The Quest for Privacy in the Internet of Things

Pawani Porambage and Mika Ylianttila, University of Oulu, Finland
Corinna Schmitt, University of Zurich, Switzerland
Pardeep Kumar, UiT the Arctic University of Norway
Andrei Gurtov, Aalto University, Finland
Athanasios V. Vasilakos, Lulea University of Technology, Sweden

To be successful, Internet of Things deployments will require secure, trustworthy, and privacy-preserving infrastructures. This survey explores IoT privacy challenges and potential solutions.

In the Internet of Things (IoT) paradigm, objects that people use to manage, monitor, and optimize the operational aspects of their daily activities are no longer unresponsive devices. Instead, they're interactive devices connected to the Internet with intelligence and many more capabilities (such as sensing, communication, processing, and storage).[1,2] However, privacy attacks and harmful consequences can occur when sensitive information is concealed or controlled without users' consent.[2] Because of application interdependency and data sensitivity, a small leakage of information could severely damage user privacy. Further, users will accept IoT deployments only if the infrastructures are secure, trustworthy, and privacy-preserving.

Because IoT comprises heterogeneous networking technologies and devices—such as radio frequency identification (RFID) tags, smartphones, and sensors—it's challenging to deploy conventional privacy protocols, as high-performing devices sometimes require advanced protocols that are too bulky for these small devices. However, lightweight privacy solutions are easily tractable by powerful attackers.[2]

Cisco estimates that by 2020 there will be more than 50 billion Web-enabled devices, including refrigerators, televisions, and scales.[3] Internet and cloud service providers (ISPs and CSPs) and consumers have already encountered many global privacy threats due to the use

of pervasive products and services. Recent press reports highlight several privacy violations in IoT applications.[4,5] For example, in June 2013, the press revealed privacy risks related to the Planning Tool for Resource Integration, Synchronization, and Management (PRISM) program, which the US National Security Agency uses to collect private electronic data belonging to users of major Internet services including Microsoft Outlook, Google, and Facebook. Further, an annual Internet security threat report claims that mobile malware attacks increased by 58 percent from 2011 to 2012, and 32 percent of those attacks attempted to steal information from the device's contact information.[5] According to a US Federal Trade Commission (FTC) report on consumer privacy, privacy by design (PbD) is the most prominent approach to overcoming IoT privacy issues.[6]

Here, we offer a holistic overview of privacy issues and challenges related to IoT technologies and applications. Compared with previous literature, we provide a broader synopsis of current research on various aspects of IoT privacy and PbD solutions from the viewpoints of academics, industries, and the general public. In addition to describing existing solutions and promising emerging approaches, we discuss open research issues and design guidelines for preserving privacy in the IoT.

Layered Representation IoT Technologies

The continuous evolution of the IoT architecture and the complexity of its underlying technologies—as well as the many visionaries involved in its development—makes it difficult to define with solid boundaries.

A horizontal representation of IoT driver technologies illustrates the connectivity and common operational platforms (Figure 1).[1,3] The functionalities of the layers presented in Figure 1 are defined with respect to the Open Systems Interconnection (OSI) model layers. The *edge network layer*, which corresponds to the OSI model's physical layer, is the data perception layer, which is responsible for sensing the physical environment, collecting real-time data, and reconstructing a general perception of the data. These technologies and devices typically have short-range communication, constrained batteries, and low storage and computational power. The *access network layer* represents the data link layer

and has heterogeneous communication technologies that enable the first stage of data transmission in terms of communication path handling and data publishing. This layer's major services include message routing, publishing, and subscribing.

The *core network layer* relates to the OSI network layer and consists of the conventional Internet Protocol and Multiprotocol Label Switching (IP/MPLS). This layer is also responsible for processing networking data and billing, as well as managing data, maintaining quality of service, supporting visualization, and enabling network security. The *service and middleware layer* resembles the OSI model's transport, session, and presentation layers. This layer abstracts and then forwards the various data formats, technologies, and communication protocols of the lower layers. It also provides data management, data filtering, data aggregation, semantic analysis, and information utilization through the management servers that facilitate cloud computing and data mining technologies. On top of it all, the *application layer*, like the application layer in the OSI model, represents the various purposes of IoT technologies from local, national, and industrial perspectives. The ultimate goal is to ensure the usability of IoT applications with low complexity and high credibility.

IoT Applications and Privacy Concerns

Privacy is the right of individuals or cooperative users to maintain confidentiality and control over their information when it's disclosed to another party. In IoT applications, privacy challenges can be identified primarily from the perspective of consumers and their stored datasets. Because both CSPs and ISPs possess a user's (client's) personal information, they could unexpectedly initiate privacy threats and attacks.

