2016

A privacy gap around the internet of things for open-source projects

Brian Cusack
Digital Forensics Research Laboratories, Auckland University of Technology, brian.cusack@aut.ac.nz

Reza Khaleghparast
Digital Forensics Research Laboratories, Auckland University of Technology, reza.khaleghparast@aut.ac.nz

DOI: 10.4225/75/58a69a6909195
Cusack, B. & Khaleghparast, R. (2016). A privacy gap around the internet of things for open-source projects. In Johnstone, M. (Ed.). (2016). *The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia.* (pp.14-20).

A PRIVACY GAP AROUND THE INTERNET OF THINGS FOR OPEN-SOURCE PROJECTS

Brian Cusack, Reza Khaleghparast
Digital Forensic Research Laboratories, AUT
brian.cusack@aut.ac.nz, reza.khaleghparast @aut.ac.nz

Abstract

The Internet of Things (IoT) is having a more important role in the everyday lives of people. The distribution of connectivity across social and personal interaction discloses personalised information and gives access to a sphere of sensitivities that were previously masked. Privacy measures and security to protect personal sensitivities are weak and in their infancy. In this paper we review the issue of privacy in the context of IoT open-source projects, and the IoT security concerns. A proposal is made to create a privacy bubble around the interoperability of devices and systems and a filter layer to mitigate the exploitation of personal and private information by marketing companies.

Keywords:
IoT, Privacy, Security, Risk, Mitigation

INTRODUCTION

The rapid development of technical capability to sponsor the Internet of Things (IoT) has also impacted the daily lives of millions of people. The ability for devices and applications to provide personal services for millions of people on a moment by moment basis, has also removed immediately barriers from personal choices, behaviours and habits. The rich information around individuals opens new marketing opportunities and information opportunities for third-party exploitation. The question of privacy, concerns access to personal information. In the case of IoT private information has the same status as any information and can become readily available to multiple layers of interested parties (Weber, 2010). The bigger issue is that much of this information can be collected unknown to the end user of the IoT. The concept of the smart home, the smart car, the smart phone and other technologies, has introduced a relationship where the gap between the human and the technology is narrowed. Every movement, motion and breath of life of the human can be monitored by sensor networks and transmitted across multiple layers of interested parties. In a medical applications this may be immensely beneficial (Wan et al., 2013). However, the human may resist when they are bombarded by multiple advertising campaigns driven by harvested data from behavioural sensors and the invitation materialize in their weakest and strongest emotional moments. Privacy and privacy protection is hence a central concern when developing open source projects.

Challenges however arise in terms of scalability. IoT applications that require large numbers of devices are often difficult to implement because of the restrictions on time, memory, processing, and energy constraints (Tan, 2011). For example, calculation of daily temperature variations around all of the country may require millions of devices and result in unmanageable amounts of data. The deployment of hardware in IoT often has different operating characteristics, such as sampling rates and error distributions, interoperability protocols and complex sensors and actuators components. All of these factors contribute to the formation of the heterogeneous network of IoT in which the data of IoT will also be heterogeneous and require a multiplicity of management systems. IoT not only has the same security issues as sensor networks, mobile communications networks and the Internet, but also has its other vulnerabilities such as privacy protection, different authentication compliance, access control network configuration issues, information storage and management problems, and so on. Data and privacy protection is one of the application challenges of IoT (Chen et al, 2009). One risk is of the IoT security is from itself, and the other one comes from the related technology of construction and implementation of the network functions. IoT itself is the integration of multiple heterogeneous networks. There are compatibility issues between different networks and they are prone to security issues. For example, it is difficult to establish the junction of relationship as the relationship of trust between nodes is constantly changing and this requires a dynamic solution (Jing et al., 2014). The application of IoT directly connects with people's everyday lives and has application in many different fields, for example: patient's remote monitoring, energy consumption control, traffic control, smart parking systems, inventory management, production chains, customization of the shopping at the supermarket, and civil protection. For all of the uses, users require the protection of their personal information related to their movements, habits and

interactions with other people. They also require their privacy be guaranteed. In the literature, there are some attempts to address such problems (eg. Fabian and Gunther, 2009).

