agreed that the benefits of smart devices outweighed any privacy concerns. While the IoT continues to gain momentum through smart home systems and wearable devices, confidence in and acceptance of the IoT will depend on the protection of users' privacy.

6.2 Security Challenge

As a growing number and variety of connected devices are introduced into IoT networks, the potential security threat escalates. Although the IoT improves the productivity of companies and enhances the quality of people's lives, the IoT will also increase the potential attack surfaces for hackers and other cyber criminals. IoT devices have vulnerabilities due to lack of transport encryption, insecure Web interfaces, inadequate software protection, and insufficient authorization. On average, each device contained 25 holes, or risks of compromising the home network. Devices on the IoT typically do not use data encryption techniques.

Some IoT applications support sensitive infrastructures and strategic services such as the smart grid and facility protection. Other IoT applications will increasingly generate enormous amounts of personal data about household, health, and financial status that enterprises will be able to leverage for their businesses. Lack of security and privacy will create resistance to adoption of the IoT by firms and individuals. Security challenges may be resolved by training developers to incorporate security solutions (e.g., intrusion prevention systems, firewalls) into products and encouraging users to utilize IoT security features that are built into their devices.

The evolution of IoT technologies (e.g., chips, sensors, wireless technologies) is in a hyper accelerated innovation cycle that is much faster than the typical consumer product innovation cycle. There are still competing standards, insufficient security, privacy issues, complex communications, and proliferating numbers of poorly tested devices. If not designed carefully, multi-purpose devices and collaborative applications can turn our lives into chaos. To prevent chaos in the hyper-connected IoT world, businesses need to make every effort to reduce the complexity of connected systems, enhance the security and standardization of applications, and guarantee the safety and privacy of users anytime, anywhere, on any device.

Beyond the security challenges mentioned in other parts of this document, we identify specific additional challenges here:

6.2.1 Diverse, Interacting, Potentially Unsecure Devices:

IoT raises a wide range of serious security challenges, since many IoT devices interact closely with the physical world. Recent news has highlighted many opportunities for attack on networked cars, power stations, and implanted medical devices. The security problem is exacerbated by the fact that many IoT devices may be built by companies that have little expertise in security, using potentially old operating systems and libraries that are not fully patched. Furthermore, if a device relies on open-source software with vulnerabilities, updating the firmware on such devices can be difficult.

6.2.2 Devices that Misrepresent Themselves:

Another risk lies in the potential for these diverse devices to be intentionally programmed to "cheat" as was the recent case where Volkswagen was found to have programmed their software to cheat on emissions tests [16]. By cheating, we mean any action that intentionally misrepresents the product's behavior for the purpose of deceiving regulators or consumers. Examples of such cheating might be misrepresenting network bandwidth usage or performance on benchmarks. As we cede more control to these devices the need to regulate them will increase, which will give manufacturers more temptation to cheat. Technologies, procedures, and policies are needed to allow inexpensive and effective auditing of the software in such devices, including methods to specify the expected correct behavior and solutions that allow for inspection of the product source code.

6.2.3 Security Threats from Ubiquitous Devices:

In a world where we are surrounded by IoT devices, the ability to limit our exposure to them decreases. If a desktop computer becomes infected, we can reboot it, run an anti-virus program, and hope the problem goes away. If one or more devices in a network of IoT devices is compromised, it may be both very difficult to know what device has been compromised or how to fix the problem to restore the overall system security. Consider how current ransom ware, which holds our data hostage, might be transformed to an attack that requires us to pay money to enter our own house or turn on the heat. Research on systematic methods for restoring IoT systems from a known good state is needed as well as tools to isolate and correct individual compromised components within the distributed system.

6.2.4 System-wide Security Abstractions:

Programming languages have evolved to incorporate features that increase productivity and reduce classes of errors. For example, Java and C# have features that prevent errors such as buffer overflows by construction – all valid programs are correct with respect to memory safety. Next-generation IoT systems, that involve physical interaction, need to have a new generation of system-wide properties (e.g., to guarantee physical safety) that are correct by construction and checked automatically. These properties involve major improvements in our ability to reason about the interaction between the software in the system and the physics of their real-world actions.

