Privacy of the Internet of Things: A Systematic Literature Review

Noura Aleisa
School of Computing Science, University of Glasgow
n.aleisa.1@research.gla.ac.uk

Karen Renaud
School of Computing Science, University of Glasgow
karen.renaud@glasgow.ac.uk

Abstract

The Internet of Things' potential for major privacy invasion is a concern. This paper reports on a systematic literature review of privacy-preserving solutions appearing in the research literature and in the media. We analysed proposed solutions in terms of the techniques they deployed and the extent to which they satisfied core privacy principles. We found that very few solutions satisfied all core privacy principles. We also identified a number of key knowledge gaps in the course of the analysis. In particular, we found that most solution providers assumed that end users would be willing to expend effort to preserve their privacy; that they would be motivated to take action to ensure that their privacy was respected. The validity of this assumption needs to be proved, since it cannot simply be assumed that people would necessarily be willing to engage with privacy-preserving solutions. We suggest this as a topic for future research.

1. Introduction

With the growth of the Internet of Things (IoT) your future morning routine might be something similar to the following scenario:

It is morning; your smart home is readying itself to support your daily routine. The alarm finds out when you have to get up by accessing your diary, it knows how long it usually takes you to get out of the house, based on the data collected from your phone, fine-tuned by consulting timings from previous days. The light is switched on, and the coffee machine starts brewing your daily dark roast. You wake, dress and eat breakfast. Your autonomous car has started itself, reversed out of the garage, and is waiting for you to hop in. On your way out, your Smartphone locks the door and activates the alarm. Your refrigerator adds 'milk' to your convenience store shopping list, so that your parcels will be ready for you to pick up on your way home from work. During your journey to work your autonomous car drives itself, using millions of embedded sensors. It goes directly to the parking spot it has detected using a networked application that receives notifications from the city's parking bay sensors.

This, then, is the wonderful new world of the Internet of Things [28, 12]. The term "Internet of Things" was first used by Kevin Ashton at Procter & Gamble in 1999, to describe an Internet-based information service architecture [3]. Generally the term refers to Internet-enabled objects interacting with each other and cooperating to achieve specific goals. These objects could be RFID, sensors, actuators or smart phones [21]. The IoT claims to improve peoples' lives. For instance, a tool could tailor room temperature based on measurements of heart rate and body temperature [62]. Other tools activate smart streetlights, monitor surveillance cameras and control traffic lights. Collected information can easily and effortlessly be shared with stakeholders [75].

The IoT maximizes convenience. However, the invisibility of data collection, usage and sharing raises privacy concerns with respect to IoT users [17]. On the one hand, we accept the fact that service providers need to access certain information in order to deliver tailored services. On the other hand, we expect our private information to be protected from unauthorized access, and not shared with 3rd parties [64].

The contribution of this paper is to provide an overview of existing IoT privacy-related research in order to identify areas of focus and to highlight areas that deserve more attention.

2. Privacy

2.1. Definition

Solove has defined privacy as "*an umbrella term, referring to a wide and disparate group of related things*" [61] (p.485). Privacy, according to Privacy International, is a multidimensional concept, which is related to four components: (1) body, (2) communications, (3) territory, and (4) information. Bodily privacy focuses on the people's physical protection against any external harm. Privacy of communications focuses on the protection of the information that is carried through any medium

URI: http://hdl.handle.net/10125/41881
ISBN: 978-0-9981331-0-2

between two parties. This includes email, mail and telephone. Territorial privacy is about establishing boundaries or limits on physical space or property, such as the home, workplace, and public places. Information privacy refers to personal data that is collected and processed by an organization, such as medical records and credit card information [63].

2.2. Privacy Stances

Westin's take on privacy is that of someone having the right to control what personal information collected about them or known to others [76]. As technology makes it trivial for organizations to maintain comprehensive digital files about every person, privacy concerns have emerged. Specifically, what data is collected, who has access to it, who controls it, and what it is used for [37]. Westin studied privacy perceptions between 1978 and 2004 and created a "Privacy Index". Westin found that people naturally fell into one of three categories with respect to their privacy stance: *Fundamentalist*, *Pragmatist* and *Unconcerned* [35]. Fundamentalists are concerned about the accuracy of collected information and uses made of it. They are generally in favor of laws supporting privacy rights as well as enforceable privacy-protecting frameworks. Pragmatists are willing to give some personal information to a trusted service provider in return for benefits. Unconcerned people have full trust that the organizations collecting their information would not abuse it.

Westin's follow-up surveys revealed that the percentage of "Unconcerned" had decreased over the last few years. He attributes this to people becoming more aware of technology and different means of preserving their privacy. It could also indicate an increasing level of concern about privacy [35]. A number of privacy breaches have made headlines in recent years. For example, this year it was reported that unsecured webcams exposed the private lives of hundreds of consumers on the Internet [52]. Hewlett Packard's 2015 report [27] reported that 80% of IoT devices raised privacy concerns.