VULNERABILITIES OF IoT

IoT must ensure the security of all layers. In addition, IoT security should also include the security of whole system crossing the perception layer, transportation layer and application layer. The Perception layer includes RFID security, WSNs security, RSN security and any others. Transportation layer includes access network security, core network security and local network security. In addition there are application layer security concerns such as, 3G access network security, Ad-Hoc network security, WiFi security and so on. Different network transmission has different technology. The Application layer includes the application support layer and specific IoT applications. The security in the support layer includes middleware technology security, cloud computing platform security and so on. IoT applications in different industries have different application requirements but each requires similar diligence for protective mechanisms (Suo et al., 2013).
IoT divides into three layers: the perception layer, the transportation layer and the application layer (Tsai et al., 2014). Each of these layers further resolves into layer elements that differentiate the service provided. In figure 1 a full summary is made of the security architecture for IoT.

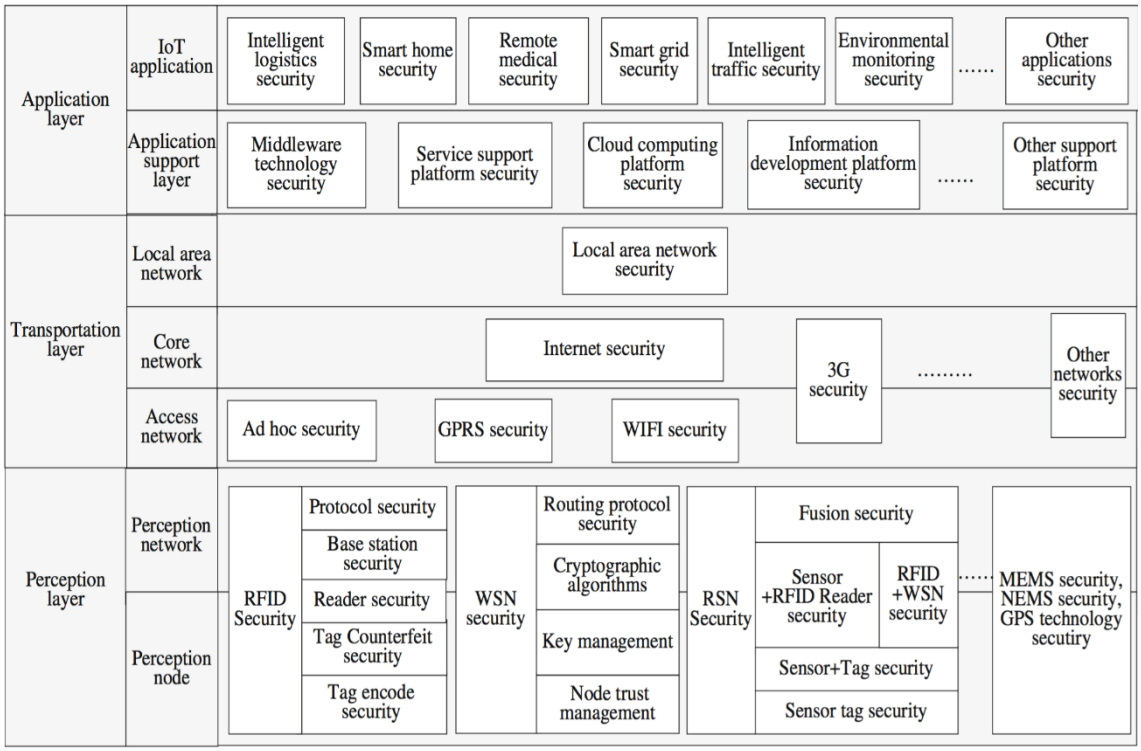

Figure 1. Security architecture of IoT (Tsai et al., 2014).

The technical architecture of the IoT has an impact on the security and privacy of the participating stakeholders. Privacy includes the concealment of personal information as well as the ability to control what happens with the information (De Turck et al., 2002; Tan and Han, 2011). The right to privacy can be considered as either a basic and inalienable human right, or as a personal right or possession. The attribution of tags to objects may not be known to users, and there may not be an acoustic or visual signal to draw the attention of the object's user. Thereby, individuals can be followed without them knowing. Electronic traces are left of their data and movement that remain in memory and in cyber- space. Further aggravating the problem (Ukil et al., 2014), it is not anymore only the authorities that are interested in collecting the respective data, but also private actors such as marketing enterprises. Since business processes are concerned, a high degree of reliability is needed. In the literature, the following security and privacy requirements are described (Akyildiz et al., 2002; Evans and Eyers, 2012):

- Resilience to attacks: The system has to avoid single points of failure and should adjust itself to node failures.