7. Privacy and Humanness

7.1 Ethical Challenges

In Internet of Things exchange environments, there are more data that can be used to define and to influence people. Will these data, which in digital form are coded as strings of zeroes and ones, lead marketers to view consumers strictly as data, slotting them into fixed categories and treating them with sterile precision in accordance to their assignment? And through the acquisition and sharing of these data-perhaps in the end, without much choice by those from whom the data are sourced-will consumers relinquish important aspects that define their humanness, and thus feel less satisfaction? In the context of mortality and being human, Gawande [40] draws upon Dworkin (1986), [41], and his perspective on autonomy to put forth, ‘‘we want to retain the autonomy-the freedom-to be the authors of our lives. This is the very marrow of being human. All we ask is to be allowed to remain the writers of our own story. That story is ever changing. We want to retain the freedom to shape our lives in ways consistent with our character and loyalties.’’ Although he was writing about mortality when framing that ‘‘the battle of being mortal is the battle to maintain the integrity of one’s life’’ [40], we believe it applies when one, through technology and associated data, can be increasingly represented, influenced, and con-trolled and as a result have choices censored. The autonomy of one’s data and thus one’s self should be respected and the individual should be provided freedom of control. We believe that the human condition calls for and requires sufficient privacy. Indeed, privacy and all that it represents or entails is a sine qua non of humanness. Without it, consumers may feel like- and become-empty souls and vessels through which organizations derive profits.

7.2 The Human Condition

Thinking more like a technologist does not suggest thinking less like or about people. In fact, we argue that it becomes more important to consider the human condition when designing technology-based solutions. We believe there is a tendency to use technology as a mass market solution to a problem in which solutions address the major issues or are believed to be robust enough to provide a reasonable solution to any problem. However, such solutions may overlook smaller details or individual preferences that may comprise the long tail and therefore may be less satisfactory than imagined. For example, consider automated phone call-in systems where customers ‘‘Listen closely as options may have changed . . . Press 1 for . . . Press 2 for . . . .’’ It seems like a grand way to handle a large volume of calls on a variety of topics. However, in application, too many consumers may be frustrated by such systems. Brands take a hit when this happens. A method intended to enhance customer service can ironically result in annoying customers. Thinking more fully through the human condition will yield more effective solutions.

8. Discussion

The nature of IoT means that researchers can now “lurk” in wait for what are, in essence, ready-made data sets [19]. However, the speed with which these new sources of data have emerged, as well as the increasingly imaginative ways that researchers are using them, risked running ahead of the development of an appropriate ethical framework for their use.

Ethicists have recognised that they face a challenge in determining how to transfer traditional deontological principles into the world of IoT, addressing the duties and obligations of the researcher, as well as how to deal with concepts such as utilitarianism, feminism, and communitarianism [20]. As research on material published on the internet involves no direct contact between the subject and the researcher. It avoids one of the problems facing much qualitative research, namely that of interviewer bias, whereby what is said is influenced by the researcher. However, the absence of such contact creates other problems, in particular those relating to informed consent and protection of the subject. This commentary considers two of the major issues in the ethics of IoT research; the difference between public and private space and the right to anonymity.

Now that people routinely share detailed information on all aspects of their lives, including embarrassing anecdotes and even incriminating photographs on social media, there are questions as to what online privacy actually means. One approach is to apply the ethic of reciprocity, or Golden Rule, whereby the researcher asks how they would feel if the roles were reversed [21].

The challenge then is to operationalize this principle. How do people’s expectations of privacy change depending on the type of IoT they are using and what are the consequences for researchers’ ethical obligations [28]?

This discussion recognises that the concept of privacy is inherently complicated and there is a need to understand how individuals will respond to violations in different contexts [29].

A related issue is that of anonymity. Anonymity is a fundamental right of subjects of research. It underpins the potentially fragile trust between the subject and the researcher and is integral to consent and provision of information as well as being a manifestation of the respect in which the researcher holds the subject in front of the computer screen. This creates many additional ethical considerations for the researcher [28,31].

9. Conclusion

The Internet of Things is the connection – via the internet – of objects from the physical world that are equipped with sensors, actuators and communication technology. IoT systems will create dramatic business opportunities and provide great benefits to individuals and society. For these systems to succeed, they must be secure, robust, and usable by humans. Progress has been made on improving the security of existing systems but IoT systems require even higher quality and introduce new complexities.

Privacy and security are the important aspect for Internet of Things (IoT) deployments. In this paper, we provided an overview of the privacy of IoT technologies, and a number of research challenges has been identified, which are expected to become major research trends in the next years. Several significant obstacles remain to fulfill the IoT vision, among them privacy. Indeed, realizing the IoT vision is likely to spark novel and ingenious malicious models. The challenge is to prevent the growth of such models or at least to mitigate and limit their impact. Meeting this challenge requires understanding the characteristics of things and the technologies that empower the Internet of Things. When every object in our daily life is connected to the Internet, they must be secure. Although the IoT improves the productivity of companies and enhances the quality of people's lives, the IoT will also increase the potential attack surfaces for hackers and other cyber criminals. Lack privacy will create resistance to adoption of the IoT by firms and individuals.