IoT networks can comprise tens to millions of devices with heterogeneous characteristics related to resource constraints, mobility, scalability, degree of autonomy, interoperability, and so on. Thus, privacy issues in IoT vary widely with respect to the applications involved.

Healthcare

One main application area is eHealth, which aims to improve the quality, efficiency, and cost of healthcare by enabling physicians to remotely monitor their patients, as well as letting individuals manage
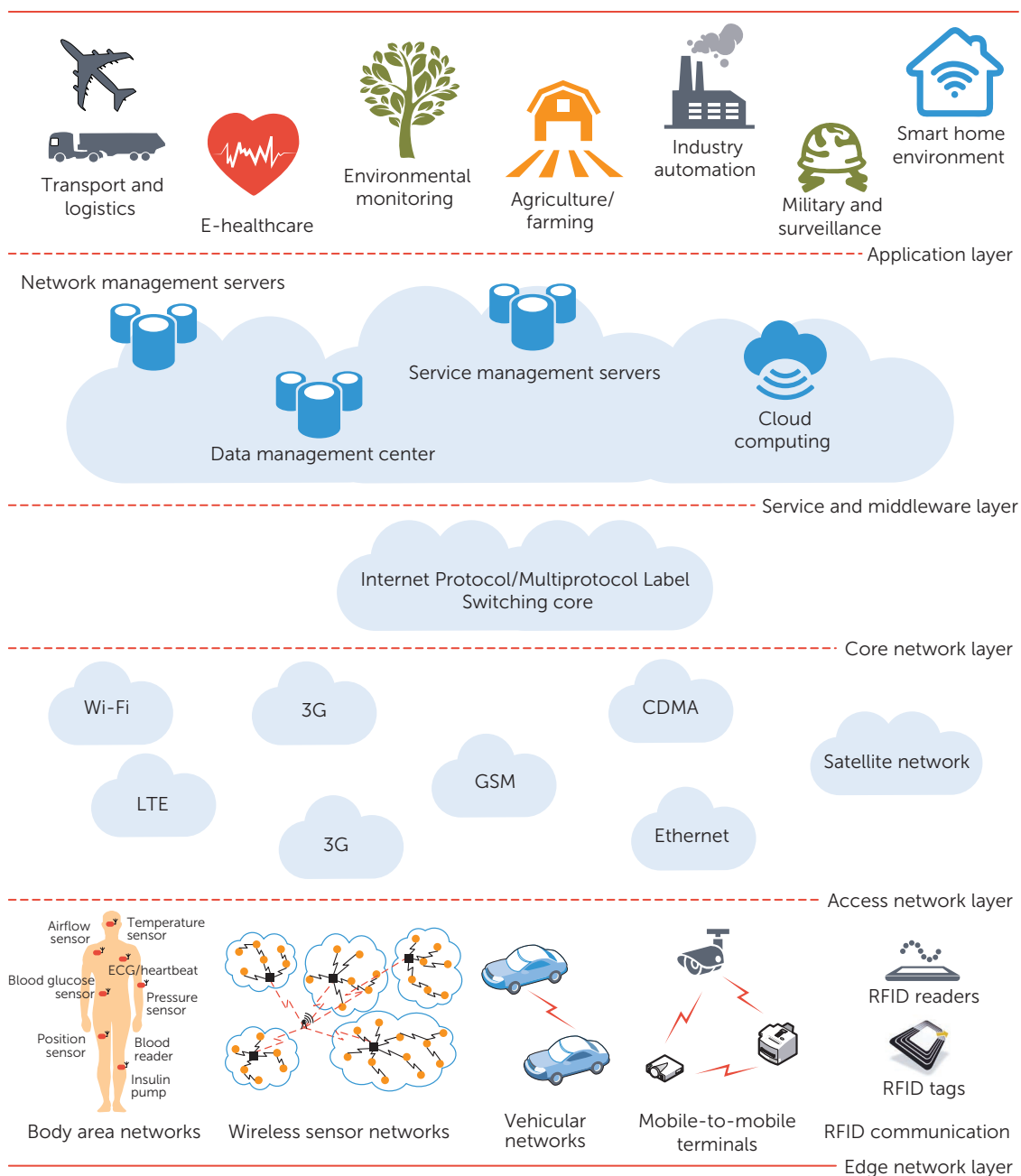
FIGURE 1. Horizontal representation of Internet of Things (IoT) driver technologies. The layers relate to the Open System Interconnection (OSI) model layers. (CDMA: Code division multiple access; GSM: Global System for Mobile Communications; LTE: Long-Term Evolution)

their own health records easily and facilitating independent living (such as through wearable health monitors for blood pressure, heart rate, and glucose level; smart apparel; and fitness trackers).[1] However, increasing the accessibility and availability of personal health records on the Internet can also lead to serious privacy issues. In June 2015, for example, a huge privacy-violation attack occurred when mal-

ware compromised blood gas analyzers to gain access to hospital networks and steal confidential data.[4] Given the risks, the privacy frameworks for IoT eHealth applications are expected to be open and transparent to patients, specify the reasons for collecting necessary health information, maintain accurate and up-to-date information, and ensure the protection of patient records.