- Data authentication: As a principle, retrieved address and object information must be authenticated.
- Access control: Information providers must be able to implement access control on the data provided.
- Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

These requirements begin to shape the design of a bubble of protection that can be created around a participant in an IoT environment. However further work is required to have policies for the erasure of data that relates to personal activity, and the protection of all data from parties who wish to exploit it for economic gain (Juels, 2006; Aleaide et al., 2013).

PRIVACY CONCERNS OF IoT

The fulfilment of customer privacy requirements is a challenging problem. A number of technologies have been developed in order to achieve information privacy goals. These Privacy Enhancing Technologies (PET) can be described in short as follows (Fabian et al., 2007; Haitao and Ting, 2012):

- Virtual Private Networks (VPN) are extranets established by close groups of business partners. As only partners have access, they promise to be confidential and have integrity. However, this solution does not allow for a dynamic global information exchange and is impractical with regard to third parties beyond the borders of the extranet.
- Transport Layer Security (TLS), based on an appropriate global trust structure, could also improve confidentiality and integrity of the IoT. However, as each ONS delegation step requires a new TLS connection, the search of information would be negatively affected by many additional layers.
- DNS Security Extensions (DNSSEC) make use of public-key cryptography to sign resource records in order to guarantee origin authenticity and integrity of delivered information. However, DNSSEC could only assure global ONS information authenticity if the entire Internet community adopts it.
- Onion Routing encrypts and mixes Internet traffic from many different sources, i.e. data is wrapped into multiple encryption layers, using the public keys of the onion routers on the transmission path. This process would impede matching a particular Internet Protocol packet to a particular source. However, onion routing increases waiting times and thereby results in performance issues.
- Private Information Retrieval (PIR) systems conceal which customer is interested in which information, once the EPCIS have been located. However, problems of scalability and key management, as well as performance issues would arise in a globally accessible system such as the ONS, which makes this method impractical.
- A further method to increase security and privacy are Peer- to-Peer (P2P) systems, which generally show good scalability and performance in the applications.

The following are reviewed literature provides further information regarding the privacy elements in a security bubble for an IoT user. In Gurses et al. (2006) a data tagging for managing privacy in IoT is proposed. Using techniques taken from the Information Flow Control, data representing network events can be tagged with several privacy properties; such tags allow the system to reason about the flows of data and preserve the privacy of individuals. Although exploiting tagging within resource-constrained sensor nodes may not be a viable solution because tags may be too large with respect to the data size and sensitivity, therefore they generate an excessive overhead. Clearly, in this case it is not suitable for IoT. In Huang et al. (2012) a user-controlled privacy-preserved access control protocol is proposed, based on context-aware and anonymity privacy policies. The privacy protection mechanisms are investigated in the research and the users can control which of their personal data is being collected and accessed, who is collecting and accessing such data, and when this happens. In Cao et al., (2011) it is presented Continuously Anonymizing streaming data via adaptive clustering (CASTLE). It is a cluster-based scheme which ensures anonymity, freshness, and delay constraints on data streams, thus enhancing those privacy preserving techniques (e.g., k-anonymity) that are designed for static data sets and not for continuous, unbounded, and transient streams.
In Aleaide (2013), the traditional privacy mechanisms are divided into two categories: Discretionary Access and Limited Access. The former addresses the minimum privacy risks, in order to prevent the disclosure or the cloning of sensitive data; whereas the latter aims at limiting the security access to avoid malicious unauthorized attacks.