2.3. Privacy Threats

Nowadays, it is even harder for us to retain our privacy, as the IoT technologies take over our daily lives. Conflicts over how organizations can access individual data are pervasive, and IoT will add to this. Ziegeldorf's literature review [84] enumerates the most common privacy threats in the IoT:

1) ***Identification*** is the most dominant threat that connects an identifier, e.g. a name and address, with an individual entity;
2) ***Localization and tracking*** are the threat of locating an individual's location through different means, e.g. GPS, internet traffic, or smartphone location;
3) ***Profiling*** is mostly used for personalization in e-commerce (e.g. in newsletters and advertisements). Organizations infer interests by association with other profiles and data sources;
4) ***Interaction and presentation*** refers to the number of smart things and new ways of interacting with systems and presenting feedback to users. This becomes a threat to privacy when private data is exchanged between the system and the users;
5) ***Lifecycle transitions*** occur when an IoT item is sold or finally disposed of. There could be an assumption that all information is deleted by the object, but smart devices often store huge amounts of data about their own history throughout their entire lifecycle. This could include personal photos and videos, sometimes not deleted upon transfer of ownership;
6) ***Inventory attacks*** apply to the unauthorized access and collection of data about the presence and characteristics of personal things. Burglars can use inventory data to case the property to find a safe time to break in;
7) ***Linkage*** of different systems makes unauthorized access and leaks of private data likely when separate data sources are combined.

2.4. Privacy Preserving Solutions

Several approaches have been proposed to preserve privacy:

Cryptographic techniques and information manipulation: This is the dominant solution, even though many sensors cannot offer adequate security protocols due to limited storage and computation resources [16].

Privacy awareness or context awareness: Solutions have mainly focused on individual applications, increasing awareness of smart devices, such as smart TVs, wearable fitness devices, and health monitor systems, collecting personal data. For instance, in recent research, a framework called SeCoMan was proposed to act as a trusted third party for users as applications might not be reliable enough to manage location information [31].

Access control*:* This is a viable solution, to be used in addition to encryption and privacy awareness. This gives users the power to manage their own data. An example of this approach is CapBAC [59]. It is essentially a distributed approach in which smart things themselves are able to make fine-grained authorization decisions.

***Data minimization*:** The principle of "data minimization" means that the IoT service providers should limit the collection of personal information to what is directly relevant. They should also retain the data only for as long as is necessary to fulfill the purpose of the services provided by the technology. In other words, they should collect only the personal data they really need, and keep it only for as long as they need it [66].

***Others*:** There are other proposed solutions that do not fall into the previous four categories, such as *hitchhiking*. This is a new approach to ensure the anonymity of users who provide their locations. Hitchhiking applications handle locations as the entity of interest. Because the knowledge of who is at a particular location is unnecessary, the fidelity tradeoff is removed [68]. Another example is the *introspection* technique that proactively protects users' personal information by examining the activities of the VM. It gathers and analyzes the CPU state of every VM, the memory contents, file I/O activity, network information that is delivered via hypervisor and detects malicious software on the VM. However, if an IoT device loses integrity due to any malicious attack, it creates risks to the users' privacy [34].

3. Methodology

To assess the limits of privacy that are potentially violated by the IoT, a systematic quantitative literature review was conducted. This method [49] has benefits as compared to a narrative style. It is capable of identifying the areas covered by existing research, and also revealing the gaps. It approaches the literature from different perspectives and facilitates delivery of new insights. Figure 1 depicts the process.

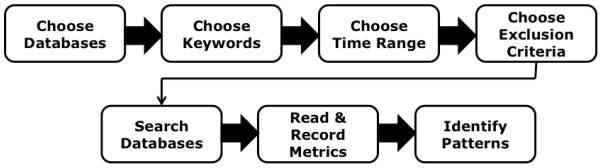

Figure 1. Systematic Literature Review

***Choose Databases**:* Papers were collected from electronic databases, including Google Scholar, Web of Science, ProQuest, Research Gate, SCOPUS, and Science Direct.

Choose Keywords: Keywords used for the searches were 'Internet of Things', 'IoT', and a combination of terms including: 'privacy', 'trust', 'awareness', 'data', 'protection', 'security', 'preserving', 'individual', 'user', and 'private'.

***Choose Time Range**:* The search was restricted to papers published between 2009 and 2016.

***Choose Exclusion Criteria**:* The academic search was restricted to papers published in English. In addition to the research papers, a search for news stories and privacy reports were also included in order to accommodate personal privacy violation perspectives. Review papers were excluded but their reference lists were followed to ensure all the research in this field was consulted.

***Read & Record**:* For each collected paper, the following information was recorded including author(s), year of publication, journal, country where the research was carried out. Each paper was categorized based on the methods used and whether analysis was quantitative, qualitative, or mixed. The rest of the criteria are related to the researched topic, it classifies the application area as home automation, smart cities, smart manufacturing, health care, automotive, or wearable devices, the type of technology used (RFID, sensor, nano, or intelligent embedded technology). The privacy protections, threats, violations, and perceptions for each type of technology were also recorded. Perceptions were categorized based on Westin's three categorizes: fundamentalist, pragmatic, and unconcerned [35].

***Identify Patterns**:* An analysis was carried out to uncover patterns in order to identify foci, gaps and to make recommendations for future research.