Smart Homes

In smart home environments, consumers can control, monitor, and measure power consumption in their home appliances remotely via the Internet. Because ISPs might have access to the overall operations and collected information about users' behaviors with or without their consent, this area also poses a potential threat to users' privacy. Residents can use RFID and sensing technologies to identify and track objects, as well as to monitor the smart home conditions.[7] If intelligent adversaries eavesdrop and accumulate timestamps of data transmissions over wireless channels, they can easily draw conclusions on residential behavioral patterns (such as when residents are at home, away, or sleeping). Because sensors and RFID tags have unique radio wave patterns and identifiers, attackers can also analyze the transmission patterns and reveal approximate information about the home's internal arrangement.

Public Safety

IoT-enabled technologies are also engaged in public safety solutions, offering cheaper and less invasive alternatives to the widespread deployment of embedded monitoring units (such as sensors, RFID techniques, and cameras). However, when too many Internet-connected modules are used in daily life, owners might not be able to fully control them. This allows governments and corporations to follow individuals' moves with or without their consent. Likewise, with the widespread use of IoT applications, all online and offline activities will be recorded and stored forever. This raises questions such as who will have access to all of this information and under what rules, and whether the public will be subjected to serious privacy infringement.[2]

Supply Management

Supply management applications in the IoT would enable seamless interoperability between RFID-based applications and different actors throughout the various phases of a product's lifecycle. Product information can be recorded beyond the manufacturing level to the purchasing and consumption levels.[7] Consequently, manufacturing companies can track customer information based on that product information. Moreover, vehicular ad hoc networks (vanets) play a major role in the IoT through intelligent transportation. When managing energy use in smart grids, consumers provide detailed information about their daily electricity consumption.[1] Such information can be used to reveal their habits and behaviors, and expose them to privacy invasions. User data about electricity consumption can be tapped

from anywhere in the Internet and can reveal user behavior patterns and private data. Because customers have less control over the data they provide to utility companies, the potential for privacy abuses could increase.

Privacy Issues and Challenges

To clearly present this material, we discuss the technological aspects of IoT privacy issues and challenges from the viewpoint of users, datasets, and underlying technologies. In addition to the technical challenges, we discuss the significant issues related to legal regulations on IoT privacy. Figure 2 summarizes the four key aspects of IoT privacy.

User Privacy

One serious user privacy issue is the identification of personal information during transmission over the Internet.[2,7] Let's say, for example, a consumer named Bob buys an RFID-tagged object with his credit card. In some situations, Bob's personal information could be automatically linked to the object and known to the CSP. Such user information leakage can lead to privacy threats in terms of tracking, localizing, and personalization. Similarly, let's assume Bob possesses a set of objects that are linked together. If adversaries can distinguish ownership of certain objects, they might be able to estimate the ownership of the remaining objects.

These types of scenarios allow user profiling and tracking. Smartphones and other mobile devices connected to the Internet could disclose the user's geographic location and compromise privacy. In practice, users have different levels of privacy awareness and concern, and thus are ready to disclose information at different levels.

In general, IoT users might encounter privacy threats in terms of tracking, profiling, access control and confidentiality, data protection, content confidentiality and reliability, and privacy detection. Because of the IoT's range, manifold privacy risks and challenges must be considered before deploying an application or solution.