Blass et al. (2011) analyses the privacy risk that occurs when a static domain name is assigned to a specified IoT node. In this work the authors propose a privacy protection enhanced DNS (Domain Name System) for smart devices, which can authenticate the original user's identity and reject illegal access to the smart device. The scheme is compatible with widely used DNS and DNSSEC (Domain Name System Security Extensions) protocols. In Elkhiyaoui et al., (2012) a fully decentralized anonymous authentication protocol for privacy-preserving target-driven IoT applications is presented. Such a proposal is based on a multi-show credential system where different showings of the same credential cannot be linked together, therefore avoiding the generating keys to be discovered. The system defines two possible roles for participant nodes. There are users, which represent the nodes originating the data, and data collectors, which are responsible for gathering the data from authorized users. Users can anonymously and unlinkably authenticate themselves in front of data collectors proving the owning of a valid Anonymous Access credential (AAC) encoding a particular set of attributes, established by the system itself. The protocol is divided in three phases: set-up, user registration, during which users obtain Anonymous Access Credentials, and Credential Proving, during which users prove the possession of a valid AAC to a data collector. Such a protocol guarantees: user anonymity, AAC un-linkability (no Data Collector or set of colluding Data Collectors can link two transactions to the same User), resistance to user impersonation, faulty and selfish nodes, nodes hindering the efficiency, and adversary controlling the Data Collectors. Moreover, such a system relies on a fully distributed approach, thus avoiding single point of failure issues. Sunmaker et al. (2010), starting from the privacy preserving data mining (PPDM) techniques, and aims at minimizing the sensitive data disclosure probability and the sensitive content analysis. In such a work, the user privacy awareness issue is addressed, proposing a privacy management scheme which enables the user to estimate the risk of sharing sensitive data. It also aims at developing a robust sensitivity detection system, able to quantify the privacy content of the information (Hachem et al., 2011).

USE CASES

Amazon Echo is a small hands-free wireless speaker that is controlled by voice. The voice command technology called "Alexa," that is inside Amazon Echo is now available on other devices, including the Amazon Fire TV and the Amazon Echo Dot and Amazon Tap. These devices exhibit state-of-the-art artificial intelligence that facilitates human requirements and human interaction. The concept is grown from a belief that all of human experience may be represented by artificial intelligence that is supported by information technology and physical devices. The information architecture shows voice command technology that allows the user to manage, control and demand personal experiences. The information requirements are managed by sensors, processes and mediating software to assure the end user has full connectivity. The IoT systems architecture is design for interoperability across different requirements so that the system may be implemented in a home, a motor vehicle, a business, or any other social situation. It allows artificial intelligence to control the requirements to satisfy the experience. The concept is that Alexa is a human friendly personification that access an access point to a multitude of systems and services. It only requires "invocation words" that tell Alexa what Skill or service that is to be activated. The communication requires a person to say things like "Alexa, ask Scout to arm my security system" or "Alexa, ask Fitbit what my resting heart rate is." (Wan et al., 2011).

These use cases of IoT are being developed as open source projects. The developers are working to make it easier for third-parties to create Skills that don't require invocation words at all. For instance, smart home gadgets that create Alexa Skills using Amazon's open application programming interface (API) will get to use existing code and standardized Alexa vocabulary for things like lights, switches, and thermostats. In this way the concept of the smart home can be built around an IoT plan and human experience may be captured within the technological confines. Software such as Alexa are leading the way for creative developers to design and implement this new future. To utilize these technologies the user says the word "Alexa," and from then on the automation monitors everything in around the human experience. The concept is strong but the privacy issues still remain. Questions arise regarding the supervision of these types of technologies. What happens if Echo is left unsupervised? The technologies are not only smart in the sense that they may be communicated to deliver actions services and experiences, but they also open the user to a global communication world through the IoT. The security wireless signals is notoriously vulnerable to external influence making the human experience vulnerable to unintended failures. Similarly the information generated regarding human behaviour may be recorded and transmitted for commercial interests. Marketing for example may become more targeted and better represent a requirement within the human life world. To some this may be a benefit but to others it may be deemed invasive (Wang and Wen, 2011).

Commercial interests are in the business of selling everything humans need from clothes to groceries, electronics goods, gifts and so on. To do that better and more efficiently, they need to know more about their users, their friends, their family and social networks. By knowing more about the users' information, they can better suggest new experiences for purchase, and to exactly time when to make the offer. Some of the characteristics collected by Alexa (through Echo) are:

- **Unique home occupants:** Echo is able to distinguish between the numbers of unique voices in a home and to map these voices onto registered users and images of people in the home.
- **Home visitors:** Echo can identify and monitor who comes to a home. This is for intended and unintended visitors, such as friends and burglars.
- **Gender and age:** From voice and photographic data trapped by Echo gender and age may be estimated.
- **Happiness, sadness, anger:** emotional states can be monitored and moods such as happiness and sadness, anger and delight, and so on can be instantaneously recorded and transmitted.
- **Who is home:** Echo can learn patterns of behaviour and detect movement within a home. From this learning real-time being is established and also all the interactions are accessible.
- **What we watch and listen to:** Echo can hear everything that is going on that includes preferences for television channels, music, statements about products being used, political statements, personal relationship statements, and so on, and so on. Such data provides up-to-date information on personal preferences although the human may not be conscious that these things are being recorded and matched against patterns.