4. Results

A total of 122 original research papers on the privacy of the IoT were identified (Table 2 in the Appendix).

4.1. Geographic scope

Privacy research was carried out by researchers in 26 countries with Europe dominating: most were from Germany (19.6%), Italy and France (12.5%).

4.2. Methods used by researchers

A wide range of methods were used to assess the privacy of IoT. Many studies used multiple methods to collect data. Based on the methods sections in Table 3, almost 52 (44.1%) papers used modeling, while only 16.9% of studies used document analysis, followed by case studies (15.2%), surveys (12.7%), observation (10.1%), and interviews (0.8%). Nearly half of the studies (45.4%) adopted quantitative research strategies, with a few using a qualitative approach (19.8%), and mixed approaches (16.5%). Another type

of data has been considered here, with 18.2% for news or reports.

4.3. Characteristics of IoT

Papers assessed technologies used in the IoT, application areas, and types of privacy protection. When papers specified what technologies were used in the IoT, most discussed the use of RFID (34.9%) and sensor technology (55.3%). Further consideration shows that 37% were about home automation, then smart cities (16.8%), and the remainder fluctuated between 13.6% and 9.6% for automotive, health care, wearables, and manufacturing (Table 3 in the Appendix).

One of the key concerns is related to secure services offered by IoT technology. The review provided a comparison between security and privacy protection solutions and individual perceptions of IoT. In terms of security protection, most papers (66.6%) mentioned that the authentication and authorization techniques are the most common security techniques used by IoT.

On the other hand, the review found that there was an increase in three privacy protection mechanisms, with 39.5% for cryptographic techniques and information manipulation, 26.1% for privacy awareness or context awareness, and 25.5% for using access control.

Most of the reviewed research considers the lack of privacy protection a major challenge. 48% of the solutions were for home automation smart products, followed by health care (20%), automotive, smart cities (12%), and 4% for wearables and manufacturing.

4.4. Threats, solutions, principles, precautions

The increasing collection of data about individuals is one of the main concerns, especially the threats to individuals caused by analysis of their data using data mining techniques [10]. The literature indicates that about 31.5% of the papers have concerns about location tracking; the next is the sharing of unanonymised data (25.9%). Concerns about profiling were mentioned in 21.3% of the papers, followed by inventory attacks (8.3%), interaction and presentation (6.5%), life cycle transitions (3.7%), and linkage (2.7%) (Figure 2).

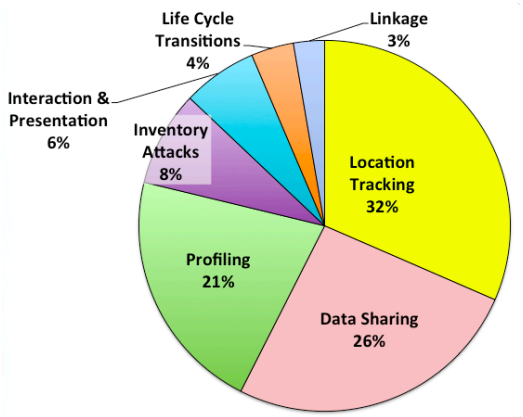

Figure 2. Highlighted IoT Privacy Threats

A wide range of privacy-preservation approaches was proposed. Over half had not been tested or evaluated; they are essentially at proposal stage. On the other hand, about 39 solutions *were* evaluated: cryptographic algorithms, access control management tools, data minimization techniques, and privacy or context awareness protocols (Table 2).

Only 4 out of 75 solutions addressed all the privacy principles identified by the OECD [46], and only eleven focused on 10 principles.

Since individuals are unable to control their own data, the potential for privacy violation has become a major concern. We classified the papers using Westin's categories. We counted most of the papers that offered privacy-preserving frameworks, discussed the privacy threats, or even demonstrated concerns about the data collected and used by IoT as *fundamentalist*. With regard to *pragmatism*, we allocated papers that encouraged trust in the privacy and security measures implemented by smart devices, without having any awareness of the collected data, to this category. Two papers argued for the benefits of a smart environment and used the "nothing to hide" argument — these were *unconcerned* authors.

The majority of the research papers were fundamentalist (112 out of 122 papers, including news and reports that were written by non-specialists), while only 6 papers were pragmatic, and 2 demonstrated unconcern.

5. Discussion

The literature has presented insights into where, how and what research has been conducted and made it possible to identify the gaps.

5.1. Primary research focus

The results suggest that countries with the strictest personal privacy measures, such as those in Europe, seem to do the most research in this area [23].

The deployed study methods fell into one of two categories: (1) analyzing the privacy violations and threats, and (2) proposing a solution to protect the IoT user's privacy. Modeling, document analysis and case studies are dominant. In contrast, few observational or survey-type studies were carried out on privacy breaches and perceptions.

The range of research demonstrates a growing awareness of the potential for privacy violation. Researchers have started exploring privacy protection mechanisms. The sheer range and variety of IoT products, each on bespoke platforms, makes this a challenging field to find solutions for.