Data Mining

According to Charu Aggarwal and his colleagues, three critical enablers of IoT privacy from a data-centric perspective are scalability, distributed processing, and real-time analytics.[8] Other privacy issues they identified in this area relate to data publishing, the context of applications, utility issues, cryptography, and adversarial collaboration.[8] Scalability matters for IoT applications that contain numerous smart objects or that manage biometric
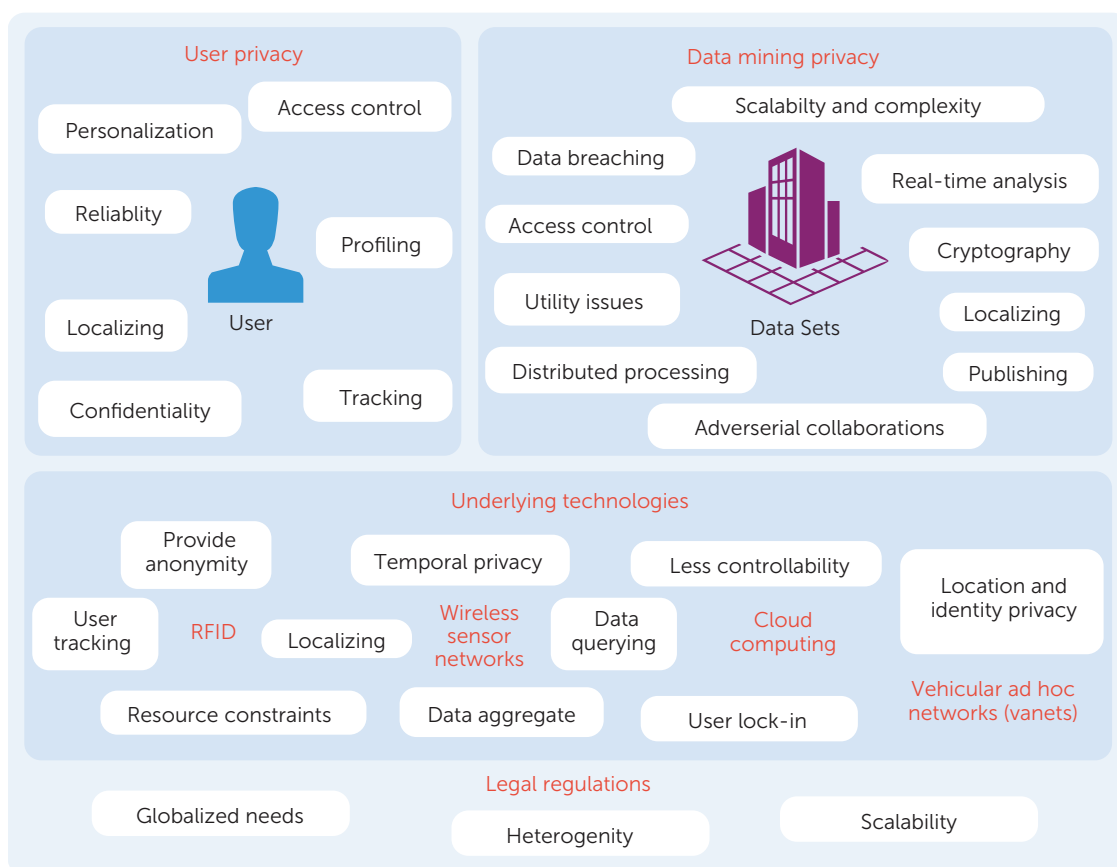
FIGURE 2. Technological and legal aspects of privacy issues in the IoT.

data that must be collected, processed, stored, and published in large volumes of real-time, highly distributed data. Distributed processing can also lead to unprecedented challenges related to data mining privacy, along with liability for data breaches (that is, the release of secure information to distrustful entities) and distinct levels of data quality. Privacy threats related to data sharing and transmitting arise with the disclosure of location and temporally sensitive data traffic. While collecting large sets of raw data, it's challenging to balance the privacy preservation in data cleaning and the intentional reduction of data quality and original purpose without losing information needed for data mining and analysis. Collecting, sharing, and transmitting sensitive data connected to humans are the most critical privacy issues in the context of applications. Computational and theoretical limitations can be associated with privacy preservation over high-dimensional datasets. Because individuals and cooperative users have different privacy constraints, the records in a given dataset should be treated differently for anonymization purposes. The collected

data might be used and published for purposes other than the original objective without user consent. Access control and maintenance of such data, with the assurance of privacy protection for the corresponding data owner should be carefully considered. Because computer storage mediums can store large volumes of data, they offer high availability at low cost. Consequently, once information is generated, it's most likely stored infinitely, and thus "digital forgetting" can lead to privacy violations from the data owners' perspective.[1]

Underlying IoT Technologies

The incorporation of RFID objects within an IoT environment can allow context-aware digital objects to represent physical objects with the abilities to sense, communicate, and interact autonomously.[2,7] Powerful adversaries might exist who can monitor all communications, trace tags within a limited time period, corrupt tags, and get side channel information on the reader output. Privacy risks of RFID technology relate to user tracking and localizing, which permit the creation and misuse of detailed

user profiles. Thus, it's important that RFID systems provide anonymity, even when the state of a tag has been disclosed.