To create a privacy bubble around the human some security features have already been built into Alexa. However the technology can do a lot if left unsupervised that not only includes cleaning the house but also being responsive to multiple layers of communication networks from outside of the home. One of the things that has been done to quell some of the automation fears is to add a variety of voice controls that put the technology into various sleep modes. These types of controls are necessary if the human is to maintain control over their private information that includes movements, locations, emotions, habits, and many other personalised information is that would not normally be made public. The intrusion of commercial interest into the spaces and the precision with which generalizations can be made is a new phenomenon. These are matters that the IoT has introduced (Yang and Fang, 2011; Jing et al., 2014).

Privacy security bubble

Our advocacy in this paper, after the review of the relevant literature, is to have a proximity around technology in which the user has protection for the use of their information. To achieve this the user must first be given the rights of ownership to their own information. At present within the multiple layers of system the content created within a word processor for example may have multiple ownership challenges. The user and creator of the content may not be aware of these competing digital rights that are behind what they are doing. In a similar sense people using robot vacuum cleaners, automated software on their mobile phone, motor vehicles, hospital services, financial services, and so on, may not be aware, and in effect may not have the digital rights to the content that they have created with the efficacy of their presence and actions. The privacy requirement in IoT is currently inadequately unaddressed and there is a wide set of research issues yet to be investigated. Privacy policies starting from a well-defined model and the correspondent development of policies that adequately deal with the scalability and the dynamic environment characterizes IoT scenarios are required. Capturing privacy requirements in the very early stages of project development is essential for creating public confidence and the adoption of novel IoT systems. Private enterprises using IoT technology will have to include these requirements into their risk management plans for governing the business activities in general.

The IoT is susceptible to intentional and unintentional compromise of information. The complexity of IoT security was shown in figure 1. Usual Internet services and other communication services are familiar with protection for the transport and application layers. However the IoT introduces the concept of the perception layer. The perception layer is made up of networks and nodes that are both social and machine. The mixing of these two elements in the perception concept introduces an ambiguity that cannot be easily addressed. The issues of ownership around information that is mediated and hosted by machines is much more difficult than the adjudication of common property rights. The owners of the machines can lay claim to content, the owners of the software can lay claim to content, and the user of the systems and the machines may not be in a position to realise that data has been created regarding their own behaviours. The user of IoT experiences and services may also not be in a position to challenge the owners of the technology and the hosted services. This therefore creates an imbalance of power that requires redress in the fashion that we suggest whereby the user and participant in the IoT environment is given a proximity measure in which they hold a primary ownership of the data. The management of such a privacy and security bubble can be done by honouring the proximity metric and enforcing it transaction by transaction. This will require the

partitioning of data into private and public categories at the point and within the modes of production. The proximity measure can be enforced as a contractual arrangement and all the other interested parties must negotiate with the human factor for access to any data created within the proximity boundary or from instances within the proximity boundary. At present such arrangements are not in place and there is no boundary for privacy. The privacy requirement in IoT is currently emerging issue by issue and it will only be when developers are impacted financially by end user resistance that the problem will be taken seriously. Consideration is required for building the privacy requirement into the front end of a project as a bubble of protection for the end-user. Suitable survey of potential end users and full HCI analysis are necessary components of every project. Human factor vulnerability and the potential exploitation of the personal data can be treated with these measures.

CONCLUSION

In this paper we have reviewed literature that addresses the security and privacy issues in the IoT. The use case of Amazon's Alexa devices illustrates open source projects that are currently active and developing. Our consideration is to assure that there is a bubble of security and privacy around the user experience so that they are adequately protected from exploitation and manipulation by multiple parties who may get access through the technology. It would be reasonable to have legislation that prescribes a proximity in terms of a physical metric around and IoT user, and anything within that proximity is owned by the user. This would mean that advertising companies and others who seek to exploit this information would have to gain permission from the owner of the information before they use it. In a hospital situation the patient already signs away these rights but with a mobile device or the sensor systems within a motor vehicle, the user is not aware of where their data is going, who was looking at it and who may have access to use it. Privacy rights advocates have called for limits on the information that companies can collect and use, but the truth is that our privacy is already being breached on a daily basis. However, that does not mean that we should voluntarily give up more of our privacy through the purchasing of devices such as the Alexa (Echo Dot), automated motor vehicles, or Pokémon applications.