Most of the papers examined in this systematic review were published in academic venues. However, a number of news reports were also included to gauge consumer concerns about privacy as well. It can reasonably be concluded that such concerns are not only being raised by technology professionals but by consumers with less technological expertise.

5.2. Threat focus

The majority of the reported threats were focused on data being collected about individuals themselves, such as their identities, location, or profiling. This information can be used to harm the users, to carry out identity theft, or burglaries.

The majority of proposed privacy-protecting applications and techniques are for smart devices used in homes or for health monitoring. These include Smart TVs, Smart Meters, light or temperature control, Smart remote health monitors, or drug tracking. Such a restricted focus could be attributed to several circumstances including: (1) the availability and the easy access of the homes or health care smart devices in the market; (2) The homes or health care smart devices are not controlled by higher authority unlike the smart cities and manufacturing solutions which are controlled by government or private organizations; (3) growth of automotive, cities, and (4) manufacturing smart technology has not become reality yet.

5.3 Gaps

Many proposed solutions must intimately involve humans in the process. Some solutions deploy access control methods, or privacy-awareness applications. For example, in [71], the study proposed the Dynamic Privacy Analyzer (DPA), a solution to make the smart-meter data owner aware of the privacy risks of sharing smart meter data with third parties. On the other hand, almost half of the proposed solutions suggested taking the human out of the loop. These proposed using cryptographic techniques and information manipulation, or data minimization, to prevent data being sniffed *en route* to servers. In [67], an original scheme called the Path Extension Method (PEM) was presented, which provides powerful protection of source-location privacy, by using an encryption technique that ensures an adversary will not be able to eavesdrop on communications.

The overwhelming majority of the researchers were fundamentalist about privacy. This is, perhaps, to be expected since unconcerned researchers would not have little interest in carrying out research in this area. It does mean, however, that they might be somewhat unrealistic about the man and woman in the street, and their privacy stance. Unconcerned consumers are likely to be unwilling to take any action at all to preserve a privacy they don't care about. Solutions seem to be designed under the assumption that consumers will naturally be willing to spend time and effort engaging with them. This assumption might well be flawed.

The question that demands investigation is whether consumers of various privacy stances would indeed be willing to expend effort to interact with privacy-preserving applications. Researchers are coming up with innovative solutions but this will be futile in the face of consumer complacency or unwillingness to engage with them.

5.4 Returning to privacy principles

Table 1 considers how many of the privacy principles the different solutions support. It can be observed that only a few cover all 11 principles; the average coverage is 6 principles. Almost all the solutions deliver security and integrity/accuracy. This is important, but the other principles are equally important. One of the least-considered principles is *purpose specification*. Designers do not seem to believe this is one of the user's rights, i.e. knowing why the smart device needs the particular data they are collecting.

The results demonstrate that designers' priorities are often to secure the collected data, to ensure that it is accurate and updated, and not transferred without protection. It is time for them to pay more attention to designing for privacy awareness and enabling protection thereof.

Privacy is all about the user; most of the principles mandate his/her involvement, entailing notification of the device policy, the data collected, the purpose of collecting specific types of information, giving him/her

the ability to control information disclosure. He/she can also ensure that the data is not going to be used for purposes other than those specified in the policy, and that collection of personal information is minimized. Having the user involved from the outset is the best way to gain trust.

5.5 Need for legislation

A significant number of ambiguities remain poorly described in the literature, and require further investigation. For example, consumers would sometimes like to know what data is recorded and transmitted by their smart device *before* they buy it. It would also be helpful if the consumer could get information about how their data is protected by the device, both on the device itself, and during transmission. This information is not generally provided. Devices ought to allow people to configure privacy preferences, in much the same way as Smartphones and Facebook currently allow people to, but perhaps because of the newness of this technology, this functionality is not offered. It is clear that the industry is going to have to be compelled to respect privacy. Their track record so far amply demonstrates that they do not have the will to do this without some compelling motivation.

6. Limitations

Although the Smartphone qualifies as an IoT device it was not explicitly included in the search keywords. We wanted to focus on papers that claimed to solve IoT-wide issues, not those focusing only on one type of device.

This review has focused primarily on privacy-related research. In some cases it is difficult to separate privacy- and security-preserving solutions. For example, encryption is primarily a security tool, but, if used, essentially preserves the privacy of communication. A further review should be carried out in order to analyze security-specific IoT solutions as well.

7. Related Research

The IoT is considered a significantly disruptive technology of this era, because it integrates several collaborative technologies, allowing for comprehensive data collection, allowing delivery of personalized services that require no deliberate interaction [10].

Opplinger [48] refers to the difficulties of preserving security and privacy because the IoT has no boundaries and he expresses the hope that researchers will consider focusing their attention on the security and privacy of IoT.

The security of IoT has received a great deal of attention. A number of reviews have suggested mechanisms to overcome the security threats and challenges of IoT [65, 82, 14, 80, 38]. Most of these reviews have concluded with a set of security practices that should be deployed by IoT product designs. This list usually includes: (1) secure booting using cryptographically generated digital signatures; (2) deploy authentication and access control techniques based on the lightweight public key authentication technology and asymmetric cryptosystems; (3) firewalls; (4) assiduous patching. Finally, they call for increased user awareness of security aspects of IoT [82]. Privacy has received far less attention from researchers.