Wireless sensor networks (WSNs) are another key underlying technology of the IoT network architecture. Given their self-organizing characteristics (to contend with the uncontrollability of the environment), constraints (such as sensor resources and network topology constraints), and the wireless transmission medium, WSNs have inherent challenges in protecting privacy and prevent existing techniques (such as public-key ciphers) from being directly transplanted in resource-constrained devices.[8] Privacy in WSNs can be addressed through data orientation (that is, querying data and aggregating sensed data without violating privacy) and context orientation (that is, protecting location and temporal privacy).[8]

Cloud computing provides a virtual infrastructure for IoT to integrate monitoring devices, storage devices, data analytics tools, visualization platforms, and client delivery.[3] This virtual infrastructure would let ubiquitous sensing devices, smart objects, users, and CSPs join the network and collaborate on a single virtual platform. With cloud computing, both individual and cooperating users can access cloud services at a low cost and without possessing expert knowledge of the underlying technologies. Nevertheless, privacy violations can occur, as users might lack control over the data processing. Therefore, the platform CSPs and developers must take responsibility for application privacy. They must protect identity information, the policy components (during negotiation), and transaction histories of the consumers, as well as provide a high degree of transparency in their operations. User lock-in scenarios can also occur when consumers are too dependent on and trusting of a particular IoT CSP. This can be intimidating, particularly when consumers want to migrate from one IoT CSP to another, but they've already revealed important information to the existing CSP and lack control over their data.

Vanets embed an on-board unit (OBU) into the vehicle system as a sensing layer node in the IoT.[9] This node communicates to the roadside infrastructure and other peer vehicles. Therefore, establishing secure communication links and providing authentication are two key requirements to enable security and privacy in vanets. Consequently, the OBU requires additional modules to support information security to ensure user privacy at the same level as identity and location privacy.

Establishing Legal Regulations for IoT Privacy

Privacy is a compliance issue sitting at the intersection of social norms, human rights, and legal mandates. In general, the participating countries' legislation is required to support basic privacy principles such as lawfulness and fairness, proportionality, purpose specification, data quality, openness, and accountability. This can be achieved through a collaboration of governmental and private organizations. The European Commission, United Nations' authorities, and other worldwide law enforcement organizations are trying to find a common ground for addressing IoT privacy issues while also empowering the existing legal framework. A strong legal framework should ensure consumers' awareness and their control over the IoT products and services they utilize.[7] National-level regulations aren't acceptable for IoT privacy because of its global nature. An adequate legal framework

> An adequate legal framework should be cross-border and compliant with international legislation.

should be cross-border and compliant with international legislation, and supplemented by the privacy sector. Although self-regulation is a simpler and less costly solution than state laws for preserving privacy, it's not enough for IoT applications due to their large-scale heterogeneous network deployments. The most challenging issues in establishing legal regulations in IoT privacy are the globally marketed and distributed nature, the durability, the involvement of pervasive environments, and the complexity of the technological developments.[7]

Privacy Framework Characteristics and Existing Solutions

After examining the complementary pieces of technology- or application-specific privacy frameworks and the IoT network attributes (that is, the technological aspects and legal regulations), we identified the most important characteristics of an IoT privacy framework (see Figure 3)[2]:

- *Openness, transparency, and a specified purpose:* consumers should be aware of the information collected during service time, the purpose of collecting that information, other parties who
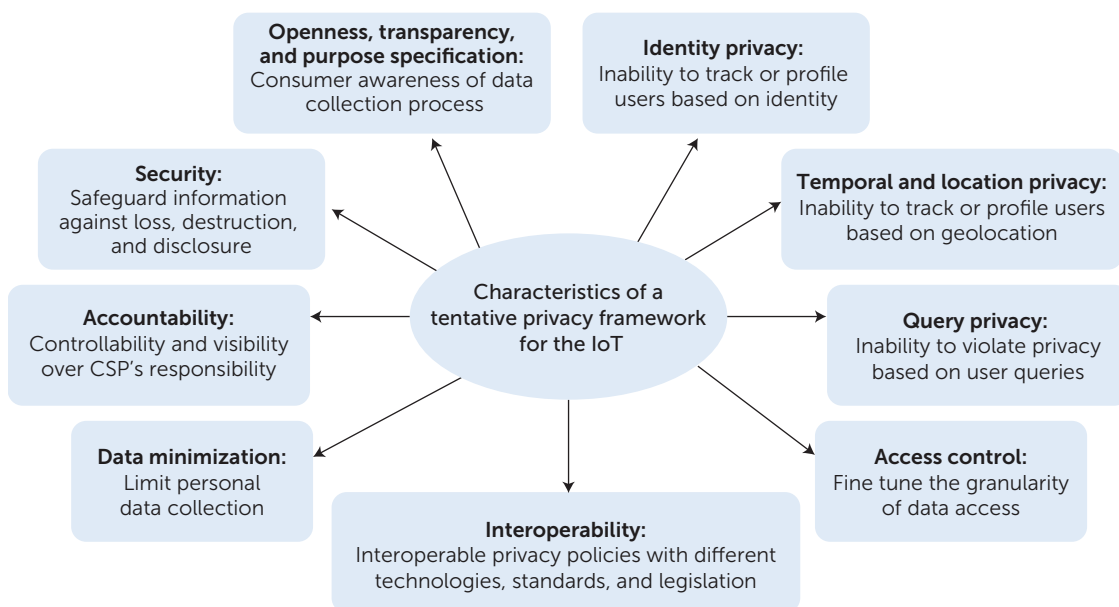
FIGURE 3. Characteristics to include when developing an IoT privacy framework.

will have access to the information, and how that information will be stored.