For future research, the following questions can be considered: (1) what are the types and levels of behaviors adopted by users as a result of their privacy concerns, and why are these adopted? (2) What are the differences in awareness, concerns, and behaviors of the general public versus business entities related to privacy?

Moreover, Support research that addresses the core underlying scientific and engineering principles dealing with large-scale issues, networking, security, privacy, real-time, and the other key questions raised in this paper.

References

[1] E. Rekleitis, P. Rizomiliotis, and S. Gritzalis, "A Holistic Approach to RFID Security and Privacy," Proc. 1st Int'l Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2010; www.nics.uma.es/seciot10/files/pdf/rekleitis_seciot10_paper.pdf.

[2] D.Clark, 'Internet of Things' in reach: Companies rush into devices like smart door locks, appliances, but limitations exist. The Wall Street Journal. Retrieved April 3, 2015, from http://www.wsj.com/articles/SB100014240527 02303640604579296580892973264

[3] L. Ding, P. Shi, and B. Liu, "The clustering of Internet, Internet of things and social network," in Proc. 3rd Int. Symp. KAM, Wuhan, China, 2010.

[4] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of things," in Proc. IEEE 23rd Int. Symp. PIMRC, Sydney, NSW, Australia, 2012, pp. 18–23.

[5] F. Bao and I.-R. Chen, "Trust management for the Internet of things and its application to service composition," in Proc. IEEE Int. Symp. Wow Mom, San Francisco, CA, USA, 2012, pp. 1–6.

[6] C. Occhiuzzi, C. Vallese, S. Amendola, S. Manzari, and G. Marrocco, "NIGHT-Care: A passive RFID system for remote monitoring and control of overnight living environment," Procedia Computer Science, vol. 32, 2014, pp. 190 – 197.

[7] B.Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F.Bu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services, " IEEE Transaction on Industrial Informatics, Vol. 10, No. 2, May 2014.

[8] A. Sarma and J. Girão, "Identities in the Future Internet of Things," Wireless Personal Comm., Mar. 2009, pp. 353-363.

[9] J. Sen, "Privacy Preservation Technologies in Internet of Things," Proc. Int'l Conf. Emerging Trends in Mathematics, Technology, and Management, 2011; http://arxiv.org/ftp/arxiv/papers/1012/1012.2177.pdf.

[10] G. Broenink, "The Privacy Coach: Supporting Customer Privacy in the Internet of Things," Proc. Workshop on What Can the Internet of Things Do for the Citizen? (CIOT 2010); Radboud University, May 2010; http://dare.ubn.ru.nl/bitstream/2066/83839/1/83839.pdf.

[11] S. Radomirovic, "Towards a Model for Security and Privacy in the Internet of Things," Proc. 1st Int'l Workshop on the Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2010; www.nics.uma.es/seciot10/files/pdf/radomirovic_seciot10_paper.pdf.

[12] B. D. Weinberg, G. R. Milne, Y. G. Andonova, F. M. Hajjat, "Internet of Things: Convenience vs. privacy and secrecy," Business Horizons," Vol.58, No. 6, November-December, 2015, pp.615-624.

[13] M.Henze, L.Hermerschmidt, D. Kerpen, R.Häußling, B. Rumpe, K. Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things," Future Generation Computer Systems, Vol.56, March 2016, pp. 701-718.

[14] R. H. Weber, "Internet of things: Privacy issues revisited," Computer Law & Security Review, Vol. 31, No. 5, October 2015, pp. 618-627.

[15] A.Botta, W. de Donato, V. Persico, A.Pescapé, "Integration of Cloud computing and Internet of Things: A survey Future Generation Computer Systems," Vol. 56, March 2016, pp.684-700.

[16] A. Antonić, M. Marjanović, K. Pripužić, I.P. Žarko, "A mobile crowd sensing ecosystem enabled by CUPUS: Cloud-based publish/subscribe middleware for the Internet of Things," Future Generation Computer Systems, Vol. 56, March 2016, pp.607-622.

[17] R.Neisse, G.Steri, I. N. Fovino, G. B.SecKit, "A Model-based Security Toolkit for the Internet of Things Computers & Security," Vol. 54, October 2015, pp. 60-76.