One systematic review of privacy threats was carried out by Ziegeldorf [84]. He first classified the evolving technologies used in IoT as: to RFID, wireless sensor network, smart phones, and cloud computing. He highlights important privacy features. These include data collection, life cycle and system interaction. The study identified privacy-preserving approaches from related work to determine whether they could mitigate in an IoT context.

The author concluded that identification, tracking and profiling were the primary threats in IoT. The remaining four threats of privacy-violating interactions and presentations, lifecycle transitions, inventory attacks and information linkage are recent additions, prompted by the rise of IoT.

This systematic literature review extends Ziegeldorf's work because his paper focused on analyzing the challenges and threats of IoT in the context of entities and information flows. This paper examines IoT-specific solutions, and identifies gaps in the research literature, specifically from an end-user perspective.

8. Conclusion & Future Work

The era of the Internet of Things has arrived. Current research is disproportionally focused on the security concerns of IoT. Yet the privacy problem is equally urgent. Future research should assess privacy perceptions related to IoT, to find out whether people would act to protect their own privacy when using IoT. Moreover, we should determine whether they would value and use a management tool that explicitly prevents privacy invasions by IoT devices, especially if some degree of effort is involved.

We plan to carry out a similar systematic literature review of IOT-related security research as future work.

An extended version of this paper with a more detailed analysis of the issues dealt with in Table 1, and some extra figures, is available from arXiv.org, titled "*Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)*"

9. References

[1] Addo, I. D., S. I. Ahamed, S. S. Yau, and A. Buduru. A reference architecture for improving security and privacy in Internet of Things applications. International Conference on Mobile Services, IEEE, Alaska, 2014

[2] Arabo, A. Privacy-aware IoT cloud survivability for future connected home ecosystem. Computer Systems and Applications (AICCSA), IEEE, Doha, 2014.

[3] Ashton, K. That Internet of Things thing. RFiD Journal, 22(7), pp. 97–114, 2009.

[4] Axelrod, C. W. Enforcing security, safety and privacy for the Internet of Things. In Systems, Applications and Technology Conference (LISAT), IEEE, Long Island, 2015.

[5] Banerjee, D, B. Dong, M. Taghizadeh and S. Biswas. Privacy-preserving channel access for Internet of Things. Internet of Things Journal, IEEE, 1(5), pp. 430–445, 2014.

[6] Bao, F. and I.-R. Chen. Trust management for the Internet of Things and its application to service composition. World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, Washington, 2012.

[7] Bose, T., S. Bandyopadhyay, A. Ukil, A. Bhattacharyya, and A. Pal. Why not keep your personal data secure yet private in IoT? Our lightweight approach. In Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), IEEE, Singapore, 2015.

[8] Broenink, G., J.-H. Hoepman, C. v. Hof, R. Van Kranenburg, D. Smits, and T. Wisman. The privacy coach: Supporting customer privacy in the Internet of Things. arXiv preprint arXiv:1001.4459, 2010.

[9] Cadzow, S. W. Privacy-the forgotten challenge in sensor and distributed systems. IET Conference on Wireless Sensor Systems (WSS 2012), IET, Poland, 2012.

[10] Caron, X. R. Bosua, S. B. Maynard, and A. Ahmad. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. Computer Law & Security Review, Elsevier, 2015.

[11] Daubert, J., A. Wiesmaier, and P. Kikiras. A view on privacy & trust in IoT. IEEE International Conference on Communication Workshop (ICCW), IEEE, London, 2015.

[12] DeLoach, D. A day in the connected world: How IoT and smart cities will change your life, http://insights.wired.com/profiles/blogs/a-day-in-the-connected-world-how-smart-cities-and-the-iot-will, 2014.

[13] Dominikus, S. Medassist. A privacy preserving application using rfid tags. International Conference on RFID-Technologies and Applications (RFID-TA), IEEE, Spain, 2011.

[14] Du, J. and S. Chao. A study of information security for m2m of IoT. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE, China, 2010.

[15] Enev, M. Machine Learning based Attacks and Defenses in Computer Security: Towards Privacy and Utility Balance in Emerging Technology Environments. PhD thesis, University of Washington, Seattle, WA, August, 2014.

[16] Feng, H. and W. Fu. Study of recent development about privacy and security of the Internet of Things. International Conference on Web Information Systems and Mining(WISM), IEEE, Hong Kong, 2010.

[17] Fink, G. A., D. V. Zarzhitsky, T. E. Carroll, and E. D. Farquhar. Security and privacy grand challenges for the Internet of Things. International Conference on Collaboration Technologies and Systems (CTS), Georgia, 2015.

[18] Florian, M., S. Finster, and I. Baumgart. Privacy-preserving cooperative route planning. Internet of Things Journal, IEEE, 1(6), pp. 590–599, 2014.

[19] Funke, S., J. Daubert, A. Wiesmaier, P. Kikiras, and M. Muehlhaeuser.End-2-End privacy architecture for IoT. Conference on Communications and Network Security (CNS), IEEE, San Fransisco, 2015.