- *Identity privacy*: it should not be possible to profile or track consumers based on their user identities.
- *Temporal and location privacy*: it should not be possible to track or profileconsumers based on events or geolocation.
- *Query privacy*: it should not be possible to profile or identify consumers based on the queries they make to service providers.
- *Access control*: users should have fine-grained access control over the data they give to service providers and be able to tune the granularity of data access depending on the users and queries.
- *Interoperability*: enable cross-border support of privacy policies among different technologies, standards, and legislation.
- *Data minimization*: collect data in lawful and fair ways and limit personal data collection to data needed to perform a given service.
- *Accountability*: the consumer and service provider should agree about the controllability and visibility of the service provider's responsibility with respect to the given service or information.
- *Security*: safeguard sensitive information against loss, unauthorized access, modification, or disclosure.

The relevance of these principles might vary depending on the contexts of the IoT application scenarios and user requirements. For instance, healthcare, smart home, and surveillance applications have high sensitivity regarding privacy-related frameworks and legal regulations. In addition to these technical characteristics, IoT privacy frameworks should always meet global legal and human rights requirements.

Existing Solutions

Several privacy-enhancing technologies (PETs) have been proposed for IoT-related applications.[7] Most existing solutions are specific to the underlying technologies or application scenarios. Privacy-oriented cryptographic solutions have been introduced for both internal and external privacy attacks occurring in WSNs.[10] However, computationally powerful attackers who can break cryptographic puzzles might pose threats to these systems. Also, resource-consuming cryptographic operations can create overhead on normal WSN operations. Current PETs for RFID technologies include limiting the distance between the reader and tags, minimalist cryptography, tag renaming and deactivation, access control, and reencryption. Minimalist cryptographyis proposed to perform cryptographic computations at the reader end, storing the resulting information in the tags. The reader can reencrypt the tag with a different key and write itinto its memory in such a way that an eavesdropper gets different encrypted tag signals at different times. Another approach is to use moderate to high-performing devices—that is, proxies—with RFID tags to protect consumer privacy.

PETs in RFID have two main objectives: to prevent unauthorized access to RFID tags by establishing secure tag-reader communication, and to preserve consumer privacy. The "privacy coach" is an interesting idea for supporting customer privacy in the IoT.[3] A privacy coach is a mobile phone application that supports customers in making privacy decisions when confronted with RFID tags embedded in smart objects. Another approach is to use aproxy as a privacy broker for preserving privacy between service providers and users.[3] This guarantees that both parties obtain required information about the other party; however, privacy proxies can create scalability and interoperability issues in IoT networks.

The Unified Modeling Language can be used to document the software requirements of IoT privacy policies, which require high-level abstraction and are suitable for heterogeneous IoT devices and services.[2] Alternatively, user privacy in the IoT can be accomplished by adapting the methodologies available for identity and location-privacy protection of hosts by exploiting public-key cryptographic algorithms and forwarding agents. Privacy-preservation technologies for data mining include statistical methods for disclosure control, such as k-anonymity, swapping, randomization, micro-aggregation, and synthetic data generation. These methodsprovide privacy-preserving approaches to the IoT through a data-centric perspective.[8] Cloud computing also adapts different privacy-preserving approaches, including data-centric, accountability, cryptography, access control, authentication, and identity management.[3] More importantly in cloud computing, service-level agreements should be clearly negotiated among stakeholders so they preserve every party's privacy. However, the technology-specific privacy-protecting mechanisms don't always provide absolute solutions for the globalized view of IoT privacy preservation.
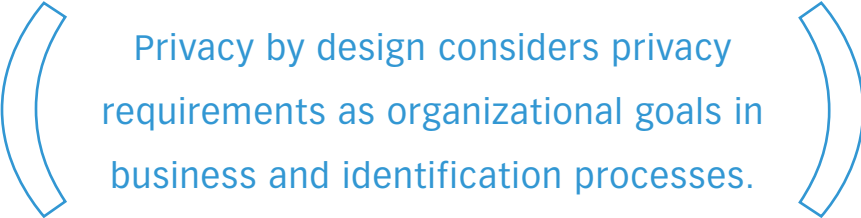
Privacy by Design
The PbD approach is a security requirement engineering methodology that considers privacy requirements as organizational goals in business and identification processes.[11,12] PbD includes seven fundamental principles:

- Anticipate and prevent privacy-invasive events at the design stage (before they occur).
- Inform queries by following purpose specification, collection limitation, data minimization, and disclosure limitation.