[18] I. Lee, K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, Vol.58, No. 4, July–August 2015, pp. 431-440.

[19] Texas Instruments. (2014). "Application areas for the Internet of Things," Retrieved April 3, 2015, from http://www.ti.com/

[20] A.Cavoukian, J.Jonas, "Privacy by design in the age of big data. Information and Privacy Commissioner of Ontario," Canada. 2012. Available at https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf

[21] G. R. Milne, "Digital privacy in the marketplace," New York: Business Expert Press. 2015.

[22] I.Rubinstein, "Regulating privacy by design," Berkeley Technology Law Journal, Vol. 26, No.3, 2011, pp.1409-1456.

[23] H. Packard, "HP study reveals 70 percent of Internet of Things devices vulnerable to attack," July 29 2014. Retrieved from http://www8.hp.com/us/en/hp-news/press-release. Html? Id=1744676#.VOTykPnF-ok

[24] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: A survey," Comput. Netw, vol. 54, no. 15, pp. 2787–2805, 2010.

[25] P. Mendes, "Social-driven Internet of connected objects," in Proc. Interconn. Smart Objects with the Internet Workshop, Lisbon, Portugal, 2011.

[26] Z. Yan, P. Zhang, A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, Volume 42, June 2014, pp. 120-134.

[27] Y. Challal, E. Natalizio, S. Sen, A. M. Vegni, "Internet of Things security and privacy: Design methods and optimization, Ad Hoc Networks," Vol.32, September 2015, pp.1-2.

[28] J. Lee, S.Oh, J. W. Jang, "A Work in Progress: Context based Encryption Scheme for Internet of Things," Procedia Computer Science, Vol. 56, 2015, pp. 271-275.

[29] V.H. Jeroen. "Fact sheet-Ethics Subgroup IoT -Version 4.0. Conclusions of the Internet of Things public consultation," 2013. Available at https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

[30] S. H. Rebecca. "Europe's policy options for a dynamic and trustworthy development of the Internet of Things," SMART 2012/0053, RAND Corp., European Union 2013, 2013.

[31] A. Samani, H. H. Ghenniwa, A.Wahaishi, "Privacy in Internet of Things: A Model and Protection Framework," Procedia Computer Science, Vol. 52, 2015, pp. 606-613.

[32] Value Ageing' project. "Incorporating European Fundamental Values In to ICT for Ageing: A vital political, ethical, technological, and industrial challenge," Ref. online: www.valueageing.eu

[33] R. H. Weber, "Internet of Things–New security and privacy challenges". Computer Law & Security Review, Vol. 26, No.1, 2010, pp. 23-30.

[34] C. M. Medaglia, A.Serbanati, "An overview of privacy and security issues in the internet of things," In The Internet of Things, Springer New York, 2010, pp. 389-395..

[35] J. S.Kumar, D. R. Patel, "A survey on Internet of Things: security and privacy issues," International Journal of Computer Applications, 2014, Vol. 90, No.11.

[36] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, Vol.76, 2015, pp.146-164.

[37] Q, Jing, A.V. Vasilakos, J.Wan, J. Lu, D, Qiu, "Security of the internet of things: Perspectives and challenges," Wireless Networks, Vol. 20, No.8, 2014, pp. 2481-2501.

[38] H.Suo, J.Wan, C. Zou, J. Liu, "Security in the internet of things: a review," In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on 2012, pp. 648-651.

[39] S. Chabridon, R. Laborde, T. Desprats, A. Oglaza, P.Marie, S.M. Marquez, "A survey on addressing privacy together with quality of context for context management in the internet of things," Annals of telecommunications-annales des télécommunications, Vol.69, No.1, 2014, pp.47-62.

[40] R.Dworkin, "Autonomy and the demented self," The Milbank Quarterly, Vol.64, No.2, pp.4-16.

[41] A.Gawande, "Being mortal: Medicine and what matters in the end," New York: Metropolitan Books, Henry Holt & Company, 2014.

Hodjatollah Hamidi born 1978, in shazand Arak, Iran, He got his Ph.D in Computer Engineering. His main research interest areas are Information Technology, Fault-Tolerant systems (fault-tolerant computing, error control in digital designs) and applications and reliable and secure distributed systems and E- Commerce. Since 2013 he has been a faculty member at the IT group of K. N. Toosi University of Technology, Tehran Iran. Information Technology Engineering Group, Department of Industrial Engineering, K. N. Toosi University of Technology.