[20] Gessner, D., A. Olivereau, A. S. Segura, and A. Serbanati. Trustworthy infrastructure services for a secure and privacy-respecting Internet of Things. 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, Liverpool, 2012.

[21] Giusto, D., A. Iera, G. Morabito, and L. Atzori. The Internet of Things 20th Tyrrhenian Workshop on Digital Communications. Springer, NewYork, 2010.

[22] Gong, T., H. Huang, P.Li, K. Zhang, and H. Jiang. A medical healthcare system for privacy protection based on IoT. Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), IEEE, Taipei, 2015.

[23] Gustke, C. Which countries are better at protecting privacy? http://www.bbc.com/capital/story/20130625-your-private-data-is- showing. 2013

[24] Hennebert, C. and J. Dos Santos. Security protocols and privacy issues into 6LoWPAN stack: A synthesis. Internet of Things Journal, IEEE, 1(5), pp. 384–398, 2014.

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

[26] JHernandez Ramos, .L., J. Bernal Bernabe and A.F. Skarmeta. Towards privacy-preserving data sharing in smart environments. Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), IEEE, Birmingham, 2014.

[27] Hewlett Packard. Internet of Things research study. http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf. 2015

[28] W. Hinch. A day with the Internet of Things, 2015. http://www.ebuyer.com/blog/2015/01/a-day-with-the-internet-of-things/

[29] Hu, C., J. Zhang and Q. Wen. An identity-based person allocation system with protected privacy in IoT. 4th International Conference on Broadband Network and Multimedia Technology (IC-BNMT), IEEE, 2011.

[30] Huang, X., R. Fu, B. Chen, T. Zhang, and A. Roscoe. User interactive Internet of Things privacy preserved access control. International Conference for Internet Technology And Secured Transactions, IEEE, London, 2012.

[31] Huertas Celdran, A., G. Clemente, J. Felix, M. Gil Perez, and G. Martinez Perez. Secoman: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications. IEEE Systems Journal, 99, pp. 1–14, 2013.

[32] International Organization for Standardization. Information technology security techniques privacy framework, iso/iec 29100, 2011.

[33] Jacobsson, A. and P.Davidsson. Towards a model of privacy and security for smart homes. 2nd World Forum on Internet of Things (WF-IoT), IEEE, Milan 2015.

[34] Kang, C. , F. Abbas, and H. Oh. Protection scheme for IoT devices using introspection. 6th International Conference on the Network of the Future (NOF), IEEE, Montreal, 2015.

[35] Kumaraguru, P. and L. F. Cranor. Privacy indexes: a survey of Westin's studies. Technical Report CMU-ISRI-05-138, CMU, 2005.

[36] Lai, C., H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen. Cpal: A conditional privacy-preserving authentication with access linkability for roaming service. Internet of Things Journal, IEEE, 1(1), pp. 46–57, 2014.

[37] Langheinrich, M. Ubicomp 2001: Ubiquitous Computing: International Conference Atlanta Georgia, USA, Springer, Berlin, 2001.

[38] Li, X., Z. Xuan, and L. Wen. Research on the architecture of trusted security system based on the Internet of Things. International Conference on Intelligent Computation Technology and Automation, IEEE, China, 2011.

[39] Liu, J., Y. Xiao, and C. P. Chen. Authentication and access control in the Internet of Things. 32nd International Conference on Distributed Computing Systems Workshops, IEEE, China, 2012.

[40] Liu, Y., X. Gong, and C. Xing. A novel trust-based secure data aggregation for Internet of Things. 9th International Conference on Computer Science & Education (ICCSE), IEEE, Vancouver, 2014.

[41] Lize, G.,W. Jingpei, and S. Bin. Trust management mechanism for Internet of Things. Communications, China, 11(2), pp. 148–156, 2014.

[42] Matyszczyk, C. Samsung's warning: Our smart TVs record your living room chatter, 2015. http://www.cnet.com/uk/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/.

[43] Mohammad, A., J. Stader, and D. Westhoff. A privacy-friendly smart metering architecture with few-instance storage. 15th International Conference on Innovations for Community Services (I4CS), IEEE, Nuremberg, 2015.

[44] Nakagawa, I., Y. Hashimoto, M. Goto, M. Hiji, Y. Kicuchi, M.Fukumoto, and S. Shimojo. DHT extension of m-cloud–scalable and distributed privacy preserving statistical computation on public cloud. Computer Software and Applications Conference (COMPSAC), IEEE, Taiwan, 2015.

[45] Notra, S., M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli. An experimental study of security and privacy risks with emerging household appliances. Conference on Communications and Network Security (CNS), IEEE, Philadelphia, 2014.

[46] OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing, 2002.

[47] Oleshchuk, V. Internet of things and privacy preserving technologies. 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, IEEE, 2009.

[48] Oppliger, R. Security and privacy in an online world. Computer, 44(9), pp. 21–22, 2011.

[49] Pickering , C. and J. Byrne. The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early-career researchers. Higher Education Research & Development, 33(3), pp. 534– 548, 2014.