- Embed privacy into the solution design.
- Obtain full functionality with a win–win situation at the end of communication, rather than requiringunnecessary tradeoffs.
- Provide end-to-end security.
- Establish visibility and transparency of a particular communication.
- Respect user privacy.

PbD is the only prominent approach that addresses privacy entirely at the design stages of IoT application deployments,[6,11,12] a verdict supported by both the FTC and the European Commission. PbD ensures IoT privacy through an emphasis on sensing technologies, cloud computing, big data analysis, and legal regulations.

> Privacy by design considers privacy requirements as organizational goals in business and identification processes.

Open Research Issues and Design Guidelines
The IoT will likely be the underlying fabric of the next generation of networks, such as 5G, which might increase network capacity and connectivity. The available PETs for underlying IoT technologies aren't directly compatible with the IoT's heterogeneous characteristics. Privacy should be improved in IoT applications from the perspective of individuals and groups. Two main principles should be followed: don't violate user privacy, and maintain user control of the operations. If the IoT technology providers can't win consumers' trust and confidence, development of innovative utilizations of these new technologies will slow down. Threats and vulnerabilities related to user privacy are major reasons for users' lack of trust in IoT applications. With multiple underlying technologies, the IoT requires general privacy preservation policies, along with common and flexible legal platforms. Certain critical IoT deployments—such as eHealth and surveillance applications—require extra attention to preserve user and data privacy.

Preserving IoT privacy using PbD is an approach still in its infancy, and open research questions remain. Specifically, to establish PbD solutions for IoT privacy, we must

- define a general model for IoT privacy;
- develop innovative enforcement PETs based on PbD to enable scalability and heterogeneity in IoT; and
- implement and integrate the solutions with the perfect balance of privacy policies, localization and tracking requirements, and sensitive data access control mechanisms.

The Social IoT is an emerging IoT paradigm. The SIoT lets objects create a social network autonomously, with minimal or no human intervention.[2] Imposing rules to protect user privacy in the SIoT is important, particularly when accessing the results of autonomous interactions between objects. It's necessary to obtain pervasive IP-based solutions to preserving privacy in the IoT, accompanied by energy-efficient, low-cost, high-performance, and scalable algorithms.

The current trend in IoT privacy protection includes user-centric and context-aware privacy policies. Other emerging trends are in context-centric and self-adaptive privacy-preserving mechanisms and protocols that support ambient intelligence. Privacy preservation of datastreams in the IoT is another relatively novel field; it might also require dynamic data access control mechanisms and data management policies. Moreover, many unsolved privacy issues have emerged due to the rapid increase in the use of genomic datasets and software packages related to medical activities.[13]

Another open research question is how we might implement incentives in the IoT architecture's privacy-preserving protocols using game theory.[14] Game theory could be used to analyze location privacy, find the economic aspects of privacy, and evaluate the balance between trust and privacy. In the next generations, context management should interact with underlying IoT technologies and address the related privacy issues to improve the quality of context. Alternatively, adapting a network virtualization solution, such as software-defined networks (SDNs),[15] is a potential approach for preserving privacy in large-scale data handling in IoT deployments and cloud management. Developing more sophisticated privacy models and appropriate design of provably private, yet practically relevant, privacy-oriented security protocols and mechanisms has been identified as an important research direction for the coming years.[16] However, more importantly, we need the PETs for the IoT to go beyond the research level and adapt with real-time deployments and practical use. Finally, new research issues might arise regarding privacy as other emerging technologies—such as software-defined networking with IoT—are introduced and combined.

The privacy challenges we've described here must be addressed to establish trustworthy IoT applications. Incorporating privacy protection at the design level would be more convenient than trying to retrofit them into the available solutions. Nevertheless, it's unlikely that technical solutions alone will be able to completely prevent privacy issues in IoT applications. We must consider—and appropriately balance—a combination of technical and legal means to achieve privacy-enhancing solutions in IoT. ●●●

Acknowledgments

References

1. D. Miorandi et al., "Internet of Things: Vision, Applications and Research Challenges," *Ad Hoc Networks*, vol. 10, no. 7, 2012, pp. 1497–1516.
2. R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, 2013, pp. 2266–2279.
3. J. Gubbi et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, Elsevier, vol. 29, no. 7, 2013, pp. 1645–1660.
4. D. Storm, "MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks," *Computerworld*, 8 June 2015; www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html.
5. *Internet Security Threat Report*, Synantec Corporation Annual Report, 2013, www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.
6. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC Report, 2012; www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer

-privacy.