REFERENCES

Akyildiz IF, Su W, Sankarasubramaniam Y, (2002). Wireless sensor networks: a survey. Computer networks 38:393-422 (2002)

Alcaide A, Palomar E, Montero-Castillo J et al. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. Computers & Security 37:111-123.

Blass E-O, Elkhiyaoui K, Molva R. (2011). Tracker: security and privacy for RFID-based supply chains. In: In NDSS'11, 18th Annual Network and Distributed System Security Symposium, 6-9 February.

Cao J, Carminati B, Ferrari E et al. Castle. (2011). Continuously anonymizing data streams. IEEE Transactions on Dependable and Secure Computing 8:337-352.

Chen M, Kwon T, Mao S. (2009). Spatial-Temporal relation-based Energy-Efficient Reliable routing protocol in wireless sensor networks. International Journal of Sensor Networks 5:129-141.

De Turck F, Vanhastel S, Volckaert B. (2002). A generic middleware-based platform for scalable cluster computing. Future Generation Computer Systems 18:549-560.

Elkhiyaoui K, Blass E-O, Molva R (2012). CHECKER: On-site checking in RFID-based supply chains. In: Proceedings of the fifth ACM conference on security and privacy in wireless and mobile networks. ACM, p 173-184.

Evans D, Eyers D. (2012). Efficient data tagging for managing privacy in the internet of things. In: Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, p 244-248.

Fabian B, Günther O. (2009). Security challenges of the EPCglobal network. Communications of the ACM 52:121-125.

Fabian B, Gunther O. (2007). Distributed ONS and its Impact on Privacy. In: 2007 IEEE International Conference on Communications. IEEE, p 1223-1228.

Gürses S, Berendt B, Santen T (2006). Multilateral security requirements analysis for preserving privacy in ubiquitous environments. In: Proceedings of the UKDU Workshop. p 51-64.

Hachem S, Teixeira T, Issarny V (2011). Ontologies for the internet of things. In: Proceedings of the 8th Middleware Doctoral Symposium. ACM, p 3.

Haitao LBCHW, Ying F (2012). Security Analysis and Security Model Research on IOT. Computer & Digital Engineering 11:006.

Hamad F, Smalov L, James A (2009). Energy-aware Security in M-Commerce and the Internet of Things. IETE Technical review 26:357-362.

Huang X, Fu R, Chen B et al. (2012) User interactive internet of things privacy preserved access control. In: Internet Technology and Secured Transactions, 2012 International Conference for. IEEE, p 597-602.
Itu-T Y (2009). Overview of ubiquitous networking and of its support in NGN. ITU-T Recommendation.
Jing Q, Vasilakos AV, Wan J. (2014). Security of the internet of things: Perspectives and challenges. Wireless Networks 20:2481-2501.
Juels A (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications 24:381-394.
Sundmaeker H, Guillemin P, Friess P et al. (2010) Vision and challenges for realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision.
Suo H, Liu Z, Wan J et al. (2013). Security and privacy in mobile cloud computing. In: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, p 655-659.
Tan Y, Han J (2011). Service-oriented middleware model for internet of things. Computer Science 38.
Tsai C-W, Lai C-F, Vasilakos AV (2014). Future Internet of Things: open issues and challenges. Wireless Networks 20:2201-2217.
Ukil A, Bandyopadhyay S, Pal A (2014). Iot-privacy: To be private or not to be private. In: Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on. IEEE, p 123-124.
Wan J, Chen M, Xia F et al. (2013). From machine-to-machine communications towards cyber-physical systems. Comput. Sci. Inf. Syst. 10:1105-1128.
Wan J, Yan H, Suo H et al. (2011). Advances in Cyber-Physical Systems Research. TIIS 5:1891-1908.
Wang Y, Wen Q (2011). A privacy enhanced dns scheme for the internet of things. In: Communication Technology and Application (ICCTA 2011), IET International Conference on. IET, p 699-702.
Weber R. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review 26:23-30.
Yang J-C, Fang B-X (2011). Security model and key technologies for the Internet of things. The Journal of China Universities of Posts and Telecommunications 18:109-112.