[50] Pocket-lint. Smart TVs are watching you, which shares your private data most? Samsung, LG, Sony and more, undated. http://www.pocket-lint.com/news/130437-smart-tvs-are-watching-you-which-shares-your- private-data-most-samsung-lg-sony-and-more.

[51] Pohls, H. C., V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. Diaz Rodriguez, and T. Mouroutis. Rerum: Building a reliable IoT upon privacy-and security-enabled smart objects. Wireless Communications and Networking Conference Workshops (WCNCW), IEEE, San Francisco, 2014.

[52] Porup, J. How to search the Internet of Things for photos of sleeping babies, 2016. ttp://arstecnica.co.uk/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

[53] Premnath, S. N. and Z. J. Haas. Security and privacy in the internet- of-things under time-and-budget-limited adversary model. Wireless Communications Letters, IEEE, 4(3), pp. 277–280, 2015.

[54] Sadki, S. and H. El Bakkali. Enhancing privacy on mobile health: an integrated privacy module. Fifth International Conference on Next Generation Networks and Services (NGNS), IEEE, Casablanca, 2014.

[55] Saied, Y. B., A. Olivereau, D. Zeghlache, and M. Laurent. Trust management system design for the Internet of Things: a context-aware and multi-service approach. Computers & Security, 39, pp. 351–365, 2013.

[56] Samani, A., H. H. Ghenniwa, and A. Wahaishi. Privacy in Internet of Things: A model and protection framework. Procedia Computer Science, 52, pp. 606–613, 2015.

[57] Sivaraman, V., H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. Network-level security and privacy control for smart- home IoT devices. 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, Abu-Dhabi, 2015.

[58] Skarmeta, A., J. L. Hernández-Ramos, and J. B. Bernabe. A required security and privacy framework for smart objects, 2015. https://www.itu.int/en/ITU-T/academia/kaleidoscope/2015/Documents/ Kaleidoscope Skarmeta.pdf.

[59] Skarmeta, A. F., J. L. Hernandez-Ramos, and M. Moreno. A decentralized approach for security and privacy challenges in the Internet of Things. World Forum on Internet of Things (WF-IoT), IEEE, Milan, 2014.

[60] Smith, C. Privacy settings not enough to stop LG smart TV from spying on users, 2013. http://bgr.com/2013/11/20/lg-smart-tv-spying/.

[61] Solove, D. J. A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), pp. 477–564, 2006.

[62] Stankovic, J. A. Research directions for the Internet of Things. IEEE Internet Of Things Journal, 1(1), pp. 3–9, 2014.

[63] Stefanick, L. Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World. DOAB Directory of Open Access Books. AU Press, 2011.

[64] Sun, G., S. Huang, W. Bao, Y. Yang, and Z. Wang. A privacy protection policy combined with privacy homomorphism in the Internet of Things. 23rd International Conference on Computer Communication and Networks (ICCCN), IEEE, China, 2014.

[65] Suo, H., J. Wan, C. Zou, and J. Liu. Security in the Internet of Things: A review. International Conference on Computer Science and Electronics Engineering (ICCSEE), IEEE, China, 2012.

[66] European Data Protective. Data protection directive 95/46/ec.

[67] Tan, W., K. Xu, and D. Wang. An anti-tracking source-location privacy protection protocol in wsns based on path extension. Internet of Things Journal, IEEE, 1(5), pp. 461–471, 2014.

[68] Tang, K. P., P. Keyani, J. Fogarty, and J. I. Hong. Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications. Proceedings of the SIGCHI conference on human factors in computing systems, ACM, Quebec, 2006.

[69] Ukil, A., S. Bandyopadhyay, and A. Pal. IoT-privacy: To be private or not to be private. In Computer Communications Workshops (INFOCOM WKSHPS), IEEE, Toronto, 2014.

[70] Ukil, A., S. Bandyopadhyay, and A. Pal. Sensitivity inspector: Detecting privacy in smart energy applications. Symposium on Computers and Communication (ISCC), IEEE, Madeira, 2014.

[71] Ukil, A., S. Bandyopadhyay, and A. Pal. Privacy for IoT: Involuntary privacy enablement for smart energy systems. International Conference on Communications (ICC), IEEE, London, 2015.

[72] Wan, K. and V. Alagar. Integrating context-awareness and trustworthiness in IoT descriptions. In Green Computing and Communications (GreenCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, IEEE, China, 2013.

[73] Wang, X. J. Zhang, E.M. Schooler, and M. Ion. Performance evaluation of attribute-based encryption: Toward data privacy in the IoT. International Conference on Communications (ICC), IEEE, China, 2014.

[74] Y.Wang and Q.Wen. A privacy enhanced DNS scheme for the internet of things. IET International Conference on Communication Technology and Application (ICCTA 2011), IET, Beijing, 2011

[75] Weinberg, B.D., G.R. Milne, Y.G. Andonova, and F.M. Hajjat. Internet of things: Convenience vs. privacy and secrecy. Business Horizons, 58(6), pp. 615–624, 2015.

[76] Westin, A. F. Privacy and freedom. 25 Washington. & Legal Law Review. 166, 25(1), 1968.