7. R.H. Weber, "Internet of Things—New Security and Privacy Challenges," *Computer Law and Security Rev.*, vol. 26, no. 1, 2010, pp. 23–30.

8. C. Aggarwal, N. Ashish, and A. Sheth, "The Internet of Things: A Survey from the Data-Centric Perspective," *Managing and Mining Sensor Data*, Springer, 2013, pp. 383–428.

9. S. Zeadally et al., "Vehicular Ad hoc Networks (VANETS): Status, Results, and Challenges," *Telecommunication Systems*, vol. 50, no. 4, 2010, pp. 217–241.

10. N. Li et al., "Privacy Preservation in Wireless Sensor Networks: A State-of-the-Art Survey," *Ad Hoc Networks*, vol. 7, no. 8, 2009, pp. 1501–1514.

11. N. Fabiano, "The Internet of Things: Establishing Privacy Standards Through Privacy by Design," *Cutter IT J.*, vol. 26, no. 8, 2013; www.cutter.com/article/internet-things-establishing-privacy-standards-through-privacy-design-417276.

12. R. Herold, "Privacy and Security in the Internet of Things," *Cutter IT J.*, vol. 26, no. 8, 2013; www.cutter.com/article/privacy-and-security-internet-things-417251.

13. M. Femminella et al., "Networking Issues Related to Delivering and Processing Genomic Big Data," *Int'l J. Parallel, Emergent and Distributed Systems*, vol. 30, no. 1, 2015, pp. 46–44.

14. M.H. Manshaei et al., "Game Theory Meets Network Security and Privacy," *ACM Computer Surveys*, vol. 45, no. 3, 2013, article 25.

15. S.J. Vaughan-Nichols, "OpenFlow: The Next Generation of the Network?" *Computer*, vol. 44, no. 8, 2011, pp. 13–15.

16. E. Borgia, "The Internet of Things Vision: Key Features, Applications and Open Issues," *Computer Comm.*, vol. 54, Dec. 2014, pp. 1–31.

PAWANI PORAMBAGE *is a PhD candidate and researcher in the Centre for Wireless Communication at the University of Oulu, Finland. Her research interests include lightweight security protocols, security and privacy on Internet of Things, and wireless sensor networks. Porambage has an MSc in ubiquitous networking and computer networking from the University of Nice Sophia-Anipolis, France. Contact her at pporamba@ee.oulu.fi.*

CORINNA SCHMITT *is head of the Mobile and Trusted Communications Team in the Communication Systems Group at the University of Zurich, Switzerland. Her research interests include mobile communications, Internet of Things, wireless sensor networks, trust, and security. Schmitt has a PhD in computer science from the Technische Universität München, Germany. She's a member of ACM and IEEE. Contact her at schmitt@ifi.uzh.ch.*

PARDEEP KUMAR *is a postdoctoral researcher in the Department of Computer Science, Faculty of Science and Technology, at UiT The Arctic University of Norway, Tromso, Norway. His research interests include network security, wireless sensor networks, Internet of Things, and smart grid. Kumar has a PhD in computer science (ubiquitous IT) from Dongseo University, South Korea. Contact him at pradeepkhl@gmail.com.*

ANDREI GURTOV *is a principal scientist at the Helsinki Institute for Information Technology (HIIT) and an adjunct professor at Aalto University, University of Helsinki, and University of Oulu. His research interests include network security, wireless and sensor networks, and 5G. Gurtov has a PhD in computer science from the University of Helsinki. He's a senior member of IEEE and an ACM Distinguished Scientist. Contact him at gurtov@hiit.fi.*

MIKA YLIANTTILA *is a professor in the Centre for Wireless Communications, Faculty of Information Technology and Electrical Engineering (ITEE), at University of Oulu, Finland, where he's also an adjunct professor in computer science and engineering. His research interests include broadband communications networks and systems, focusing on wireless security, mobility management, distributed systems and novel applications. Ylianttila has a doctorate in communications engineering from the University of Oulu. He's a senior member of IEEE. Contact him at mika.ylianttila@ee.oulu.fi.*

ATHANASIOS V. VASILAKOS *is a professor of mobile systems at the Lulea University of Technology, Sweden. His research interests include networks, cloud computing, security, big data, and medical informatics. Vasilakos has a PhD from the University of Patras, Greece. Contact him at th.vasilakos@gmail.com.*