[77] Wong, K.-S. and M. H. Kim. Towards self-awareness privacy protection for Internet of Things data collection. Journal of Applied Mathematics, pp. 1-9, 2014.

[78] Wright, D. and C. Raab. Privacy principles, risks and harms. International Review of Law, Computers & Technology, 28(3), pp. 277–298, 2014.

[79] Wu, Q.-X. and L. Han. Secure solution of trusted Internet of Things base on TCM. The Journal of China Universities of Posts and Telecommunications, 20, pp. 47–53, 2013.

[80] Xiaohui, X. Study on security problems and key technologies of the Internet of Things. Fifth International Conference on Computational and Information Sciences (ICCIS), China, 2013.

[81] Yao, Y., L. T. Yang, and N. N. Xiong. Anonymity-based privacy- preserving data reporting for participatory sensing. IEEE Internet of Things Journal, 2(5), pp. 381–390, 2015.

[82] Zhao, K. and L. Ge. A survey on the Internet of Things security. 9th International Conference on Computational Intelligence and Security (CIS), IEEE, China, 2013

[83] Zhou, L., Q. Wen, and H. Zhang. Preserving sensor location privacy in Internet of Things. Fourth International Conference on Computational and Information Sciences (ICCIS), IEEE, China, 2012.

[84] Ziegeldorf, J. H., O. G. Morchon, and K. Wehrle. Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), pp. 2728–2742, 2014.

# Privacy Preserving Solutions	Number of Privacy Principles Covered									
	2	3	4	5	6	7	8	9	10	11
	CRYPTOGRAPHIC TECHNIQUES									
	2	4	5	4	6	2	4	1	2	1
	DATA MINIMIZATION									
	1			1		1			1	1
	ACCESS CONTROL									
			1	2	6	2	3	1	4	1
	DIFFERENTIAL PRIVACY									
									1	
	PRIVACY AWARENESS									
	1		4	5	2	2	3		3	1
	OTHER									
				5						
	TOTAL									
	4	4	10	17	14	7	10	2	11	4

Table 1. Privacy Principle Coverage

Privacy Protection Themes	Total	Literature Reference
TESTED AND EVALUATED		
Cryptographic Techniques & Information Manipulation	15	[1, 67, 44, 36, 18, 53, 22, 5, 64, 30, 7, 13, 77, 59, 73]
Data Minimization	3	[15, 7, 59]
Access Control	6	[1, 30, 31, 13, 39, 59]
Privacy/Context Awareness	12	[1, 31, 55, 5, 81, 7, 71,70, 77, 69, 59, 8]
Differential Privacy	0	
Other	3	[34, 6, 40]
NOT EVALUATED		
Cryptographic Techniques & Information Manipulation	16	[24, 25, 79, 9, 20, 51, 41, 54, 43, 26, 45, 58, 47, 19, 2, 56]
Data Minimization	2	[25, 19]
Access Control	14	[25, 9, 57, 20, 41, 54, 26, 45, 58, 72, 47, 19, 29, 74]
Privacy/Context Awareness	9	[25, 41, 33, 54, 72, 4, 2, 56, 11]
Differential Privacy	1	[19]
Other	2	[82, 68]

Table 2. Five Key Themes of Solutions

	Total	EU	Other
METHODS USED			
Observation	12	4	8
Surveys	15	8	7
Interviews	1	1	0
Focus groups	0	0	0
Field Research	0	0	0
Case studies	18	8	10
Document analysis	20	9	11
Modeling	52	19	33
Unspecified	29	2	27
TYPE OF DATA			
Qualitative	24	10	14
Quantitative	55	22	33
Mixed	20	8	12
News or reports	22	1	21
APPLICATION AREAS			
Home automation	47	11	36
Smart cities	21	11	10
Smart manufacturing	12	6	6
Health Care	16	5	11
Automotive	17	6	11
Wearables	12	4	8
Unspecified	62	23	39
TECHNOLOGIES			
RFID	36	14	22
Sensor technology	57	18	39
Nano technology	1	0	1
Intelligence embedded technology	9	6	3
Unspecified	51	17	34
PRIVACY PROTECTION			
Cryptographic techniques & information manipulation	62	23	39
Data minimization	13	6	7
Access control	40	17	23
Privacy/Content awareness	41	16	25
Differential Privacy	1	1	
Other	16	6	20
PRIVACY THREATS			
Identification	28	9	19
Location & Tracking	34	9	25
Profiling	23	9	14
Interaction & Presentation	7	2	5
Lifecycle transitions	4	3	1
Inventory attack	9	3	6
Linkage	3	1	2
Unspecified	71	26	45
PRIVACY PERCEPTIONS			
Fundamentalist	112	39	73
Pragmatic	6	2	4
Unconcerned	2	1	1
Unspecified	6	2	4
PRIVACY OR SECURITY VIOLATIONS			
Accidental or inadvertent violation	1	0	1
Failure to follow established privacy and security policies and procedures	1	0	1
Deliberate or purposeful violation without harmful intent	15	2	13
Willful and malicious violation with harmful intent	26	6	20
Unspecified	82	33	49

Table 3. IoT Privacy-Related Papers